Spring 2008
Volume 10
Number 1

The Guardian

The Source for Antiterrorism Information

In This Issue

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

The Pentagon, Room MB917
Washington, DC 20318

"We will prevail. We will prevail in this ideological struggle because liberty is powerful. Liberty is hopeful. The enemy we face can only convince people to join their cause when they find hopelessness. And so our strategy is threefold: one, protect the homeland; two, stay on the offense against these folks; and three, provide an alternative—a hopeful alternative to despair and doubt and hopelessness."

—President George W. Bush
January 31, 2008

"We should also remember that terrorist cells in Europe are not purely homegrown or unconnected to events far away—or simply a matter of domestic law and order. Some are funded from abroad. Some hate all western democracies, not just the United States. Many who have been arrested have had direct connections to al Qaeda. Some have met with top leaders or attended training camps abroad. Some are connected to al Qaeda in Iraq. In the most recent case, the Barcelona cell appears to have ties to a terrorist training network run by Baitullah Mehsud, a Pakistan-based extremist commander affiliated with the Taliban and al Qaeda—who we believe was responsible for the assassination of Benazir Bhutto.

What unites them is that they are all followers of the same movement—a movement that is no longer tethered to any strict hierarchy but one that has become an independent force of its own. Capable of animating a corps of devoted followers without direct contact. And capable of inspiring violence without direct orders.

It is an ideological movement that has, over the years, been methodically built on the illusion of success. After all, about the only thing they have accomplished recently is the death of thousands of innocent Muslims while trying to create discord across the Middle East. So far they have failed. But they have twisted this reality into an aura of success in many parts of the world. It raises the question: What would happen if the false success they proclaim became real success? If they triumphed in Iraq or Afghanistan, or managed to topple the government of Pakistan? Or a major Middle Eastern government?"

—Secretary of Defense Robert M. Gates
February 10, 2008

"We need partners, relationships, and it's the strength of those relationships that I think is most vital in terms of how we're going to engage the challenges that we have in the future. Front and center in that is the whole issue of terror tied to weapons of mass destruction, and one of the things I worry the most about is those two things coming together. And I know for a fact that there are those that are seeking to a significant extent to bring those two together.

Clearly, right now, we have challenges in Iraq and Afghanistan. Broadly, quite frankly, we've got challenges in the Middle East, from what I call "Tehran to Beirut." That ... is an incredibly important part of the world, and we're a long way from a stable environment."

—Chairman of the Joint Chiefs of Staff ADM Mike Mullen
February 22, 2008

GUARDIAN FEEDBACK AND CONTRIBUTIONS

The Guardian is soliciting input for the Summer 2008 edition. Please direct your comments, feedback, and articles to: guardian@js.pentagon.mil

Editor's Note on "Lessons Learned: The Fort Dix Six" (Winter 2007 edition): The article's opening paragraph should have said "arrested in May 2007," not May 2006, as was printed. To update our readers, the trial of the Fort Dix conspirators has been moved to September 29, 2008.

I am asking you, the *Guardian* readership, for your feedback at www.guardianfeedback.xservices.com. Your input will help make the *Guardian* a more useful product to the Protection community. The inputs to the magazine we have had never cease to amaze me. To date, these thoughtful injects into the all-hazards approach stimulate good discussion and facilitate an important dialogue for the community.

While many consider our most dangerous threat to be al Qaeda–affiliated groups, other terrorist groups, such as Hezbollah, should not be discounted. Just as troubling, the threats to our forces from criminal elements and random acts of violence remain the more probable threat. The force protection provisions implemented are to protect ourselves not just from transnational terror groups, but from the myriad individuals and groups that wish us harm. While the recent attack against the recruiting station in NYC was without an apparent terror nexus, it nonetheless was an attack.

At a recent threat conference, I heard Mr. John Robb, author of *Brave New War*, speak about open-source warfare and what he terms "Global Guerrillas." He points out that the future terror threat will morph into small, agile groups, operating toward independent ends without external guidance. They will use replication and learning from other groups to increase both their chances of success and their attempts to increase the carnage of their attack. This is a topic in which I am interested: future asymmetric and disruptive threats that our adversaries may employ. We should all be thinking of the future threat and how to prepare ourselves.

As we see highlighted in Iraq and Afghanistan, the majority of missions undertaken by DOD are in conjunction with our interagency partners. The same is true of the Protection mission. Law enforcement and intelligence agencies must be leveraged while preparing the force protection construct. Indeed, the civilian agencies will often have the lead in the investigation, prosecution, and thwarting of an attack. Not being "in control" of the situation is counter to the method under which most military commands operate, especially if a threat is directed toward our personnel. Nevertheless, it is incumbent upon all of us to get smart on how interagency actions work, not just for terrorism, but particularly in the planning phases of consequence management.

The threats to our way of life remain serious and tangible. As we witness the atrocities and self-defeating results of extremism in Iraq, Afghanistan, and Pakistan, we must never forget that they underestimate our resolve to prevail.

The price of freedom is eternal vigilance.
—Thomas Jefferson

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

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

SUBMITTING NEWS & ARTICLES

The opinions, conclusions, and recommendations expressed or implied within are those of the contributors and do not necessarily reflect the views of the Joint Staff, DOD, or any other agency of the Federal Government. The editors invite articles and other contributions on antiterrorism and force protection of interest to the Armed Forces. Local reproduction of our newsletter is authorized and encouraged.

Joint Terrorism Task Forces: Protecting DOD from Terrorist Attacks

By Mr. Gregory Fuller, CIFA

The terrorist attacks on the Khobar Towers, the USS COLE, and the Pentagon are only the most recent and visible reminders that DOD is one of the prime targets, if not the prime target, of terrorist aggression against the United States. Even today, in places like Iraq, Afghanistan, and Indonesia, the men and women of DOD live under the constant threat of imminent terrorist attacks. Of all the steps DOD has taken to prevent and protect against future terrorist attacks, what has DOD Counterintelligence (CI) done?

Overseas, DOD has partnered with the Department of State to establish the Force Protection Detachment (FPD) program (for more information, see "Force Protection Detachments: Partnering with Foreign Nation Counterparts" in the April 2007 issue of *The Guardian*). The FPD program permanently places DOD CI special agents at overseas locations with significant numbers of "in transit" DOD ships, personnel, and aircraft—but without a permanent DOD CI support presence—to provide current and actionable force protection information to the in-transit commander.

In the United States, DOD has partnered with the Federal Bureau of Investigation (FBI), the lead agency for counterterrorism (CT) within the United States, by placing DOD CI special agents on FBI-led Joint Terrorism Task Forces (JTTFs). Designated by the FBI as the "nation's front line on terrorism," JTTFs are charged with protecting America from terrorist attacks. DOD special agents work shoulder-to-shoulder with FBI special agents investigating suspected terrorist activity, coordinating counterterrorist activities, and sharing terrorist information.

Designated by the FBI as the "nation's front line on terrorism," JTTFs are charged with protecting America from terrorist attack. DOD special agents work shoulder-to-shoulder with FBI special agents investigating suspected terrorist activity, coordinating counterterrorist activities, and sharing terrorist information.

In the News

In a recent case, DOD special agents working on JTTFs were an integral part of the investigation and apprehension of Hassan Abujihaad, a former US Navy sailor. Evidence suggested Abujihaad (also known as Paul R. Hall) corresponded via e-mail with

known al Qaeda operatives during his duty aboard the USS BENFOLD. In the e-mails, Abujihaad provided sensitive ship locations and vulnerabilities, praised those responsible for the USS COLE bombing in Yemen, and discussed killing fellow naval personnel. In March 2007, officers from the Phoenix JTTF arrested Abujihaad and charged him with supporting terrorism and terrorist organizations with the intent to kill US citizens and transmitting classified information to unauthorized people.

Barely four months before these events, Derrick Shareef (who had significant connections with Abujihaad) was arrested in December 2006 by members of the Chicago JTTF. Shareef was arrested after having purchased several hand grenades and a handgun with the intent of attacking a Chicago-area shopping mall during the last Friday before the Christmas holiday.

These cases, along with the recent disruption of terrorist attack plans at Fort Dix and New York's Kennedy airport, support the belief that future terrorist activities are likely to be conducted by small groups of people with either prior military training or access to a military facility.

The Inception of JTTFs and DOD Participation

The devastating attacks on the World Trade Center and the Pentagon in September 2001 exposed significant weaknesses in our national security architecture. Terrorists were training and planning attacks within our borders while coordinating with terrorist networks outside the United States. Subsequently, the 9/11 Commission identified the critical necessity of interagency cooperation and communication. The FBI, charged with the lead to counter terrorist activity within the United States, chose JTTFs as the primary investigative and operational method to achieve interagency cooperation and communication.

The JTTF program was established by the FBI's CT division based on a 1980 New York City task force model that incorporated members from federal, state, and local law enforcement to combat an increasing number of terrorist bombings. Prior to 9/11, there were 35 JTTFs in existence throughout the United States. The FBI has since expanded the number of JTTFs to one at each of its 56 field offices and to approximately 46 of its annexes. Over 2,000 full- and part-time non-FBI personnel from more than 600 federal, state, and local agencies currently participate on JTTFs in support of terrorist-related investigations.

The FBI also established the National Joint Terrorism Task Force (NJTTF), a multiagency task force co-located with the National Counterterrorism Center in McLean, Virginia. The NJTTF serves as a point of fusion for 44 federal, state, and local agencies, each providing full-time representatives and meeting daily to share timely CT-related information. Fully 27 percent of the NJTTF is composed of DOD agency representatives (12 agencies in all), ensuring DOD interests are well represented at the national level.

The DOD JTTF program

The DOD JTTF program enables Service CI agencies to partner with local, state, and federal law enforcement agencies at FBI-led JTTFs to detect and neutralize terrorists, terrorist-enabling individuals, and organizations that threaten DOD interests, such as in the case of Hassan Abujihaad. The DOD special agents work closely with FBI special agents on terrorism-related investigations with an eye toward the DOD connection in each case. DOD agents participate in significant CT operations to identify, recruit, and direct assets in the identification and collection of information on suspected terrorist cells and organizations operating within the United States and targeting DOD and US assets. Additionally, special agents perform a vital liaison role, continually exchanging information with participating JTTF agencies and facilitating the coordination of activities between FBI and DOD.

In March 2002, Congress appropriated funding for DOD

Hunting Foreign Intelligence Officers

Under the jurisdiction of the FBI, one DOD special agent was able to identify and investigate an undercover intelligence officer from a hostile foreign government operating within the United States. The operative was collecting information on US Soldiers in the Denver area in an attempt to recruit Iraqis, conduct preoperational surveillance, and gather intelligence. When the operative discovered that he was being investigated, he fled the United States and disappeared.

At that point, the FBI would normally have forwarded the case to DOD for eventual follow-up—but because a DOD special agent was already assigned to the Denver JTTF, that agent continued the investigation without interruption. Working with other DOD agencies, he located the operative in Iraq and coordinated with the US Army Special Operations Command to develop a strike plan. The operative was subsequently arrested and incarcerated and has since provided valuable information in the War on Terror.

participation in the FBI's JTTF program. Currently, DOD provides over 75 CI special agents to nearly 50 of the more than 100 JTTFs. DOD CI representation is comprised of one or more special agents from the Air Force Office of Special Investigations, Army Military Intelligence, or Naval Criminal Investigative Service. Assigning CI agents to the FBI's JTTFs enables DOD to be directly involved in FBI terrorist investigations and CT activities affecting DOD equities, provides access to FBI-derived terrorist threat data, and improves operational partnerships with US law enforcement agencies.

DOD Interaction on the JTTFs

Although the FBI maintains jurisdiction and investigative oversight, JTTFs enable non-Bureau participation in a wide range of investigations and operations related to suspected terrorist activity. The JTTFs also serve as a focal point for sharing collective resources and hard-to-access, agency-specific information from each participating agency.

Expanded Jurisdiction

Because of the broad range of laws under the purview of the FBI, DOD special agents, by virtue of their assignment to the JTTFs, are able to participate in significantly more investigations and operations than would otherwise be available to them. This expanded participation translates into more thorough DOD involvement in CT cases.

Deputation is one tool that JTTFs use to expand the jurisdiction of state and local law enforcement officers. Some JTTFs deputize all agents as a matter of practice, whether they are federal, state, or local law enforcement officers. Deputation expands the jurisdiction of the special agents to the FBI's jurisdiction, protects the agents' parent organization by elevating all litigation to the federal court system, and provides all JTTF participants with unified identification credentials, which reduces public confusion over varied agency badges.

Advocacy in Cases

DOD special agents are the resident experts on the Department for JTTFs and are best able to identify a real or potential DOD nexus among developing JTTF cases and leads. Furthermore, DOD agents advocate further development of potential DOD-related cases and leads that would not otherwise be pursued, enhancing the protection of DOD equities. Additionally, because DOD agents can identify a DOD nexus sooner than other agents could, they are involved earlier and in more cases.

Database Access

The agencies participating on the JTTFs are easily able to share, through the discretion of their special agents, agency-specific information within the task force. This information sharing enables DOD to develop a fuller understanding of a person, place, or organization.

DOD agents have supported information security checks for local military security forces. In the event of a suspicious person requesting access, the local security office can contact the special agent and request a more thorough background check in real time. The special agent, in effect, enables the local security forces to better respond to suspicious persons while intelligently adjusting the force protection responses quickly and more accurately.

The FBI's Guardian database system is designed to share a terrorist-related investigative lead with all the appropriate JTTFs. Through this system, a DOD agent can nominate a DOD-related terrorist lead for review and action by any JTTF, leveraging all JTTFs and participating special agents to develop DOD leads. The Guardian system's storage and sharing capabilities also make it the ideal solution to replace the DOD Threat and Local Observation Notice (TALON) database, which has now been terminated. Currently, DOD suspicious incidents and activity reports are being entered into the Guardian database, providing additional information in support of JTTF investigations.

A Better DOD Workforce

The collaborative efforts of DOD CI special agents working in conjunction with members of the federal, state, and local law enforcement agencies foster a significantly greater level of interagency trust and communication. In addition to the primary benefits to DOD previously mentioned, JTTFs also enhance and expedite coordination and information sharing among DOD and the participating agencies.

Accelerated Interagency Coordination

JTTFs are catalysts for accelerated interagency coordination and allow

The Keen Eye of DOD Experience

A commercial photo lab employee provided the FBI with photographs showing suspicious items, possibly improvised explosive devices (IEDs) commonly used by terrorists. Although the FBI special agents recognized the items in the photographs as suspicious, it was the DOD special agent who recognized the location of the photographs as a ship's berthing area; the address in one of the pictures as that of a ship at sea's mailing address; and the possible IEDs to be, in reality, training items for crew exercises. The DOD agent was able to prevent valuable time and resources from being spent on a needless investigation through his knowledge of Navy equipment and his placement on the JTTF.

DOD special agents to leverage their task force partners to provide increased and regular support to DOD events. Events that previously took weeks or months to coordinate can now be coordinated in days or weeks among fellow special agents. A DOD agent needs only to reach out to a fellow agent within the room, rather than over the telephone or across the city, to coordinate a DOD event. Additionally, for specific threats, emergencies, and crises, DOD special agents are already fully integrated into the JTTFs and are able to immediately engage in appropriate responses, investigations, and operations rather than arriving at a JTTF after the event and trying to learn the task force's practices while the rest of the team is focused on developing the investigation.

In the hours after the bombing of the USS COLE, the FBI immediately began putting together a task force to investigate the crime. One of the first members of the task force was a DOD special agent already assigned to the New York JTTF. The DOD agent served as a vital link in coordinating FBI activities with the US Navy and DOD. Based on his experience on the JTTF, the DOD special agent was able to translate and clearly articulate FBI requirements to the Navy leadership and, in turn, advise the FBI on the proper Navy protocols and culture. This communication dramatically reduced the confusion and misconceptions to which high-profile, multi-agency terrorist investigations are prone.

Experience and Tools

Each special agent brings his or her own agency's unique tools, techniques, training, and experiences that are useful to investigations and operations. These experiences and tools focus all of the assets of the various organizations on developing terrorist cases and creating faster responses, clearer leads, and better information, which result in improved case resolution. Some examples of agency-specific experience or tools include the local police department's detailed knowledge and understanding of the local area, the FBI's Crime Lab, the Drug Enforcement Agency's El Paso Intelligence Center (EPIC), and numerous multiagency databases within the Department of Homeland Security.

Stronger Professional Relationships

DOD special agents work daily with their fellow agents, building and strengthening their professional relationships. The team concept of a JTTF creates an enhanced level of trust and understanding among the various agencies' special agents. The JTTF environment encourages coordination and collaboration to guarantee that every member is working toward the same goal. Task force experiences also facilitate better working relationships with other agencies when former DOD agents take their JTTF experiences with them in their DOD careers. DOD agents are able to draw on these past JTTF experiences to "break the ice" and accelerate building new interagency relationships in their future assignments. Furthermore, because they have worked so closely with fellow special agents from other agencies, they understand the restrictions and capabilities of the non-DOD organizations and can more easily work through these challenges to achieve greater success.

These examples of benefits to DOD's participation on JTTFs are far from exhaustive. DOD special agents regularly reap these and other benefits throughout the course of the day, each time drawing DOD closer to the FBI and other participating agencies while simultaneously seeking, finding, and neutralizing the next terrorist threat to DOD and to the United States.

In the hours after the bombing of the USS COLE, the FBI immediately began putting together a task force to investigate the crime. Based on his experience on the JTTF, the DOD special agent was able to translate and clearly articulate FBI requirements to the Navy leadership and, in turn, advise the FBI on the proper Navy protocols and culture. This communication dramatically reduced the confusion and misconceptions to which high-profile, multiagency terrorist investigations are prone.

Making DOD a Hard Target

The previous terrorist attacks on the Khobar Towers, the USS COLE, and the Pentagon and averted attacks like that at Fort Dix serve as grim reminders of the terrorist threat to the United States. Would-be terrorists indicate that the terrorist threat has not gone away but is constantly changing to exploit weaknesses in our national security. The FBI's JTTF program has become the primary investigative and operational arm in the fight against terrorist activity in the continental United States. The DOD JTTF special agents serve as a vital link among the FBI, other participating agencies, and DOD in providing information essential to protecting Service members and in participating in investigations and operations to detect, deter, and disrupt terrorist plans at home and abroad. With DOD coverage in nearly 50 JTTF offices, DOD special agents are on the front line in the War on Terror in the United States.

Critical Infrastructure: Vital Incident Response and Reporting

By MAJ Jason Strickland

MAJ Jason Strickland is a Critical Infrastructure Protection (CIP) Planner at Standing Joint Force Headquarters North (SJFHQ-N), USNORTHCOM's deployable Directorate.

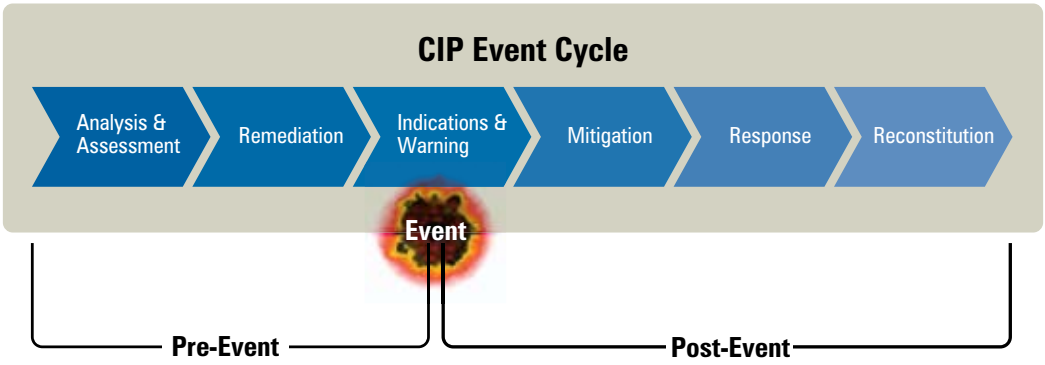
Much of the Defense Critical Infrastructure Program (DCIP) has been focused to date on pre-incident activities such as identification, prioritization, assessment, deterrence, mitigation, and prevention. The consequences of an all-hazards catastrophic event for our nation's critical infrastructure and key resources (CI/KR) must also be appropriately addressed.[1] Current DCIP publications do not broach the subject of catastrophic incident response in regard to defense critical infrastructure. Department of Defense Directive (DODD) 3020.40, the authoritative DCIP document, limits the DCIP to "identification, assessment, and security enhancement" of DOD critical infrastructure and vaguely mentions "support incident management" in word but not in action.[2] The Defense Industrial Base (DIB) Sector-Specific Plan, required by the National Infrastructure Protection Plan (NIPP), neglects any mention of response activities as they pertain to either DOD-owned infrastructure or that which falls under the DIB.[3] Military operators and planners must understand and adapt to effects in the remaining 17 CI/KR sectors[4], which have direct bearing on DIB assets, DOD facilities, and the ability of the military to fulfill its assigned missions. This article outlines recommendations for DOD response to a catastrophic incident as it pertains to critical infrastructure.

First, I will address one of the major findings from Hurricane Katrina: Build a common operating picture (COP) for the Department of Homeland Security (DHS) and DOD.[5] Second, I will discuss DOD's presence in the vicinity of that incident. Finally, I will offer recommendations that should be considered by DHS and DOD.

Learning from Our Past

One of the many lessons learned from Hurricane Katrina regarding critical infrastructure and DOD's response was that an effective COP did not exist between DHS and DOD.[6] Although there are many ways to achieve a COP via networks, RSS feeds, SharePoint portals, and other technologies, the key enabler of information sharing in this context is relationships. Repeatedly in after-action reviews regarding interagency activities, the importance of preexisting operational relationships surfaces as an area to improve among agencies, governments,

> *"The chief of strategy for Ahmadinejad, Hassan Abbassi, has said: 'We have a strategy drawn up for the destruction of Anglo-Saxon civilization ... we must make use of everything we have at hand to strike at this front by means of our suicide operations or means of our missiles. There are 29 sensitive sites in the US and the West. We have already spied on these sites and we know how we are going to attack them....'"*
>
> *—Senate Committee on the Judiciary Wartime Executive Power and the NSA's Surveillance Authority II; February 28, 2006; testimony of R. James Woolsey*



departments, and organizations. This need is especially important with regard to interagency partners and Defense Support of Civil Authorities (DSCA) events as they pertain to DOD. In more conventional settings, the DOD has had an "I'm in charge" mentality (and appropriately so) with regard to our standard (nondomestic) mission set. In DSCA, the paradigm shifts to local agencies, first responders, and, ultimately, the Incident Commander.[7] At US Northern Command (USNORTHCOM), this perspective is certainly being promulgated.[8] Both formal and informal relationships continue to be established to take advantage of the wealth of information available for commanders and decision makers. USNORTHCOM established a robust Joint Interagency Coordination Group (JIACG), composed of more than 60 agencies, to facilitate relationships among interagency partners with whom the DOD and USNORTHCOM may interact during a catastrophic event. Many of these agencies maintain a full-time presence at USNORTHCOM, whereas others fold into the JIACG when responding to a crisis (or during appropriate exercises). This activity relates to sharing critical infrastructure information by focusing on the formal and informal relationships at the three-letter agency level. DHS, DOD, and USNORTHCOM have exchanged senior representatives to emphasize the importance of these relationships. Exchanges also take place informally and at lower levels. Within USNORTHCOM's Force Protection/Mission Assurance Division, relationships are established with the DHS Office of Infrastructure Protection's Protective Security Advisors (PSAs) and the National Infrastructure Coordinating Center (NICC), with state critical infrastructure representatives, with Defense Infrastructure Sector Lead Agents (DISLAs), and with intelligence and law enforcement organizations. USNORTHCOM also has access to DHS data networks (e.g., Constellation/Automated Critical Asset Management System [C/ACAMS], Cyber Warning Information Network [CWIN], Homeland Security Information Network (HSIN)). All of these relationships facilitate aggressive information sharing and result in a more effective COP, supporting the national strategy for protecting CI/KR.[9]

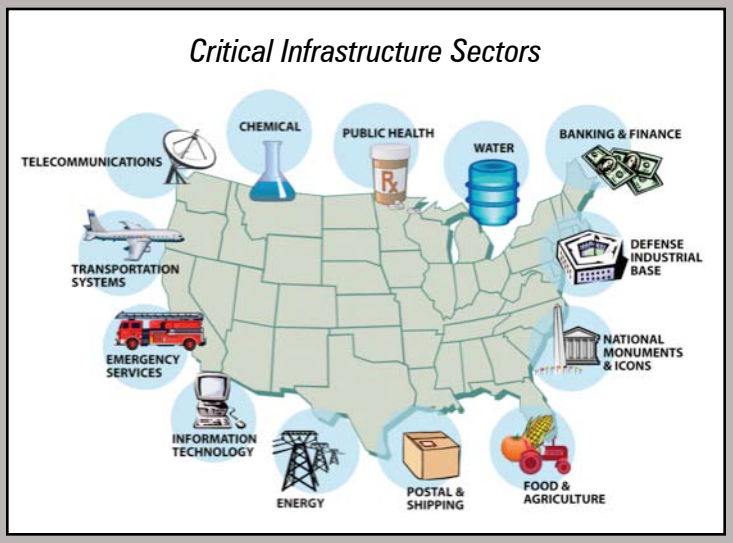
This emphasis on critical infrastructure information sharing is supported by the Governors' Homeland Security Advisory Council. Protecting critical infrastructure remains the third-highest concern among the 56 state and territorial homeland security advisors.[10] Increasingly, the states are working together to share information regarding critical infrastructure through organizations such as the All Hazards Consortium, a group of eight mid-Atlantic states and the District of Columbia that share in a "culture of collaboration" to prepare the region for all types of hazards.[11] The DOD would be well served to maintain informal relationships with organizations of this type to foster rapid interagency response once a catastrophic event occurs.

On-Scene Activities

Although information sharing among DHS, DOD, and others continues to improve, on-scene activities in the aftermath of a catastrophic incident are crucial to fulfilling DOD's responsibilities within the National Response Framework (NRF). DOD response begins with the activation of a Defense Coordinating Officer (DCO) or a Defense Coordinating Element (DCE) that serves as DOD's single point of contact within the Joint Field Office (JFO).[12] It is well known that in the event of a significant catastrophic event, the DCE assigned to the affected Federal Emergency Management Agency (FEMA) region will quickly become overwhelmed and need rapid augmentation.[13] With regard to critical infrastructure, the DCE must speedily coordinate with the DHS Infrastructure Liaison (IL) within the JFO. The IL is usually a DHS PSA who serves as the chief advisor to the Unified Coordination Group in support of the Principal Federal Official (PFO) regarding all CI/KR.[14] DOD's interests can and should be represented by having their own envoy within the JFO (as a part of the DCO or DCE working in either the Operations or Planning Section) who can coordinate with the IL. From this location, a DCIP representative can adequately exchange appropriate information with the IL, USNORTHCOM, US Army North (ARNORTH), Emergency Support Function (ESF) 3 members (if activated), the DCO or DCE, and local infrastructure-

related agencies. Most of the critical infrastructure on which DOD relies falls outside of traditional military installations and, in fact, is not owned by DOD.[15] The overwhelming majority of defense critical infrastructure is the DIB and is managed by the Defense Contract Management Agency (DCMA). Having a DOD infrastructure representative on-scene who can adequately communicate the interests, capabilities, dependencies, and priorities of DOD in mid-crisis would be beneficial for all parties.[16]

Consider as an example a DIB asset that contains the overwhelming majority of the anthrax or smallpox vaccinations for DOD personnel. An incident occurs nearby that permanently disrupts the power to this facility. The IL in the JFO may not recognize the necessity to protect (or ensure power generation for) such a facility. In contrast, a DOD representative can advise the Unified Coordination Group on-scene through the IL to prioritize recovery of this facility. As another example, suppose that a natural disaster severely affects one of DOD's power projection platforms, thereby rendering the installation unable to fulfill critical responsibilities for a numbered operations plan (OPLAN). Although senior federal decision makers will undoubtedly influence this situation in Washington, on-scene a DOD infrastructure representative can work with the local or regional representatives in order to promptly restore this crucial capability.



A DOD representative can gain situational understanding as to why DOD forces may need to be employed to protect non-DIB assets. As a final example, consider the Trans-Alaska Pipeline System (TAPS) running through that state. Imagine a catastrophic event occurs that requires use of Title 10 forces to protect vulnerable points along the pipeline, despite its not being a DIB asset. Although this scenario is unlikely, it remains a possibility and therefore captures the necessity of having a DOD infrastructure representative in the JFO.

Simple Suggestions

Based on the previous discussion, I recommend the following for consideration. First, establish and formalize a standing (though not necessarily permanent) relationship among DOD, USNORTHCOM, and DHS at the NICC, the epicenter of critical infrastructure information sharing. The NICC, within the DHS OIP, serves as the cornerstone of multidirectional communication exchange between the private sector, the interagency critical infrastructure protection (CIP) community, state and local CIP stakeholders, and DHS for reporting threats and impacts to the nation's CI/KR. The NICC is one of five elements of the DHS National Operations Center (NOC) and often receives vital, timely information regarding an incident concurrent with local law enforcement or other operations centers. Because the information at the NICC is frequently reported by the private sector (and keeping Protected Critical Infrastructure Information [PCII] and other private-sector information-sharing sensitivities and limitations in mind), the NICC often has situational awareness of critical incidents and their impacts prior to absorption into standard DHS (and certainly DOD) operational reporting channels. Furthermore, this information is not limited to the CI/KR realm. Through its relationships with other NOC elements, the NICC often coordinates intelligence information, Law Enforcement Sensitive reporting, and information on incidents from across the interagency community. Interaction with these sectors is fundamental to DOD's ability to project power because in the event of an all-hazards scenario, there may be significant effects to military capabilities related to electric supply, transportation, communications, etc.

Results of this relationship were already tested and proven with great success during TOPOFF4 and the USNORTHCOM exercise VIGILANT SHIELD in October 2007 and in previous national-level exercises (NLEs) involving USNORTHCOM. USNORTHCOM (as well as DHS) would greatly benefit by having a representative in the NICC during National Special Security Events (NSSEs), operations, crises, and exercises. This infrastructure representative could assist in information exchange and, ultimately,

assist DOD in anticipating potential DSCA mission assignments (MAs). Additionally, at the DCIP Monitoring and Reporting Table Top Exercise (TTX) II, hosted by the Defense Intelligence Agency (DIA) in February 2008, one of the conclusions with regard to the DCIP Monitoring and Reporting Concept of Operations was to explore the possibility of a more formalized relationship between DCIP and the NICC.

The mission of the National Infrastructure Coordinating Center is to maintain operational awareness of the nation's critical infrastructures and key resources, and provide a mechanism and process for information sharing and coordination among government and industry partners.

A second recommendation was to formalize reporting procedures in DODD 3020.40. As indicated previously, there is a lack of emphasis on this aspect of the DCIP. Procedures are in place to report on threats and hazards to defense critical infrastructure; however, formal mechanisms to describe post-incident critical infrastructure do not exist in the directive.[17,18] Initial questions from commanders and decision makers following a catastrophic event will be directed to critical infrastructure operators and analysts. What is the impact to our (DOD) assets? When will partial and full capability be restored? Are there any cascading effects on other assets in the vicinity of the event? These inquiries, among others, must have a reporting mechanism so that commanders can make informed decisions on how to respond. This situation further emphasizes the importance of having a DOD infrastructure representative in the vicinity of the JFO talking directly with the IL, the Joint Force Headquarters–State (JFHQ-State) representatives, and the appropriate personnel in a state Emergency Operations Center (EOC).

Final Remarks

Since its formal inception, the DCIP has made great strides in identifying, prioritizing, and assessing CI/KR. We are moving in parallel with DHS to ensure effective protection measures are taken for our Task Critical Assets (TCAs) and Defense Critical Assets (DCAs). In essence, most "before the event" risk is being resourced, assessed, and mitigated; however, "after the event" risk remains an area of concern. An effective COP between DHS and DOD can be further enhanced. First, DCIP and DIB representation near the vicinity of the event (JFO, JFHQ-State, state EOC) can facilitate rapid assessments of the infrastructure and the effects on surrounding CI/KR. Second, liaising with the NICC immediately after a catastrophic event will provide DOD and USNORTHCOM with accurate, timely, relevant, and authoritative national infrastructure information. Finally, NICC representation will provide an enhanced capability and will help DOD anticipate future requests for assistance (RFAs) based on the situation at hand.

---

1 Department of Homeland Security (DHS). National Response Framework, January 2008, p. 42.

2 DODD 3020.40, Defense Critical Infrastructure Program, 19 August 2005, p. 2. (An updated version of DODD 3020.40 is currently in review for publication at a later date.)

3 DOD. *Defense Industrial Base: Critical Infrastructure and Key Resources Sector-Specific Plan as Input to the National Infrastructure Protection Plan,* May 2007.

4 DHS recently approved an 18th CI/KR sector (Critical Manufacturing) (Chertoff, Michael, memorandum, Department of Homeland Security, subject: Identification and Establishment of the "Critical Manufacturing" Sector as a Critical Infrastructure/Key Resource (CIKR) Sector, March 3, 2008).

5 SURVIAC TAT 04–17, *Improving Situational Awareness of Critical Infrastructure Through Application of Hurricane Katrina Lessons Learned*, July 2006.

6 The DHS National Operations Center (NOC) maintains a COP on the Homeland Security Information Network (HSIN).

7 DHS. Federal Emergency Management Agency (FEMA) 501, National Incident Management System, 1 March 2004, p. 13.

8 For the purposes of this article, focus is on domestic catastrophic events; thus, all references are to USNORTHCOM. Certainly other combatant commands (COCOMS), departments, and agencies within DOD have important CI/KR concerns as well.

9 Bush, George W. *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*, February 2003.

10 National Governors Association (NGA) Center for Best Practices. *2007 State Homeland Security Directors Survey*, 18 December 2007.

11 All Hazards Consortium. http://www.ahcusa.org/whoIs.htm.

12 DHS. *Joint Field Office Activation and Operations: Interagency Integrated Standard Operating Procedure*, 28 April 28 2006, p. 19.

13 With few exceptions, requests for Defense Support of Civil Authorities (DSCA) originating at the Joint Field Office (JFO) are coordinated with and processed through the Defense Coordinating Officer (DCO). The DCO may have a Defense Coordinating Element (DCE), consisting of a staff and military liaison officers to facilitate coordination and support to activated Emergency Support Functions (ESFs). DHS, *National Response Framework*, January 2008, p. 68.

14 DHS. *Office of Infrastructure Protection Strategic Plan: FY 2008–2013*, August 2007, p. 14.

15 DOD. *Defense Industrial Base: Critical Infrastructure and Key Resources Sector-Specific Plan as Input to the National Infrastructure Protection Plan*, May 2007, p. 5.

16 DCMA is in the process of developing such a response capability with the National Guard.

17 Information Assurance Technology Analysis Center. *Defense Critical Infrastructure Program Monitoring and Reporting Project*, November 2006.

18 A formal reporting system from DOD DCIP does exist whereby DOD provides the NICC with DIB reporting during incidents of national significance.

USSOCOM Tiger Team Studies Battlefield Biometrics Technology

By Mr. Craig Archer and Major Charles Seifert, USA, US Special Operations Command

BOOM! A breaching charge explodes; Special Operations Forces (SOF) enter the enemy's domain. Bullets, dust, noise. Voices are heard shouting commands in the darkness of the night; the enemy has been overcome by SOF and Coalition forces.

Unfortunately, the targeted individual of this operation is not there. Some combatants have been killed in action. Ten living individuals remain. They are confused, scared, and do not answer questions. SOF has space on the helicopter for only five people. Who should be detained? Who should be left behind?

The team leader quickly directs sensitive site exploitation (SSE) to commence. The intelligence sergeant collects biometrics on the living and the dead. Seven minutes later, the US Special Operations Command (USSOCOM) Interagency Task Force Biometric Portal returns a response indicating one of the captured individuals is on the Terrorist Watch List. This individual is the leader of a kidnapping and execution cell with ties to al Qaeda in Iraq. He and four other High Value Individuals are removed from the target. Mission accomplished on a day when it was better to be lucky than good. Was it really luck—or the result of superior leadership, training, and equipment?

USSOCOM built a capability in fall 2006 to leverage biometrics as a combat enabler. Under the guidance of J-24 (the requirements and acquisition cell for USSOCOM's Intelligence Directorate) and the USSOCOM Interagency Task Force, a biometrics architecture was built to meet SOF's requirement for rapid hostile-force positive identification and hold/release decision data. This task required match reporting, dossier building, the fielding of biometric collection kits to create an identification match report on an objective, and a SOF biometrics training program. J-24 staff faced a tremendous task when they were asked to document these requirements. They put together a team of operators from the components and staff in USSOCOM to work the issue. They put their collective thoughts and requirements into the Special Operations Identity Dominance (SOID) and Capabilities Development Document (CDD).

Biometrics are measurable physiological and behavioral characteristics that can be used to verify a person's identity. Currently, these characteristics include fingerprints, iris scans, facial photos, and DNA samples.

As of December 14, 2007, the SOF Biometrics Portal has received 14,125 records and matched 2,828 individuals, representing a 20 percent match rate. The portal has been utilized to match individuals from OEF, OIF, US Central Command (CENTCOM), US Southern Command (SOUTHCOM), US European

Command (EUCOM), and US Northern Command (NORTHCOM). It has provided worldwide personal identification capability in times as fast as 7 minutes and 19 seconds. SOF operators have captured 92 High Intelligence Value personnel and 17 National Ground Intelligence Center (NGIC) Watch List enemy combatants utilizing the SOF Biometric Portal.

In order to continue improving this effort, a Tiger Team from USSOCOM's Antiterrorism and Force Protection Branch and the USSOCOM Interagency Task Force traveled to Afghanistan and Iraq in fall 2007. The mission was to assess the use of biometrics and nonlethal weapons by SOF. The team, led by Col Paul Burke, USMC, included Maj Rich Munsey, USA, Maj Tom Follmer, USA, LCDR Dan O'Shea, USN, Master Sgt John Nettles, USA, and Mr. Craig Archer.

According to the DOD Biometrics Fusion Center (BFC), biometrics are measurable physiological and behavioral characteristics that can be used to verify a person's identity. Currently, these characteristics include fingerprints, iris scans, facial photos, and DNA samples. Future potential biometrics may include palm prints, voice, gait, heart rhythm, and even body odor.

SOF and conventional forces use a variety of biometric tools to gather information on captured insurgents. These tools are also used to validate the identities of local nationals seeking employment or training and to authorize or deny access to US bases or installations. Most tools used by SOF revolve around the matching of fingerprints. All SOF records transmitted over the USSOCOM Biometrics Portal are stored and matched against the Automated Biometric Information System at the BFC and are simultaneously matched against the Integrated Automated Fingerprint Identification System at the Federal Bureau of Investigation (FBI). Records are then matched against the National Counterterrorism Center (NCTC) and NGIC Watch List and returned to the operator who submitted the file. This activity happens in a matter of minutes, ensuring that the operator on the ground has identity dominance to assist the decision-making process.

The Tiger Team assessed how SOF and conventional forces are using biometric information on the battlefield, focusing primarily on determining the capabilities required to improve the system. They traveled first to Qatar to brief Maj Gen John Mullholland, USA, Commander of USSOCOM-Central. The Tiger Team then continued to Bagram, Afghanistan, to meet with members of the Combined Joint Special Operations Task Force–Afghanistan (CJSOTF-A). While in Afghanistan, the team conducted and observed live testing of the SOF Biometrics Architecture using the Broadband Global Area Network System. This system, commonly referred to as "SIPR in a Ruck," increased upload speed of biometric data and provided fast replies to submissions for operators on target.

The team also met with Operational Detachments, Operational Detachment BRAVOs, and the CJSOTF-A to discuss equipment and architecture issues important to the Special Forces Soldiers on the ground. Craig Archer, USSOCOM Biometrics expert, was able to solve many of the equipment, software, and interagency issues experienced on the ground. Soldiers clearly identified the need for field support representatives and training enhancements that will be incorporated into permission training and other institutional training events.

The Tiger Team assessed how SOF and conventional forces are using biometric information on the battlefield, focusing primarily on determining the capabilities required to improve the system.

In a parallel effort that may meet these needs, USSOCOM established a Biometrics Analysis and Coordination Cell (BACC). This cell, activated in October 2007, supports operators and staff on the ground with advanced analysis seven days a week. The cell is fielded on a test basis for 120 days to develop Human Terrain Mapping, Link Analysis, Rapid Biometric Identification Analysis Report dissemination, and any other analysis needs to support SOF missions with the "so what" after positive identification of individuals on the battlefield.

The Tiger Team identified command emphasis as the key to biometric success. Leadership at the command level in CJSOTF-A stressed the importance of biometric collection. Some required reporting on a daily basis through the situation report (SITREP). This emphasis on the tracking and leveraging of biometrics collected against detainees led to an effective tool to energize identity documentation and tracking. Success and failure of this program clearly rests on the commander and his staff.

The teams also met with COL Samuel Dudkiewicz, USA, Combined Joint Task Force-82 Biometrics Manager, to discuss the practical application and integration of biometrics equipment and software in the biometrics community. In addition, the Tiger Team met with Combined Explosives Exploitation (CEXE)

Members from the SOCOM Biometric Tiger Team met with CJSOTF-A team members to observe a demonstration of the BGANS (Broadband Global Area Network System). BGANS is being used in Afghanistan to quickly transmit and receive biometric data and information.

cells and the FBI in both Kandahar, Afghanistan, and Bagram. CEXE cells are staffed to process latent prints on improvised explosive devices (IEDs); however, the current level of staffing limits their ability to fully support biometric prosecution of data associated with other terrorist activities.

Because of this gap in exploitation requirements, CJSOTF-A has built an SSE cell in Kandahar. This cell is integrating with interagency partners to develop an internal capability to process biometrics, latent prints, physical evidence, digital media exploitation, explosive residue testing, chemical analysis, and other technical skill sets. The cell is staffed with an Air Force scientist and is augmented with various disciplines (e.g., biology, forensics) that are pertinent to SSE collection, with the primary support afforded by the Chemical Detachment personnel of the Group Support Company. The SSE cell is a hybrid organization formed through interagency collaboration and is another example of the need to process information to obtain identity dominance on the battlefield. Lessons learned from this cell were brought to USSOCOM J-24 and submitted to the SOID requirements manager.

The Tiger Team identified command emphasis as the key to biometric success.

In Iraq, the team discussed biometrics with COL Kenneth Tovo, USA, commander of the CJSOTF in Iraq. COL Tovo's command emphasis has been critical to the success of biometric use by SOF. Forces in Iraq are both gathering more data and using this data to identify known insurgents and terrorists. Eleven NCTC and NGIC Watch List "TIER I" terrorists were identified and captured by SOF during this last rotation in Iraq through the use of biometrics. Many of the successes in Iraq have included the capture of insurgents who are attempting to receive SOF training disguised as Iraqi soldiers. The Biometric Portal has proven to be a successful force protection weapon providing identity dominance in the Global War on Terror (GWOT).

The team also met with the program manager forward for biometrics, COL Natalie Jacaruso, USA, and the MNCI biometrics lead, CDR Jon Lazar. The team solved some outstanding issues regarding data sharing and system cross-talk between SOF and conventional forces. The Biometric Automated Toolset (BAT) system has been provided with all of SOF's biometric records for inclusion in local databases. Although there are still issues and problems to overcome, a concerted effort is being made among the various commands and agencies to resolve the problems. Multiple biometric collection tools are currently being used in theater by different agencies and international organizations. The Tiger Team's observations of these systems reinforced the need for USSOCOM to match all records against the DOD-recognized national database directed for biometric storage at the BFC. Currently, USSOCOM is the only DOD entity to check all records against the Department's Automated Biometric Identification System (ABIS) and FBI databases. This synergy allows our operators to match against combined interagency knowledge versus a local isolated database.

The USSOCOM team returned with more than 30 lessons learned and inroads to collection sources not previously available to SOF. These lessons and improvements recommended by operators and staff are currently being disseminated across the command. Some have already been implemented (e.g., BACC), while others will take longer to enact. SOF operators on the ground familiar with the program are convinced of the validity and utility of battlefield biometrics. A 10th Special Forces Group (Airborne) Soldier commented, "I believe USSOCOM should send a biometrics team twice a year," when discussing lessons learned and experiences from the Soldier's perspective on biometric operations. The challenge now is to maintain the momentum, spread the word, solve the inevitable equipment and software issues, and build on the successes already realized.

Col Paul Burke and MAJ Tom Follmer contributed to this report.

Special Event Antiterrorism Risk Assessments: Leveraging Doctrine

By Pete Huller, Installation ATO, US Army Garrison, Presidio of Monterey, California

Author's note: I have created a restricted community on the AT Enterprise Portal, POM Community, which contains the risk assessment worksheet discussed in this article and many more AT-related documents. DOD personnel working in the AT arena are welcome to join.

Managing risk can be a lot like scripting a training exercise: You try to anticipate all of the potential issues and Murphy's Law, but in the end, you have to accept the fact that you will not be able to cover all the bases. Therefore, it is a good idea to develop a comprehensive method of addressing as many variables and situations as possible. Any event has a certain measurable level of risk because the possibility always exists that something may go awry, or that some aspect of planning did not cover an unforeseen event. The trick with risk management is to assess the potential problem areas based on the current threat and its likelihood, and to develop controls to mitigate the risk to an acceptable level. Put another way, the goal of risk management is to quantify the risk to the extent possible to more successfully and appropriately identify the measures, procedures, or controls required to mitigate the risk to a level the commander can accept. Army Risk Management Doctrine provides an excellent framework for the Antiterrorism Officer (ATO) to implement when assessing risk for special events like ceremonies, graduations, or parades.

Commanders at all levels must determine the level of risk they are willing to accept. In terms of the terrorist threat to a special event, commanders need to base that decision largely on the ATO's sound analysis of the situation. FM 100–14, Risk Management, identifies the subject as "the process of identifying, assessing, and controlling risks arising from operational factors and making decisions that balance risk costs with mission benefits." To accomplish this process accurately, one must address a wide variety of factors and planning considerations. Special events occur on every military installation and are accompanied by an inherent level of risk. The ATO must provide the commander with an assessment based on a detailed analysis of risk factors and planning considerations along with recommended controls to mitigate risk when and where necessary. At the same time, FM 100–14, Risk Management, states: "Using a standardized risk assessment card or checklist may be of some value initially in the mission analysis and Course of Action (COA) development or in cases where a routine task is performed in an unchanging environment or static situation. However, such a tool used alone will not likely identify all hazards for every mission in a changing operational environment."

The Presidio of Monterey's AT Office, with input from other Installation Management Command ATOs such as Fort Carson's, developed an AT risk assessment planning worksheet loosely based on the Army's Risk Management Process. When applied in conjunction with doctrinal risk management guidance and matrices, this document provides an ATO with the ability to effectively assess potential risks across a broad spectrum and to advise the commander on the acceptable level of risk for a given event. Naturally,

all installations, events, and threat environments are different, but with a holistic approach to managing risk, an ATO can successfully provide the commander with a sound risk assessment.

According to FM 100–14, "Risk is characterized by both the probability and severity of a potential loss that may result from hazards due to the presence of an enemy, an adversary, or some other hazardous condition. Perception of risk varies from person to person." Although this statement is true, it is important to also view risk in terms of the enemy's perspective; or as we used to describe it during the Cold War era, "Think Red." The type of event, the attendees, the venue, the media attention, and other factors will influence the value of a target in the mind of the enemy. Not all targets are created equal, at least not in the minds of our adversaries. Some will further the enemy's goals and achieve their objectives, which is why it is so critical that the ATO knows the current threat for the given environment.

A good AT program ensures that all personnel affiliated with the installation, whether they live and work on the installation or in its vicinity, are aware of their role as sensors. Local law enforcement and intelligence agencies are not resourced to see and hear everything of a potentially threatening nature to a military installation; therefore, all stakeholders must embrace their role of being sensitive to suspicious activities and reporting them in a timely manner and in sufficient detail.

The first and most important step in initiating any AT risk assessment is identifying hazards. In terms of AT, the terrorist threat is the critical focus. Make no mistake: Identifying potential threats is no easy task. The ATO applies a variation of Intelligence Preparation of the Battlefield; however, there is no matrix or formula to use and usually there is no way to be sure that the assessment of the threat is 100 percent accurate. Coordination with intelligence and law enforcement agencies provides the ATO with necessary terrorist threat information; however, the perceived absence of a threat does not necessarily constitute the lack of a threat. History has shown, as in the case of the 1994 bombing of the Murrah Federal Building in Oklahoma City, that terrorists do not cooperate with threat assessments. This unpredictability is why it is so critical to understand the threat to the extent possible in order to determine whether it is advisable to hold the special event.

Threat is assessed based on four specific factors: Operational Capability, Intentions, Activity, and Operating Environment. National-level intelligence agencies have assessed that terrorist groups are already operating in the United States. That being said, we must understand the operational capability of a particular group to carry out an attack. For example, a group like Hamas may be quite able to attack a military formation with sniper fire; however, their ability to attack with weapons of mass destruction is significantly lower and therefore less likely.

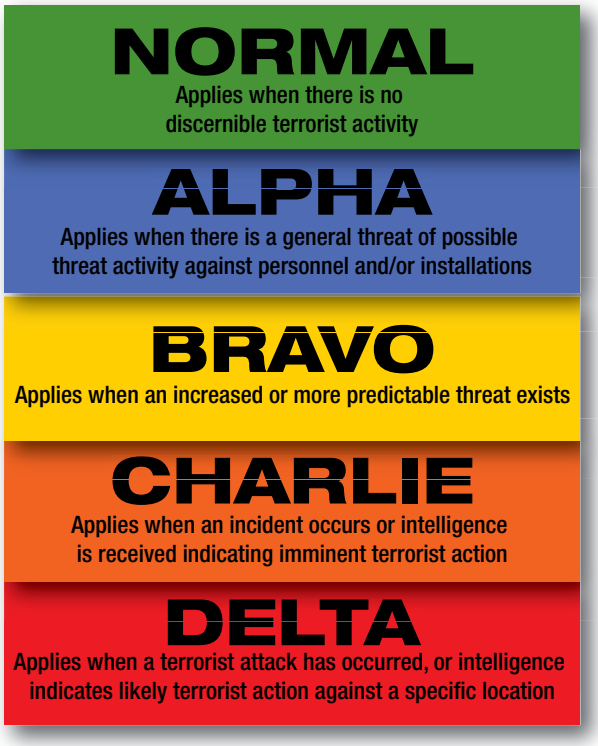
A second important consideration in assessing threat is whether there has been a stated intention to attack. On May 22, 1998, Osama bin Laden stated: "Killing Americans and their Allies, civilian and military, is an individual duty for every Muslim…We do not differentiate between those dressed in uniforms and civilians." In this statement, he clearly outlined the intention of al Qaeda to attack military (and civilian) personnel.

A good AT program ensures that all personnel affiliated with the installation, whether they live and work on the installation or in its vicinity, are aware of their role as sensors. Local law enforcement and intelligence agencies are not resourced to see and hear everything of a potentially threatening nature to a military installation; therefore, all stakeholders must embrace their role of being sensitive to suspicious activities and reporting them in a timely manner and in sufficient detail. The return on this investment is visibility on possible enemy activity, the third factor used to assess threat. Reports of surveillance, elicitation, and other indications of terrorist activity enable intelligence organizations to assess the presence and actions of terrorist organizations properly.

Lastly, one must establish the overall effect of the operating environment on a terrorist group's activities. Does the environment favor the enemy? Does the enemy have freedom of movement in the operating area? Will the local populace recognize suspicious activities and report them? Will the local populace be a source of support—material, political, or social—for the enemy? The answers to these questions will assist the analyst in determining the impact of the operating environment on enemy or terrorist operations.

The ATO is typically neither trained nor resourced to conduct in-depth threat analysis as described above. He or she must rely on local and state police, regional threat analysis centers, and defense and national intelligence agencies for threat assessment. This information is not always a mouse-click away, which means that the ATO must work to establish relationships with his or her counterparts and the aforementioned organizations. These liaison efforts are crucial to the success of an ATO in understanding the threat in his or her area.

The Force Protection Condition (FPCON) system also assists the ATO. Major commands set the FPCON for their subordinate elements based on the established threat level. When the FPCON is



FPCON System

Major commands set the FPCON for their subordinate elements based on the established threat level. When the FPCON is elevated to BRAVO or higher, ATOs must implement prescribed measures that may limit or prohibit large gatherings, especially outdoors; however, when the FPCON is at ALPHA, the ATO's job is actually more complex because the constraints are fewer and the threat is of a much more unpredictable nature.

elevated to BRAVO or higher, ATOs must implement prescribed measures that may limit or prohibit large gatherings, especially outdoors; however, when the FPCON is at ALPHA, the ATO's job is actually more complex because the constraints are fewer and the threat is of a much more unpredictable nature. This reality supports the need for a solid installation AT awareness program, as well as for focused liaison efforts.

The process does not end with identifying the local threat. Just as in a conventional military operation where the commander's staff assesses hazards based on Mission, Enemy, Terrain (and Weather), Time–Troops, Civilians (METT-TC), the ATO implements the risk management process in the context of AT focusing on the same dynamics. The ATO must classify the threat through the prism of the type of special event (e.g., change of command ceremony), where it is to be held (e.g., post parade field), who will attend (e.g., general officers and other VIPs), and other considerations. The probability of a terrorist event may be linked to these variables, assuming the presence of such an enemy in the area of operations.

In an increased threat scenario, commanders must decide whether the risk outweighs the expected benefit of holding the special event. In any operation, some degree of risk always exists; however, the objective of managing risk is not to remove all risk, but rather to eliminate unnecessary risk and mitigate whatever acceptable risk remains. Again, the ATO's job is to present the commander with the maximum amount of data available to make an informed decision on assuming risk and the means to mitigate it.

Controls are the means of mitigating assessed risk. First and foremost, controls need to be achievable and coordinated. Much of this need may be standard operating procedure and may be virtually locked in because of the repetitive nature of certain special events. At the same time, the ATO and the Director of Emergency Services must synchronize the necessary protective measures to minimize potential vulnerabilities. These measures may well be part of the installation's AT plan or may be specific to special events. That said, the ATO must coordinate the plan to ensure that all stakeholders know their roles. It is easy to say, "Sweep the area two hours prior," but if the organization designated to perform this mission is not tasked in advance and is not aware of the specific requirements, then the mission is set up for failure. Controls must also suit the particular event, the vulnerability, and the environment.

Feasibility is another aspect of ensuring controls will be effective. One must assess the ability of organizational assets to implement the intended control measure or to coordinate with outside agencies. For example, an effective means of ensuring a particular building is clear is to employ military working dogs; however, many installations do not possess this capability. Advance coordination is required to ensure this control is implemented at the time and place required.

The ATO has to review all types of threats and determine probability in order to make reliable mitigation recommendations. The probability of a threat scenario must then be compared with the

severity of such an incident to determine vulnerability. As the Initial Risk Level Matrix (see Appendix) shows, an extremely high level of risk could exist if the probability and severity are significant enough. Conversely, a scenario in which the probability is unlikely and the severity is negligible poses minimal vulnerability for the event and therefore enables the commander to assume minimal risk.

It is possible that there could be a rocket attack against an installation; however, the probability in a given situation or time frame may render the probability of such an attack extremely low due to a number of factors (e.g., lack of enemy capability). With low probability, this particular threat will likely not receive as much attention as another scenario such as a person attacking a formation with an automatic weapon, which local, state, and federal agencies may deem more probable based on available information. If the special event is a building dedication, the ATO almost has to reverse the normal protection paradigm of "outside-in." Thinking Red again, the ATO must imagine that a terrorist will pin his attack on the likelihood of the target being in a certain place at a certain time. In this case, the planning for controls must be suitable to the situation and begin at ground zero; that is, the event location. Going back to the building dedication scenario, it makes sense that a critical task would be to sweep the building prior to the event. Alternatively, if the event is an open-air change-of-command ceremony, a bomb sweep might be less suitable because of the lack of concealment on-site. (Of course, this scenario presupposes that security personnel have limited potential concealment locations at the parade field.) The point is that recommended controls must be appropriate for the event as well as for the location and must be wargamed well in advance.

The commander must review all of the planning efforts and proposed controls and decide whether they are sufficient in terms of the risk he or she is willing to accept. Naturally, other considerations intervene such as effects on operations, resources, and convenience. (Many ATOs reluctantly accept the fact that we must assess the element of convenience in implementing mitigation measures.) It is very easy to direct the closure of all Access Control Points and thereby greatly reduce or eliminate the threat of a vehicle-borne improvised explosive device, but the commander must recognize the repercussions of implementing this type of control measure and assess the suitability, as discussed above.

A critical element of the planning process that we have ignored thus far includes coordinating with civilian law enforcement and first responder agencies in advance of the event. The DOD is required to follow the tenets of the National Incident Management System (NIMS); as a result, many military installations nowadays are heavily reliant on civilian counterparts to respond to crisis situations. Your civilian counterparts must be apprised of special events occurring on the installation because they may incur an above-average risk to the local community. As such, the ATO must provide prior notice so that these agencies are aware of the potential for involvement in an emergency on the local military installation. An implied task here is to conduct training exercises in which the DOD and local agencies are well-versed in their respective roles in the Incident Command System (ICS). As always, prior planning will go a long way toward averting poor performance, and we all know that hope is not a course of action.

Once the threat is identified, controls are addressed, and all seems in order, the commander must focus on residual risk; that is, the risk that remains once control measures are implemented. Again, the goal is to manage risk to an acceptable level because it is virtually impossible to eliminate all risk. It is in this stage that prior planning becomes significant because the installation's Terrorist Threat Incident Response Plan will dictate measures to take in the event that the residual risk becomes a reality.

Although the main thrust of special event risk assessments focuses on force protection and protection of DOD assets, the commander must also consider the collateral effects of a terrorist attack during a special event, especially the risk to personnel. For example, terrorists may target a certain demographic of the installation, resulting in many of those people being killed or injured. A second-order effect might be that those who were targeted might be extremely hard to replace, thus resulting in a third-order effect—namely, mission degradation.

We must accept certain incontrovertible truths, and one of those is that there will always be a certain element of risk in any military operation, including mundane events like training school graduations. Nevertheless, a basic tenet of our training holds that "Commanders are responsible and accountable for their own actions and those of units under their charge." Those of us who support our commanders must ensure that we execute the due diligence to enable that commander to identify risks and execute controls to mitigate risks to an acceptable level. We can only do so via a thorough planning process that addresses the threat and associated contingencies. Documenting this process provides leaders at all levels with the visibility to know what measures have been taken, what actions have been coordinated and by whom, and ultimately, that we have done all within our capability to protect our most precious resource: our DOD Service members and civilians.

Appendix

U.S. Army Garrison
Presidio of Monterey

Special Event Antiterrorism Risk Assessment Packet

Presidio of Monterey and Ord Military Community

ANTITERRORISM RISK ASSESSMENT
PLANNING WORKSHEET

EVENT NAME: _____

EVENT LOCATION: _____

DATE(S) and TIME OF EVENT Starts: _____ **Ends:** _____

ESTIMATED NUMBER OF ATTENDEES / PARTICIPANTS: _____

TERRORIST THREAT ASSESSMENT:

1. THREAT (Circle one)	Low	Medium	High	
2. SYMBOLIC VALUE (Circle what applies)	Historical	Political	Military	
3. FPCON (Circle one)	ALPHA	BRAVO	CHARLIE	DELTA

(**Note**: At FPCON BRAVO and higher, review standoff requirements and use of Military Working Dogs (MWD). If MWD is required, coordinate with DES at least 3 weeks prior. If an MWD dog team is not available, the unit or agency will coordinate with the building/facility manager and DES to conduct a bomb sweep. Once bomb sweep is complete, access into the area must be restricted—including deliveries to the facility or building.)

ADDITIONAL CONSIDERATIONS:

MEDIA ATTENTION: PAO (Circle one)	Advertised	On-post	Off-post	On-post and off-post
PUBLIC INVITED: (Circle one)	YES	NO		
EVENT VISIBILITY: (Circle one)	Day	Night	Both	

Emergency Lighting Note: Request from DES if needed.
KEY TERRAIN: _____
(Areas that may provide an enemy control of a situation)
OBSTACLES/CONCEALMENT: Present? If so, type: _____
VENDORS: Planned for the event? If so, ensure names and vehicle information are provided at least 2 weeks in advance to DES.

AT POC: Pete Huller, (831) 242-7027, peter.huller@us.army.mil, or Ernest Schmidt, (831) 242-7884, ernest.schmidt@us.army.mil

Presidio of Monterey and Ord Military Community

ANTITERRORISM RISK ASSESSMENT
PLANNING WORKSHEET (Cont'd)

VISITOR / HRP or VIP COORDINATION

ADDITIONAL SECURITY: Will Personal Security Detail (PSD) accompany the HRP or VIP? (Check one below)

Yes, POM PD should coordinate with them **No, POM PD should coordinate security with CID**

VEHICLE PASS REQUIRED? If so, coordinate with DES.

VIP PARKING:

• If the event includes VIP parking and the FPCON is BRAVO or higher or there is a specific threat to the event or against a specific VIP/HRP, then protocol should provide VIP parking passes for the event.

•SECURITY SWEEPS: Date/Time conducted _____ POC _____

If standoff is required, explain how it is enforced:_____
_____

POTENTIAL FOR DOMESTIC DISTURBANCE: Demonstrations (Circle One) **Yes** **No**

Est. Size of Demonstration (Circle One) **Small < 50** **Medium > 50** **Large > 100**

COORDINATION FOR OFFSITE OR OFF-POST EVENTS:
Criminal Threat Assessment: Yes No
Date Completed:_____ **POC**_____

Presidio of Monterey/Ord Military Community

PLANNED PRIMARY GATHERING—SECURITY DECISION MATRIX

Category 1 FPCON	Category 2 # People at Event	Category 3 HRP (1 or 2) Attending	Category 4 Media Attention
Normal & ALPHA	100 or fewer *	Yes	Off-Post Event and/or Advertised Off-Post and/or Public Invited to POM/ OMC
BRAVO	75 or fewer	Yes	Off-Post Event and/or Advertised Off-Post and/or Public Invited to POM/ OMC
CHARLIE	50 or fewer	N/A	N/A
DELTA	N/A	Cancel Event	N/A

ALPHA = Categories 1 through 4 must all be considered. If all criteria are met or exceeded, security must be coordinated for the event.*

BRAVO = Criteria in Categories 1 through 4 must all be considered. If all criteria are met or exceeded, security must be coordinated for the event.*

CHARLIE = HRP attendance and media attention (Categories 3 and 4 above) to the event is immaterial. Criteria in Categories 1 and 2 must be considered. If met or exceeded, security must be coordinated for the event.*

DELTA = All special events are canceled. HRP movement is guarded.*

* Special Note: At any FPCON, commanders may decide to implement specific measures regardless of above criteria. The threat will be considered for all events. Specific threats may require higher security measures at lower FPCONs. The Antiterrorism Office is available to review event security plans.

Appendix

AT Risk Criteria Matrix

1. UNIT/EVENT/ACTIVITY: _____ 2. DTG BEGIN: _____ 3. DATE PREPARED:
Event Name END:

	Extremely High	High	Moderate	Low
Terrorist Threat Level (Coord. w/ S-2)	High	Significant	Moderate	Low
Criminal Threat Level	Critical	High	Medium	Low
Geo Specific Warning (Coord. w/ S-2)	Yes	-	-	No
World Travel Warning (Coord. w/ S-2)	-	-	-	No
Size of Force / Group / Event	Greater than 1000	Greater than 500 but fewer than 1000	Greater than 300 but fewer than 500	300 or fewer
Visibility of Target / Event	U.S. Signature International Media Coverage	U.S. Signature National Media Coverage	U.S. Signature Regional/Local Media Coverage	No U.S. Signature No Media Coverage
Significance of Target / Event	U.S. President	HRP 1 & 2 or (=) Civilian	General Officer in attendance	No General Officer in attendance
Duration of Event	Longer than 3 weeks	Longer than 1 week but shorter than 3 weeks	Longer than 3 days but shorter than 1 week	Shorter than 3 days
Location of Target / Event	Event in another country	Event off post or attendees billeted off post	Event on installation or attendees billeted off post	On secured installation or attendees billeted on post
AT/FP Plan Addresses Target / Event	No security measures countermeasures can be implemented	Security responsibility not determined	AT/FP Plan partially addresses event	AT/FP Plan addresses event
Vulnerabilities Identified	Inadequate compensation measures	Significant vulnerabilities without adequate compensation measures	Some vulnerabilities cannot be mitigated	Acceptable level of vulnerabilities

Severity Interpretation

Severity of Consequence					
Category/ Descriptive Words	Personnel Illness/ Injuries	Number of Personnel Casualties	Building Damage/ Equipment Loss ($)	Social/ Psychological Impact	Recoverability
I Catastrophic	Death or Severe Injuries	> 10	> $1M	High	> 180 days
II Critical	Death or Severe Injuries	< 10	$250K to $1M	Significant	> 90 days
III Marginal	Severe or Minor Injuries	> 10	$1K to $250K	Moderate	< 30 days
IV Negligible	No Injuries or Minor Injuries	< 10	$1K	Low	< 1 week

Initial Risk Level Matrix

PROBABILITY

SEVERITY	FREQUENT	LIKELY	OCCASIONAL	SELDOM	UNLIKELY
Catastrophic	E	E	H	H	M
Critical	E	H	H	M	L
Marginal	H	M	M	L	L
Negligible	M	L	L	L	L

PROBABILITY

FREQUENT: Occurs often, continuously experienced.
LIKELY: Occurs several times.
OCCASIONAL: Occurs sporadically.
SELDOM: Unlikely, but could occur at some time.
UNLIKELY: Can assume it will not occur.

SEVERITY

CATASTROPHIC: Death of 10 or more personnel, system loss, major damage, significant property damage of over $1M, mission failure.
CRITICAL: Death or severe injuries of less than 10 personnel, major system damage, significant property damage of $250K to $1M, significant mission degradation.
MARGINAL: Severe and minor injuries, minor system damage, property damage up to $250K, some mission degradation.
NEGLIGIBLE: First aid or minor medical treatment, minor system impairment, property damage of less than $1K, little or no impact on mission accomplishment.

RISK LEVELS (See Risk Level Matrix)

EXTREMELY HIGH (E): Significant terrorist target if vulnerabilities are not mitigated.
HIGH (H): High probable terrorist target if vulnerabilities are not mitigated.
MODERATE (M): Possible terrorist target if no additional security measures implemented.
LOW (L): Execute event or mission with standard security measures.

Antiterrorism Risk Assessment

RISK ASSESSMENT WORKSHEET

1. UNIT/EVENT/ACTIVITY:	2. DTG BEGIN: END:	3. DATE PREPARED:
4. PREPARED BY:		

5. IDENTIFIED VULNERABILITIES	6. INITIAL RISK LEVEL	7. RECOMMENDED MEASURES	8. RESIDUAL RISK LEVEL	9. WHO IMPLEMENTS	10. WHO SUPERVISES	11. RESIDUAL ACCEPTED RISK

12. OVERALL RISK LEVEL AFTER MEASURES ARE IMPLEMENTED (Circle one): LOW MODERATE HIGH EXTREMELY HIGH	13. ACCEPTED RISK DECISION AUTHORITY SIGNATURE: (Rank/Last Name, First I, Duty Position)
REMARKS:	

SMADS: Strategic Mission Assurance Data System

By LTC Pat Briley, Joint Staff

Department of Defense Directive (DODD) 3020.40, signed on 19 August 2005, changed the Critical Asset Assurance Program to the Defense Critical Infrastructure Program (DCIP). Since that time, DOD and all of its subordinate organizations have been coming on board and meeting the responsibilities outlined in this directive. One of the tasks given to the Office of the Assistant Secretary of Defense for Homeland Defense and America's Security Affairs (OASD (HD&ASA)) was to develop and implement DCIP Enterprise Architecture (EA) to ensure a net-centric approach to promote DCIP interoperability of information systems and processes.

Background

Like most geospatial systems, the Strategic Mission Assurance Data System (SMADS) evolved from a Microsoft Word document to an Excel spreadsheet to an Access database that was then geospatially enabled via ESRI ArcView. The database was converted from Access to Oracle, and the ArcView has been upgraded to ArcGIS 9.2. SMADS was initially developed in early 2003 at the request of the US Strategic Command (USSTRATCOM) Commander, ADM James O. Ellis, Jr. He wanted to know where all of his critical systems, assets, and infrastructure were located, and the new tool was first used operationally after a major power outage in 2003. This initiative aimed at providing fully integrated Web capabilities to quickly and accurately characterize and assess threats, hazards, and consequences of a full spectrum of global events. This effort not only attempted to meet minimal policy directives but was designed to provide relevant information that answers the following questions: What happened? What was affected? How can I continue to operate? SMADS was not designed to be a tool used only by experts; instead, it was designed with simplicity in mind so that anyone can perform some level of mission impact analysis with minimal training. Furthermore, it is designed to give senior leadership, both civilian and military, a five-minute response to a request for information (RFI).

SMADS is located on the Secret Internet Protocol Router Network (SIPRNET) and is a Web-based data repository located in Omaha, Nebraska, with a replica server soon to be located in an undisclosed location. SMADS users can visualize assets via a mapping capability using ESRI's ArcGIS 9.1, identify assets associated with specific missions and functions, and identify certain threats and hazards. Approved users can edit their data via a Web-based graphic user interface (GUI) to update their data anytime a change in status occurs.

In April 2007, OASD (HD&ASA)'s Critical Infrastructure Protection (CIP) Office and the Joint Staff J-34 made the decision to begin placing Task Critical Assets (TCAs) on SMADS. About a year before, the Joint Staff began soliciting the combatant commands and Services for their Defense Critical Infrastructure (DCI). By the third Joint Staff Action

Package to the combatant commands, the term Defense Critical Infrastructure had been changed to Task Critical Assets because of the rapidly changing DCIP doctrine. At the time, there was still only one approved DCIP document, DODD 3020.40, but there were several coordinating documents, including DOD Instruction (DODI) 3020.nn, the DCIP strategy document, and some white papers on criticality. Some TCAs will eventually become Defense Critical Assets (DCAs), which are assets of such extraordinary importance to DOD operations in peace, crisis, and war that their incapacitation or destruction would have a very serious, debilitating effect on DOD's ability to fulfill its mission. DCAs will not be identified on SMADS because of their higher classification.

SMADS seemed like a logical choice to be the repository for TCAs as the bill for research and development (R&D) had already been paid by USSTRATCOM. The kinks had already been worked out of the system, and it was free for the other combatant commands and Services to use. Even though USSTRATCOM's plate was already full with its ongoing requirements, it still continued to support the entire DCIP community until OASD (HD&ASA) provided funds for additional contractor support in late 2007. SMADS is now available for all of DOD and for some non-DOD organizations to use and is currently the system of choice for USSTRATCOM, the US Joint Forces Command (USJFCOM), the US Navy, the Defense Sector for Space, the Joint Staff, Counterintelligence Field Activity (CIFA), and others. Another asset characterization tool used by the DCIP community is the Critical Asset Management System (CAMS), which is being used by the US Army (USA), the US Air Force (USAF), the US Marine Corps (USMC), and the US Central Command (USCENTCOM). Recently, a Data Exchange Working Group (DEWG), chaired by the Joint Staff and the Mission Assurance Division, Dahlgren, arranged for CAMS and SMADS to "talk" to each other. The DEWG is continuing to work out the IT issues so these two systems, as well as others like the Critical Infrastructure Protection Log (CIPLOG) and the Mission Assurance Tool (MAT), can also communicate through Web services. With all of the improvements and modifications to the data, it is anticipated that more organizations will adopt SMADS as their system of choice because of the cost and ease of use.

The DCIP Geospatial Data Strategy approved in September 2006 requires OASD (HD&ASA) to develop a Web-based, service-oriented DCIP EA in which geospatially referenced databases for each defense sector are linked to an overall DCIP geospatial database and system of record. The strategy also calls for the implementation of a Web-services approach to link the DCIP EA to other geospatial tools and capabilities. The DEWG is tackling these tough problems. As of late March 2008, it appears that the DCIP community will be using Web services for information sharing on the SIPRNET by early 2009. This functionality does not mean that SMADS will go away—quite the contrary. Every organization must have a system with the capability to utilize Web services; in layman's terms, that means each system must talk to the others. For example, when someone at the US Transportation Command (USTRANSCOM) wants to see all of USAF's Tier 1 assets associated with a numbered operational plan (OPLAN), their system pushes out the request via Web services, and in a matter of seconds, that data is displayed in real time.

When the Commander of USSTRATCOM was named the Vice Chairman of the Joint Chiefs of Staff, many people within the Beltway thought that Gen James E. Cartwright would bring a much-needed technology upgrade with him to Washington, DC. As the National Military Command Center can attest, SMADS is now being used 24 hours a day in our watch centers, and the center's personnel have been trained. So far, the US Northern Command (USNORTHCOM) and the US Pacific Command (USPACOM) have undergone SMADS training. (To request in-house training on SMADS, please contact the USSTRATCOM SMADS team.) The J-34 has said that SMADS is an interim fix for the DCIP community. Until Web services are up and running, SMADS must be updated with current data by mission owners and asset owners.

SMADS-DCIP is differentiated from SMADS in that SMADS focuses primarily on USSTRATCOM critical infrastructure and key resources, whereas SMADS-DCIP focuses on TCAs for all combatant commands, Services, Defense Sectors, and even the Department of Homeland Security (DHS). Within this system, users may allow manipulation of data via hypertext transfer protocol (HTTP) through a Web browser such as Internet Explorer or Firefox. Approved users can view all combatant command TCAs as well as the TCAs of Services and Sectors. The DHS Tier 1 and Tier 2 data are also viewable on SMADS. As of March 2008, not all of the Sectors have their data on SMADS; it is anticipated that all combatant commands, Services, Sectors, and DOD Field Agencies will have all of their TCAs on SMADS by June 2008. This system was not designed to take the place of unclassified geospatial systems such as Mission Assurance Division's TRITON, USNORTHCOM's SAGE, the National Geospatial-Intelligence Agency's (NGA's) Palanterra, or even Google Earth. SMADS was designed for users to manipulate and visualize classified data up to the SECRET level on a geospatial platform.

Using SMADS: Setup, Login, and Navigation

Setting Up a SMADS Account

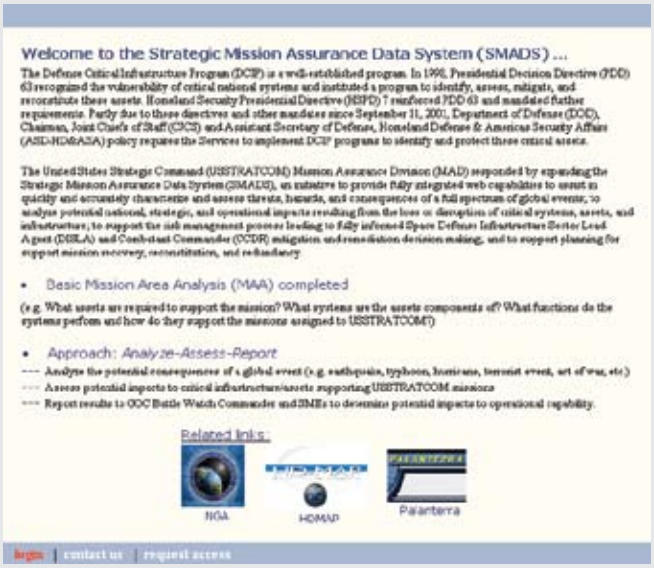


Figure 1. Index Page. This page is UNCLASSIFIED.

To get a SMADS account, go to https://www.stratcom.smil.mil/smads and click "request access" (see Figure 1). From this URL, the user can navigate not only to SMADS but to NGA, to Missions Assurance Division's HD-MAP, and to NGA's Palanterra. Like SMADS, all of these Web sites require user identification (USERID) and a password.

Logging into SMADS

Figure 2. Login Page. This page is UNCLASSIFIED.

Once the user has registered, the login screen will appear (see Figure 2). The UserName is the user's SIPRNET e-mail address, and the password is established during registration.

People within the DCIP community who are listed in the Critical Infrastructure Protection Integration Staff (CIPIS) roster are automatically approved for access once they register online for a SMADS account. Each combatant command lead will be contacted for verification and approval of individual read or edit privileges. Those persons not listed or who are outside of the DCIP community are approved by J-34 or by USSTRATCOM, respectively. A CIPIS roster, called CIPIS POCs, is located on SMADS and is updated quarterly. The OASD (HD&ASA) CIP Office is the proponent for keeping this list current.

Navigating SMADS

Figure 3. Menu Bar. This page is UNCLASSIFIED.

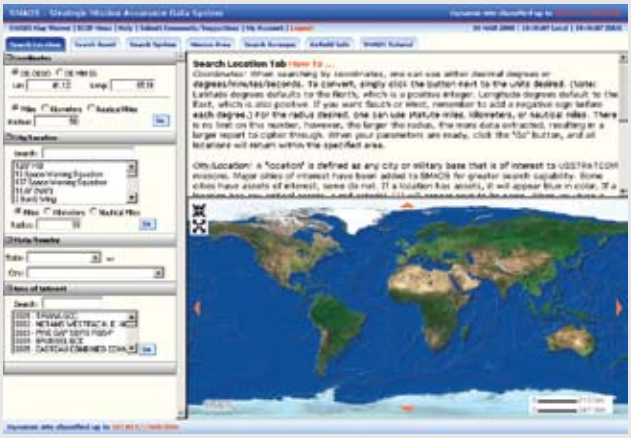


Figure 4. SMADS Search Page. This page is UNCLASSIFIED.

Once the user logs in, the main screen appears. Use the SMADS menu bar (see Figure 3) to navigate the following options: SMADS Map Viewer, DCIP Menu, Help, Submit Comments/Suggestions, My Account, and Logout. The SMADS Map Viewer is primarily for USSTRATCOM users, although other users may find this tab useful. The DCIP Menu consists of the DCIP Map Viewer, View/Edit Assets, View/Change History, View Users, DCIP User Manual, and DCIP Glossy. The Submit Comments/Suggestions section on SMADS is very useful: Whenever a user has a question that does not warrant an immediate response or a suggestion for improvement, filling out the comment section is the method to communicate with the SMADS developers at USSTRATCOM.

Using SMADS: DCIP Menu

The Help Menu is accessible from the SMADS homepage and consists of Release Notes, SMADS User Manual, Contacts, and the CIP Portal. Release Notes update users on changes within the SMADS and DCIP applications. The user can read or print the SMADS User Manual. The DCIP Glossy provides the user with a SMADS information brochure that can be used as a handout or in presentations. Contacts contain a list of SMADS Administrators to call during duty hours (Central Time Zone). The CIP Portal provides access to the USSTRATCOM CIP SharePoint site.

The capabilities of the DCIP Menu and the DCIP Map Viewer will be explained in detail below. The SMADS User Manual and the DCIP User Manual are kept up to date and can be downloaded as PDF files. Finally, the "logout" button (see Figure 3) can be used to log out of the system, or the user can just click on the X in the top right corner of the window.

Under the DCIP Menu tab (see Figure 3), a list of options is available, including View/Edit Assets, which shows TCAs with supporting information for the combatant commands and the Services. The Defense Sectors and DHS assets will be viewable only from the DCIP Map Viewer.

Figure 5. Read-Only View. This page is UNCLASSIFIED.

Read-Only View. If a user does not have edit capability, then that user is said to have "read-only" permission and will have access to the Read-Only screen (see Figure 5). Sort data by using the scroll-down tools. The first tool is a key word search. The next tool filters by organization; it contains combatant commands, Services, and Defense Sectors. Third is the Filter by Tier tool, which sorts tier levels 1 through 3. The options available with the data include "View" and "Map It." The Extract to Excel button allows the user to download SMADS data onto his or her desktop in an Excel file for further manipulation.

Figure 6. Read/Edit View. This page is UNCLASSIFIED.

Read/Edit View. In the Read/Edit screen shown in Figure 6, the user has edit capability as indicated by the blue Edit button. In addition to Read-only functionality, a user with edit capability can also add a new asset from this tab or modify existing information. The Map It button can help verify latitude and longitude of the submitted asset by showing it on a map.

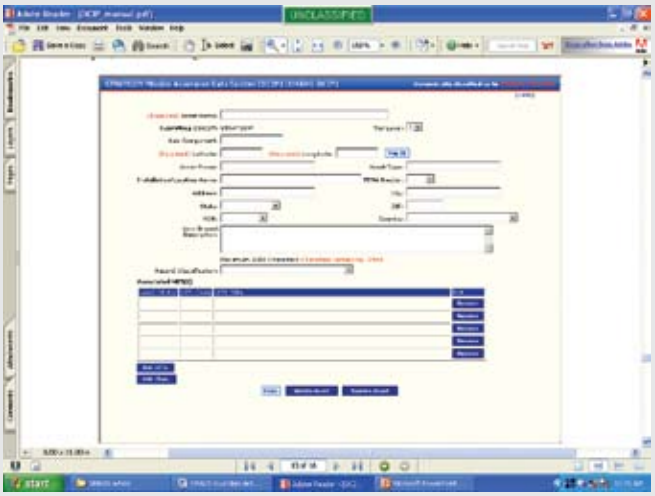


Figure 7. Edit Asset. This Page is UNCLASSIFIED.

When the Read-Only user clicks the View button or the Read/Edit user clicks the Edit button, the Edit Asset screen appears (see Figure 7). This screen displays the supporting data for that particular TCA and shows details such as the Federal Emergency Management Agency (FEMA) region, loss impact description, associated OPLANs to which that asset is linked, and all Joint Mission Essential Tasks (JMETS) that it supports.

Using SMADS: Map Viewer

DCIP Map Viewer

The DCIP Map Viewer on SMADS is shown in Figure 8.

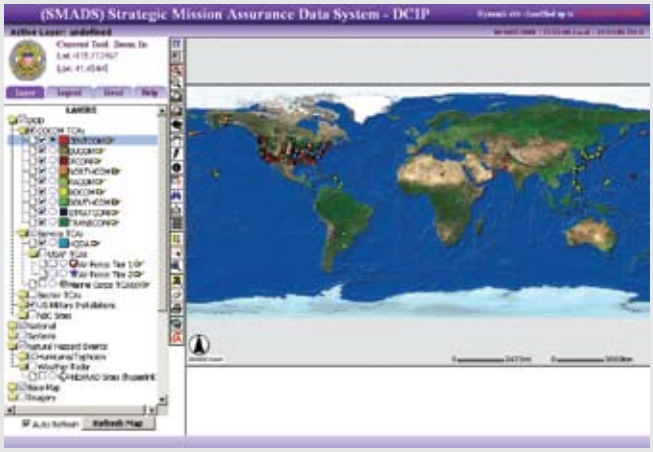


Figure 8. Map View. This page is UNCLASSIFIED.

Layers Tab. Users can view all TCA submissions for all combatant commands, Services, and Defense Sectors on this screen. Recently, the USAF's Tier 1 and 2 assets were broken out so that they could be distinguished on the map. This detail will be added for all Services and combatant commands soon. Most of the Defense Sectors are also listed. DHS's Tier 1 and 2 assets are visible as well as infrastructure such as railways and roads, electrical lines and substations, nuclear plants, and airports. This screen will be upgraded periodically and modified as new data becomes available. The tools in the vertical column between the map and the layers are explained under the Help tab. A one-word description of each tab can be found by hovering over it with the mouse cursor.

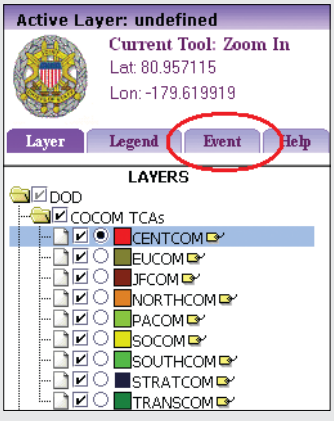


Figure 9. Layers tab. This page is UNCLASSIFIED.

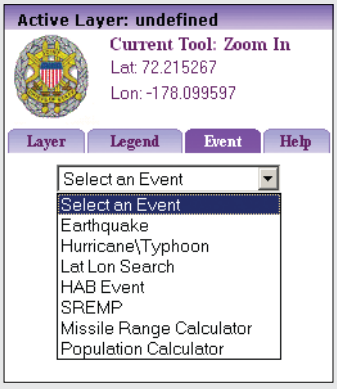


Figure 10. Event tab and drop- down menu. This page is UNCLASSIFIED.

Event Tab. Once the Event Tab is selected, a drop-down box appears and the following options are available: Earthquake, Hurricane/Typhoon, Lat Lon Search, High Altitude Burst (HAB), Source Region Electro-Magnetic Pulse (SREMP), Missile Range Calculator, and Population Calculator. The Lat Lon Search tool will probably be utilized most often when the user performs an operational analysis.

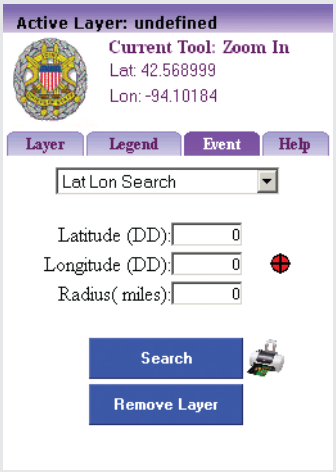


Figure 11. Lat Lon Search. This page is UNCLASSIFIED.

To perform a Lat Lon search, select Lat Lon Search in the drop-down box. Enter the latitude and longitude of the center of the search area by typing it into the appropriate cells or just click the red circle with the crosshairs (see Figure 11) and then click the location on the map to autopopulate the latitude and longitude cells. Enter the desired search radius and then click the Search button. The results will be displayed on the map on the right side of the screen. To view the CIP report for that area, click the printer icon to the right of the blue Search box. This report will include the map and all of the TCAs in that area with all supporting information (e.g., JMETS, OPLANs, combatant command). This report can be saved in a variety of formats, including PowerPoint, Outlook e-mail, and SKIWeb posting, and is extremely useful.

The Earthquake event (see Figure 12) is similar to the Lat Lon Search in that the user must enter latitude and longitude and then the magnitude of the earthquake and a damage level: Probable Moderate to Severe Damage, Probable Light Damage, Barely Felt, or All. Once a damage level is chosen, the map is populated with data. This tool does not take into consideration the type of earthquake or the structure of the bedrock and only gives data in concentric zones.

Once the Hurricane/Typhoon event is selected (see Figure 13), the actual storms that have been characterized by the Naval Meteorological and Oceanographic Center and the Joint Typhoon Warning Center will automatically be listed and updated every two hours. Once a particular storm is selected, the tool will zoom to that location and show the storm's projected path and time.

Using SMADS: Map Viewer

Figure 12. Earthquake Event. This page is UNCLASSIFIED.

The High Altitude Burst (HAB) event requires latitude and longitude and the height of the burst in kilometers. Once the Burst Horizon button is clicked, the map will zoom to show the burst horizon footprint as a transparent overlay. This overlay can be printed by utilizing the printer icon. It will include not only the map but any TCAs in the overlay, similar to the Lat Lon Search. Bear in mind, however, that electromagnetic pulse (EMP) can travel well outside the burst horizon via conducting materials such as power lines, pipelines, and railroads.

The Source Region Electro-Magnetic Pulse (SREMP) event is very similar to the HAB event. After latitude and longitude are entered, the tool asks for yield of the nuclear detonation in kilotons (see Figure 14), either manually or by selecting a weapon type from the drop-down box. Select Extensive Damage Probable, Damage Probable, or Disruption for areas on the map to be viewed. The map will zoom to show the estimated range of effect for the selected EMP levels as red, yellow, or green circles. The user can manipulate the map using the different layers, such as roads, railways, or electric lines, to make the data more useful. Again, the printer icon prepares the map for printing.

Figure 13. Hurricane/Typhoon Event. This page is UNCLASSIFIED.

Figure 14. SREMP Event. This page is UNCLASSIFIED.

The Missile Range Calculator event plots a threat fan based on a missile launched from a hostile location (see Figure 15). The data can be manipulated by the weapon type, range of the weapon, and estimated azimuth. Detailed intelligence in the form of imagery makes this tool extremely useful when planning for the protection of critical infrastructure.

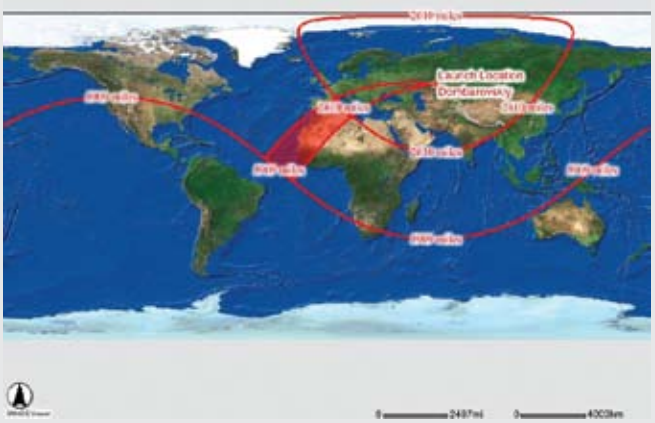


Figure 15. Missile Range Calculator Event.
This page is UNCLASSIFIED.

The last event tool is the Population Calculator. The latitude and longitude data is populated either manually or autopopulated utilizing the red circle with the crosshairs. The desired search radius (miles) is entered and then the population within the circle is estimated. No CIP report is provided with this event, but a notification is provided of the population possibly affected.

The Road Ahead

SMADS is a great tool for working with classified assets on the SIPRNET, but what about those assets that are more highly classified? During the data calls, the Joint Staff realized there would be assets that cannot be placed on the SIPRNET because of higher classification. We are currently not tracking those assets linked to Special Access Programs restricted sites or Intelligence, Surveillance, and Reconnaissance (ISR) assets that are normally above the SECRET level. We plan to develop a "SMADS-like" system on the Joint Worldwide Intelligence Communication System (JWICS) to track not only these assets but the DCAs as well. We are also engaging the DEWG and the DCIP community on how to best link vulnerability assessments such as those on the Critical Vulnerability Assessment Management Program (CVAMP) and the Vulnerability Assessment Catalog (VAC) to SMADS and other systems via Web services.

We plan to develop a "SMADS-like" system on the Joint Worldwide Intelligence Communication System (JWICS) to track not only these assets but the DCAs as well. We are also engaging the DEWG and the DCIP community on how to best link vulnerability assessments such as those on the Critical Vulnerability Assessment Management Program (CVAMP) and the Vulnerability Assessment Catalog (VAC) to SMADS and other systems via Web services.

One item noticed during training sessions at the Joint Staff, USPACOM, and USNORTHCOM was the absence of military units on SMADS. This system was not initially designed to provide the common operating picture (COP) for DOD but it is gaining ground by adding features all the time. One recent suggestion is to add military units with metadata detailing the number and type of personnel and equipment that are available. This system is not meant to be used as a readiness tool because such a system is already in place; instead, the system will assist the Homeland Defense mission and Defense Support to Civil Authorities (DSCA). Operationalizing SMADS with live feeds from other data sources such as Command and Control, Battle Management, and Communications (C2BMC) and the Global Command and Control System (GCCS) to see the locations of various military units, Carrier Strike Groups, Expeditionary Strike Groups, and other mobile assets would be a great feature; however, this coordination would take some time, and it has not yet been decided whether it will be undertaken. The number one rule for SMADS is to pull data from the "authoritative source" instead of replicating work that has already been tasked elsewhere.

With the constant update of Homeland Security Infrastructure Program (HSIP) Gold layers, there is never a shortage of data layers that could be added to SMADS and to other geospatial tools such as Palanterra and HD-MAP. The SMADS developers are listening to the field and will consider any reasonable request regarding layers of data that could affect DOD assets and assist users in operational analyses. Much data on the NIPRNET could be used on SMADS, but because of cross-domain problems within the IT community, SMADS cannot yet transfer data directly; transfer must be done through "sneaker net" or by burning data onto a disk and transferring it manually. This occurred during the California wildfire support provided by SMADS.

Other items being developed include a date/time stamp on all data contained in SMADS so a user can determine the age of the data. The data in SMADS changes approximately every day as users go in and modify their data. All users can view change history for their current organizations.

When Web-mapping services become available later this year, SMADS will have the capability to consume imagery at one meter resolution for any place where DOD assets are located. Some areas will have even better imagery.

Additional layers that are being considered for inclusion into SMADS are undersea communication cables and oil and natural gas distribution sites and refineries.

Conclusion

SMADS has been used extensively for the past few months at the Joint Staff to keep the senior leadership informed during real-world and exercise crises. SMADS is not the COP that has everything for everybody, but it is one tool that caters to the DCIP community and can provide information at the classified level for a variety of events. SMADS has truly operationalized the Defense Critical Infrastructure Program.

Role Playing in Today's Training Environments

By Lindsey Nagtzaam, Military Analyst, TRADOC

Introduction

Role playing is a common technique used to train and prepare soldiers. Although common, role playing is conducted differently among Services, groups, and agencies. In an effort to standardize training tasks, conditions, and standards while consolidating role playing techniques and focusing role-players, trainers, and role-playing programs, the US Army Training and Doctrine Command (TRADOC) G2 recently published the *Contemporary Operational Environment (COE) Actors and Role-Players Handbook* and an accompanying training support package (TSP). The handbook provides various role-playing considerations across the Services and in the interagency, interdepartmental, and multinational training arena. The purpose of the handbook is to orient leaders, trainers, scenario writers, and role-players who are training in the COE. Each participant must know and understand the COE, the actors within it, and their effects on training exercises.

The TRADOC G2 is responsible for development, management, administration, and approval of the COE concept for the Army. In that capacity, the TRADOC G2 is responsible for documenting the doctrine, organization, and capabilities of an opposing force (OPFOR) that is appropriate for training the Army's leaders, Soldiers, and units for the COE.

The proponent of TRADOC G2 that is responsible for the Army's OPFOR program and other threats-based material is the TRADOC Intelligence Support Activity (TRISA)–Threats program, based at Fort Leavenworth, Kansas.

The *COE Actors and Role-Players Handbook* is on the TRISA-Threats Web site, which is accessible through the Battle Command Knowledge System (BCKS), a portal of the US Army's Army Knowledge Online (AKO) system. To access the information on BCKS, you must possess an Army user name and password.

The *COE Actors and Role-Players Handbook* is an unclassified reference. Using the variables of the COE, a methodology outlines the orientation and training of role-players in COE education and training exercises. The handbook is a reference guide for trainers and

The purpose of the* Contemporary Operational Environment (COE) Actors and Role-Players Handbook *is to orient leaders, trainers, scenario writers, and role-players who are training in the COE. Each participant must know and understand the COE, the actors within it, and their effects on training exercises.

role-players, and a supplement to the Field Manual (FM) 7–100 series of COE OPFOR doctrine. The FM 7–100 series can be found at AKO (www.us.army.mil) and at the General Dennis J. Reimer Training and Doctrine Digital Library (www.adtdl.army.mil).

The study and integration of the various actors in the COE improves the readiness of US military forces. As a living document, the handbook will be updated to ensure it remains a current and relevant resource. The current version of the *COE Actors and Role-Players Handbook*, dated August 1, 2007, is the first edition published by TRADOC G2.

Each of the chapters contains specific information designed to assist those involved with role-players, scenario developers, training developers, and exercise directors in developing a realistic and challenging operational environment (OE). Electronic links are provided within the handbook to provide expanded information resources. The term *role-player* is used throughout the handbook to refer to people who are hired or assigned to portray particular characters within a training exercise.

Concepts

The *COE Actors and Role-Players Handbook* may be utilized as a stand-alone reference or in conjunction with the following references: Joint Publication 1–02, FM 3–0, FM 7–0, the FM 7–100 series, FM 6–22, the Army Universal Task List (AUTL), and the Universal Joint Task List (UJTL). Additional references may also assist users in their role-player training. To maximize the benefit of the content, users must understand the following COE variables prior to applying techniques and concepts from the handbook:

- **Political:** Distribution of power, will, legitimacy
- **Military:** Capabilities, flexibility, instrument of a particular political system
- **Economic:** Haves and have nots, resources, legitimate and black markets
- **Social:** Culture and ethnic composition, groups of people, institutions
- **Information:** Perception management, flow of information
- **Infrastructure:** Systems, technological advancement
- **Physical Environment:** Defining factors, complex terrain, adverse weather
- **Time:** Operational planning factor, tool, does not favor the United States

In the operational world or the training environment, any OE can be defined in terms of these variables (PMESII-PT). The linkage among variables is critical for successful analysis and application to role playing. The links between the variables set or create the conditions of each environment. Trainers and scenario writers must understand this synergy and be able to adapt actions based on the dynamic nature of this relationship.

The start point for understanding the OE must be those critical factors that reside in all OEs and have the greatest impact on the military. The conceptual template for any future military operation must incorporate the expected characteristics of these variables.

Actors may portray noncombatants such as locals, displaced persons, members of the media, or humanitarian relief workers.

Although these variables can be useful in describing the strategic environment, they are also useful for defining the nature of a specific OE. Each condition will vary according to a specific situation. These variables are interrelated and sometimes overlap. Different variables will be more or less important in different situations. Each OE is different because the content of the critical variables are different. Trainers and role-players must understand this synergy in order to present a realistic application of PMESII-PT for training units.

A myriad of actors exist within the COE. When the term *actor* is presented, imagine an actor on a stage. Actors in the COE sense of the word are not on a stage; actors are entities. Actors are depicted by role-players through characters. For example, during a training event focusing on humanitarian assistance, a role-player may assume the role of a nongovernmental agency volunteer who, while in character, meets with a platoon leader to discuss a recent fuel shortage in the district. Actors may portray the following paramilitary organizations:

- Insurgent organizations
- Guerrilla organizations
- Private security organizations (situation-dependent; may also be noncombatant)
- Criminal organizations
- Other armed combatants.

Actors may also portray noncombatants:

- Armed noncombatant
  - Public security organizations
  - Locals

- Unarmed noncombatant
  - Medical teams
  - Media
  - Humanitarian relief organizations
  - Displaced persons.

Refer to FM 7–100.3 for a complete list of paramilitary organizations, combatants, and noncombatants.

Utilizing their understanding of the COE, its variables, and its actors, trainers and role-players may apply their knowledge to role playing. In Chapters 3 through 7, the *COE Actors and Role-Players Handbook* discusses concepts, considerations, techniques, and tools for trainers, role-players, scenario writers and designers, and others. Before applying these chapters to training, role-players must be defined; Chapter 2, "Role-Play Terminology," describes the types of role-players used in role playing and describes the specifications of each. The terms used in this particular chapter of the handbook are not doctrine; however, in an effort to consolidate terminology used across the US Army training spectrum, the terms should be used in training.

Role-players participate in a fictional riot with Indiana National Guard Soldiers.

Considerations

The following section briefly discusses the contents of Chapters 3 through 7. The contents of each chapter build from the preceding chapter. The culmination of the handbook is a conceptual example of a training program developed through application of the techniques presented in the previous chapters.

Chapter 3, "Individual and Collective Training Considerations"

Application of role-player terminology occurs when preparing role-players for integration with training units. Role-players must gain an understanding of the training unit's mission and training objectives in order to effectively enhance training and perform accurately on the battlefield. This chapter discusses concepts of how to successfully conduct role-player training in order to assist trainers in the development of professional and successful role-players. It provides trainers with the considerations required to orient role-player training and coordination toward the training unit's mission. It maintains a battle focus by linking individual and collective battle tasks with tasks on the unit's mission-essential task list (METL) for all training events.

Chapter 4, "Tools for Trainers"

Trainers who are integrating the unit mission into role-player training will need tools to facilitate the process. This chapter provides tools and techniques to improve role-player confidence, track character assignment, and assess overall role-player performance. The techniques and tools are designed for trainers to utilize individually or in conjunction with the handbook.

Chapter 5, "Role-Player Outfitting Materiel"

This chapter provides an overview of the clothes and accessories necessary to create and represent characters in today's COE. In this chapter, trainers will find suggestions for clothing fidelity, factors to consider when outfitting role-players, resource management considerations, use considerations for military versus civilian role-players, a timeline for outfitting and materiel planning, and a section on role-player certifications.

Chapter 6, "Media Affairs and the Role-Player"

This chapter provides trainers and role-players with considerations for media training and role playing. Trainers will find types of media role-players and media affairs planning and training.

Chapter 7, "Training Program Concept"

This chapter provides trainers, scenario designers, and role-players with ideas for enhancing a preexisting training program or for developing a new one.

Application

Combining the COE concept with the contents of the handbook could be challenging for those who are unfamiliar with its terminology. The following example is provided as a "take-away" product to initiate and improve role-player training.

For the purpose of this example, ART 8.4.3.1.1, Provide Disaster Relief, from FM 7–15 will serve as the unit's training objective.

Step 1: Frame the Training Scenario

Frame the training scenario within the context of the identified training objectives and identify applicable role-players. Within a flood-ravaged town, the

Role-players at the Fourth Street Market, Camp Funston, Fort Riley, Kansas.

following specialized and generic role-players are required to achieve the training objective:

- Two emergency preparedness administrators (specialized role-players)
- Five medical professionals (specialized role-players)
- Two construction company owners (specialized role-players)
- 10 to 20 displaced families (generic role-players).

Care must be given to identify the optimal mix of characters in the scenario to satisfy the training objective, the commander's end state, trainers, and role-players.

A displaced family member states: "Our town was recently ravaged by a flood. The levy broke, and we were unable to save our belongings. Everything we own is gone. Who is going to help us? Where do we turn for assistance?" Interaction among all role-players and the training unit will assist this person and other displaced civilians.

Step 2: Identify PMESII-PT Variables

Identify PMESII-PT variables within the scenario in conjunction with the established training objectives. The example utilizes the economic, infrastructure, and time variables. (Keep in mind that not all variables apply in this example and may not apply in yours either.)

The given variables will manifest themselves in this manner for the flood-damaged city:

- **Economic.** Emergency preparedness administrators dispatch teams to assess the damage to the flooded city. Administrators begin to create a budget for cleanup of the town. Aid is needed immediately.
- **Infrastructure.** Emergency preparedness administrators begin to work with the construction company owners on temporary home plans for the displaced civilians. Former farmland is selected as the site for temporary homes.
- **Time.** Displaced civilians grow anxious as days pass and they remain in a shelter. Construction companies have begun to build temporary homes, but progress seems slow. Volunteers arrive to help with the cleanup.

Trainers and scenario writers must ensure that each variable that is chosen for the scenario and for role-players possesses both a beginning and an end state. This structure establishes and supports role-player dynamics and a framework for the scenario.

The following conditions manifest in the OE of the flood-ravaged town:

- The economic climate of the town has deteriorated.
- Displaced civilians are completing forms from the emergency preparedness teams in order to collect assistance funds.
- One construction company has halted construction because of theft and looting on several temporary home sites.
- Medical professionals are overwhelmed and running out of supplies.

These conditions describe the manner in which the role-players must interact with each other and with the training unit. The role-players now have a basic set of instructions to support the training objective. With this information, a special-skill role-player can engage in a series of interactions that enhance the training environment.

Step 3: Address Role-Player Dynamics

In this step, trainers must ensure role-player dynamics such as role echeloning, scripted role playing, and emerging relationships are understood within the scenario. These dynamics, when present, will create an adaptive living environment for the training unit within the scenario based on their actions and reactions. For example, role echeloning will occur between an emergency preparedness administrator and the senior officer present. The senior officer present at the cleanup site will choose one of the two emergency preparedness administrators as the lead administrator for the town cleanup. The senior officer will work directly with the lead administrator

versus two administrators in order to lessen confusion. The senior officer will create support teams to work directly with the displaced civilians.

One displaced person states: "Things got really bad here these last few weeks. I didn't think we would ever have a place to call home. Now that LTC Harper assigned assistance teams to all of our families, I see a light at the end of our tunnel. Our kids can return to school in a nearby town. We have started to receive our aid, and the medical teams are helping me get my prescriptions."

must conduct a cross-walk of all these steps. Trainers will cross-walk PMESII-PT, training objectives, dynamics of role playing, and demographics of the training unit to ensure achievement of the desired training objective.

During the cross-walk in this example, trainers and scenario designers overlooked the need for translators within the flood-ravaged town. This oversight occurred because trainers thought the emergency preparedness teams had translators on staff. As a result of the oversight, the need for additional skilled

Role-playing is an effective exercise in preparing soldiers for the complex situations that they encounter in the real world and on the battlefield.

Step 4: Consider Unit Demographics

The balance between scripted and free role play depends on the overall experience of the unit, the complexity of the training objective, and the ability of the role-players. Less experienced units will require more scripted role play to control the conditions in which they are training.

In the context of this example, the training unit is considered experienced with a mix of soldiers who have been previously deployed to provide disaster relief. Trainers must be considerate of the training unit's level of experience in relation to the training objective and role-player experience. With a more experienced training unit, trainers and scenario designers can include an increased amount of role-player dynamics.

After two deployments to assist hurricane victims in 2005, LTC Harper's expertise is obvious. He understands the needs of the civilians and the needs of the emergency, medical, and construction teams.

Step 5: Assess Scenario Fidelity

To effectively achieve the training objective, trainers role-players was added to the overall role-player requirements. Constant reassessment of role-players, both generic and special-skill, should occur throughout the training scenario preparation and exercise.

Summary

The *COE Actors and Role-Players Handbook* and TSP provides leaders, trainers, scenario writers, and role-players with a model and the information needed to accomplish holistic role-play training within the COE.

A need remains for current products that conform to the warfighter's high operations tempo (OPTEMPO) and the COE. TRISA-Threats strive to provide these quality products for those training with the OPFOR. Utilization of these products will greatly enhance training programs, not only within the military services but across agencies and groups.

TRISA-Threats, the proponent for this handbook, also offers several other products for use by the warfighter. Refer to the TRISA-Threats Web site for additional information on the products.

Defending Against the Unknown: Antiterrorism and the Terrorist Planning Cycle

By LTC Ashton Hayes

LTC Ashton Hayes is a US Army Military Police (MP) officer currently assigned to the Office of the Assistant Secretary of Defense for Special Operations/Low-Intensity Conflict and Interdependent Capabilities as assistant for Antiterrorism Policy. From October 2003 to March 2006, he served as Commander, 716th MP Battalion. During his command, the 716th supported operations in Iraq and Afghanistan. In Afghanistan, the unit was responsible for the security and protection of Bagram Air Base and the surrounding area.

Even without specific threat information, garrison commanders can deter and prevent potential attacks by developing antiterrorism (AT) programs that focus on exploiting vulnerabilities in the consistent planning methodology of today's terrorists. For a garrison commander, an attack prevented is a greater victory than an attack defeated.

In May 2007, a plot to attack Fort Dix, New Jersey, was disrupted and dismantled by a four-month investigation led by the Federal Bureau of Investigation (FBI) that culminated in the arrest of six suspects.[1] In August 2007, after a year-long investigation, German authorities arrested three Islamic Jihad Union operatives for preparing to conduct attacks against European and American interests in Germany.[2] In both cases, outstanding professional investigative and surveillance work was conducted by the law enforcement organizations after information or intelligence was received that indicated specific individuals were conducting attack planning.

Intelligence or criminal information is the key to successful law enforcement or counterterrorism operations. Since the attacks against America on September 11, 2001, our law enforcement officials and counterterrorist professionals have arrested, captured, or killed hundreds of people who have attacked or planned attacks against American or Western interests. The operations have run the gamut from long, meticulous investigations such as the case of the "Fort Dix Six" to dramatic "Tom Clancy–like" operations such as the unmanned Predator attack against terrorists in Yemen in 2002[3] or the more recent January 29, 2008, Predator attack that killed al Qaeda senior leader Abu Laith al-Libi.[4] These operations have one similarity: In all cases, planning was started for the eventual operation based on some nugget of intelligence or tidbit of information. The

Can a commander develop an AT program that protects the installation without having to rely on threat information? The answer is absolutely yes, and in fact, the commander may be able to prevent or deter attacks before they are ever fully planned. The fact that commanders must protect their installations even in the absence of any known or actionable intelligence is why AT programs must remain resourced and supported.

greatest tactical plan ever developed or the most precise and technologically advanced weapon will not kill or capture a terrorist if the terrorist cannot be found.

That is not to say that operations designed to capture or kill terrorists are easy. Without a doubt, the complex planning and coordination required make such operations very difficult; the operations described above possessed the advantage provided by intelligence or criminal information in identifying the target. But counterterrorism missions are not the only challenging operations in the fight against terrorism.

Today's garrison commanders also face a very challenging responsibility in trying to balance tactical defensive science with the art of risk management to develop AT programs that defend against terrorist threats that may never appear. This challenge is even more daunting if there is no intelligence or criminal information indicating a potential threat, which is usually the case. Can a commander develop an AT program that protects the installation without having to rely on threat information? The answer is absolutely yes, and in fact, the commander may be able to prevent or deter attacks before they are ever fully planned. This article will identify three AT planning principles that, when properly applied, will focus the strengths of a commander's AT program against the inherent vulnerabilities of the planning methodology attributed to terrorists.

Antiterrorism Victory Without Prior Warning

There are many instances of attacks occurring or reaching final preparation without any indication or warning to the defender. In February 2007 at Bagram Air Base, Afghanistan, a suicide bomber tried to gain access to the base during Vice President Dick Cheney's visit.[5] In this case, the bomber detonated outside the base because the established and strictly enforced AT and access control procedures prevented the bomber from gaining entrance. Although lives were tragically lost, the loss could have been much greater if the bomber had made it onto the base.

Another example of an AT program that succeeded without any advance intelligence occurred in 2007 at Dover Air Force Base (AFB). This particular incident focused on the perceptions and decisions of the Fort Dix Six plotters. The suspects surveilled Dover Air Force Base but rejected it for attack because the base "was too difficult of a target because of its high security."[6] With absolutely no intelligence indicating that an attack was even under consideration, the Dover AFB security and antiterrorism professionals prevented a possible attack.

Just how did the Dover AFB commander achieve such success? The answer is, through the careful and diligent execution of a base protection and AT program that not only helped prevent attacks but, just as importantly, discouraged attacks.

Therein lies the strength of today's DOD AT program. By its very design, the DOD AT program protects our personnel and resources from attack and discourages would-be terrorists from even considering an attack. Additionally, AT programs do not need intelligence or criminal information to succeed. The fact that commanders must protect their installations even in the absence of any known or actionable intelligence is why AT programs must remain resourced and supported. A counterterrorism operation or criminal investigation can be meticulously planned, resourced, and ready to go, but if there is no target or if the intelligence is wrong, then the operation will not be as successful as desired. A robust AT program can help prevent this outcome.

If an AT program can succeed despite a lack of intelligence, how can commanders prepare their installations to best deter or disrupt a potential terrorist attack? The answer is, by developing an AT program that is layered, integrated, and focused on defeating or deterring the terrorist before an attack occurs through the disruption of the "Terrorist Planning Cycle."

Figure 1. Marine Barracks building [*Marine* magazine, November 1993.]

DOD Antiterrorism History

In 1983, the tragic bombing of the Marine Barracks in Beirut, Lebanon (Figure 1),[7] led to the development of the DOD AT program. The DOD had always taken measures to protect its personnel and resources, but the Beirut bombing brought the term antiterrorism to the forefront of military thinking. Since then, the AT program has undergone several evolutionary changes because the program has always adapted to the latest enemy tactic.

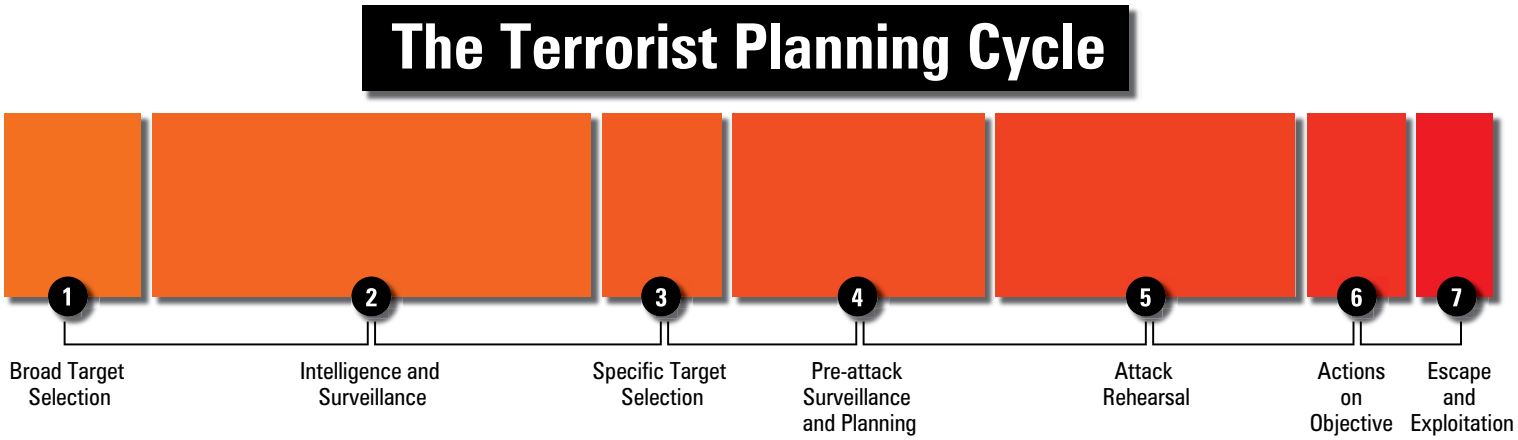


Figure 2. The Terrorist Planning Cycle as defined in the *Military Guide to Terrorism in the Twenty-First Century*

Antiterrorism programs and initiatives must continue to play an integral role in the fight against terrorism primarily because the threat is not going away. The June 2007 National Intelligence Estimate stated that "Al Qaeda retains an undiminished desire to attack the United States".[8] More recently, in February 2008, Director of National Intelligence Michael McConnell briefed Congress on the belief that al Qaeda is continuing to work and improve its capabilities to place operatives inside the United States.[9] The threat is real and will remain so for the foreseeable future.

Garrison commanders have responsibility for protecting the installation populace, resources, and facilities from terrorist attack. Today's commanders will apply risk management as they decide how much emphasis to place on AT in their organizations. Geographic location, threat, size, and criticality are just some of the criteria that must be considered by the commander when developing the AT program. Regardless of the size or location of an installation, the success of an AT program is directly proportional to the emphasis and priority given to the program by the commander. The question commanders must continually ask themselves is: Am I doing enough to protect my people?

Conversely, while our leaders struggle to protect their personnel and facilities, the terrorists are also diligently working to figure out how to target our installations and facilities. Much like combat operations, adversaries are working to try and outwit each other in a potentially deadly game of cat and mouse. How can the AT program assist the commander on the ground in achieving success against the target?

There is no perfect answer. By applying the strengths of an AT program to the vulnerabilities of the planning methodology attributed to terrorists, a commander can better achieve success. The goal is not necessarily to catch the terrorist but to deter an attack from occurring. As previously mentioned, an attack that never occurs is just as much a victory if not a greater victory than an attack that occurs and is defeated.

The Terrorist Planning Cycle

If commanders develop AT programs that are designed to protect against terrorist attacks, then it is only logical that the terrorists will have a methodology for identifying targets and planning attacks. In August 2007, the US Army Training and Doctrine Command (TRADOC) created the *Military Guide to Terrorism in the Twenty-First Century*, which discusses how terrorists think and operate.[10] In the guide, TRADOC defines what is called the Terrorist Planning Cycle as a seven-phase process (Figure 2).

Phase 1: Broad Target Selection

The attackers use open source media and research sources to identify what type of target would best further their goals.

Phase 2: Intelligence and Surveillance

In this phase a great deal of time and effort is spent analyzing every detail, including travel patterns, security measures, and practices and procedures. A specific target is not usually identified at this point, as the analysis of the gathered intelligence will help the terrorists further narrow their list of possible choices. Intelligence gathering can be a very short process or can last for years depending on the desires and experiences of the terrorists.

Phase 3: Specific Target Selection

At this point, the terrorists take all the information and intelligence gathered during Phase 2 and make a decision to commit to a particular target.

Phase 4: Pre-Attack Surveillance and Planning

In this phase, the terrorists really begin to focus on the "nuts and bolts" of the planning for the operation. Decisions are made regarding access to target, transportation, escape route, and types of weapon or attack. More focused surveillance of the target is required to fully understand all the nuances of the existing security measures.

Phase 5: Attack Rehearsal

Like any good military operation, rehearsals are the key to a successful terrorist attack.

Phase 6: Actions on Objective

At this point, the terrorist hopes to have several tactical advantages, including time, place, and conditions of the attack, as well as a possible element of surprise.

Phase 7: Escape and Exploitation

Depending on the attack method, plans for escape and exploitation may be well rehearsed or they may not exist at all, as in the case of a suicide attack. Escape may not be the priority in Phase 7. The more likely priority is exploitation of the attack. Regardless of whether or not the terrorists successfully escape the attack, the terrorist organization will try to use all available media outlets to publicize the attack to the intended audience.

Using the AT Program to Counter the Terrorist Planning Cycle

Terrorists generally follow the Terrorist Planning Cycle. So what? How can commanders use their AT programs to help defeat or deter a threat that may not even be known? After all, a commander can only devote so many resources to the protection of the base.

Even in a world of limited resources and potentially no actionable threat information, the Terrorist Planning Cycle offers two opportunities for a commander to disrupt or deter a potential attack. During Phase 2 (Intelligence and Surveillance) and Phase 4 (Pre-Attack Surveillance and Planning), a commander may be able to deter a potential attack by creating a defensive bubble that is deemed too hard for the terrorists to exploit.

How can a commander exploit the weaknesses in the Terrorist Planning Cycle? Known and unknown terrorist threats can potentially be deterred and subsequently defeated by following three AT program principles that support the inherent strengths of AT while simultaneously capitalizing on the vulnerabilities in the Terrorist Planning Cycle.

Principle 1: Baseline AT Consistency

The first principle is to always maintain a baseline AT consistency, especially with regard to access control procedures. If terrorists are conducting surveillance, they should, at a minimum, always see an installation that never goes below a certain level of scrutiny. Because access control points are the most likely means of entry for a terrorist, it is critical that the access control procedures reflect a baseline consistency.

Even in a world of limited resources and potentially no actionable threat information, the Terrorist Planning Cycle offers two opportunities for a commander to disrupt or deter a potential attack. During Phase 2 (Intelligence and Surveillance) and Phase 4 (Pre-Attack Surveillance and Planning), a commander may be able to deter a potential attack by creating a defensive bubble that is deemed too hard for the terrorists to exploit.

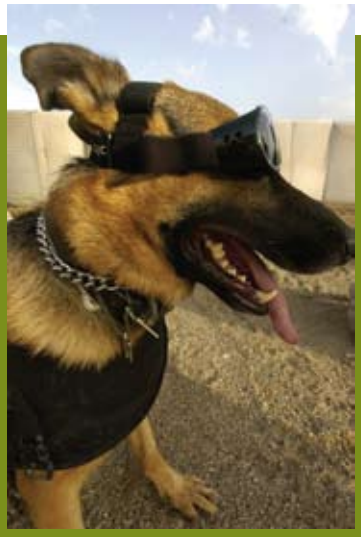
Even more problematic is the fact that there may be absolutely no indications or warnings that a particular installation is under surveillance or being targeted. Remember, the greater and least costly victory for the defender is an attack that does not occur because it was deterred.

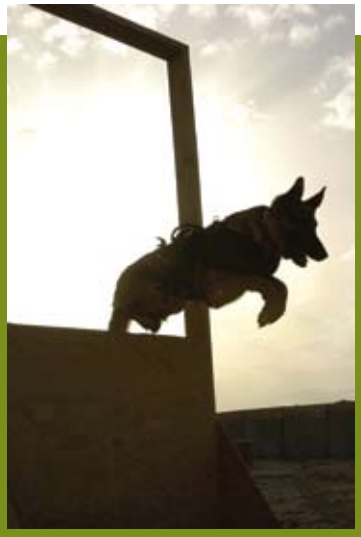
The vulnerabilities can be identified in the Terrorist Planning Cycle by listening to the terrorists themselves. Dr. George Habash, the founder of the Popular Front for the Liberation of Palestine and a well-known terrorist tactician, said, "The main point is to select targets where success is 100% assured."[11] Terrorists are much less likely to target an installation that is well secured because the chance of success is diminished; however, that does not mean an installation will not be targeted, especially if the overall objective is to target the US military. This uncertainty is where the opportunities to exploit the vulnerabilities of the Terrorist Planning Cycle come into play.

DOD Instruction (DODI) 2000.16 requires that all DOD components have an access control program, even at the lowest Force Protection Condition. The military departments vary in their program requirements from a minimum of a DOD ID card to a DOD vehicle registration sticker and a DOD ID card, but they all have a minimum standard. Commanders must ensure that the minimum standard is not lowered. Watchful terrorists will quickly pick up on "chinks in the armor" when looking at access control procedures.

Principle 2: Judicious Use of RAMs

The second principle is the regular and creative use of Random Antiterrorism Measures (RAMs). In today's environment, there is no way that a commander can afford to maintain and enforce all possible access control measures. Such a bold attempt would be too costly, and more importantly, the inconvenience to the population would be too extreme under normal circumstances. But, by capitalizing on





Whether it is military working dogs checking cars or extra personnel on the gates, a changing appearance will help to drive potential terrorists away.

all of the available enforcement and protection tools, a commander can create a sense of uncertainty for any would-be terrorists because the picture at the gates is always changing. Whether it is military working dogs checking cars or extra personnel on the gates, a changing appearance will help to drive potential terrorists away. The key is to not let the RAMs reduce the baseline consistency. RAMs must augment access control procedures, not replace them.

Principle 3: Remain Alert

The final principle is simply to pay attention and react to unusual circumstances. If threat indicators are identified, then commanders must prepare to adjust their protection procedures appropriately and not wait for future indicators. Adjusting protection procedures does not mean that a commander needs to immediately institute the most restrictive inspection procedures. The response may be nothing more than working closer with local law enforcement officials to try to verify the veracity of the indicators.

The commander must always think about what the indicators are saying. Ignoring the indicators because they always seem to be false can eventually lead to the "boy who cried wolf" mindset. Keeping the protection procedures as a priority will ensure that the commander and staff do not let a sense of complacency creep into daily operations.

Conclusion

Well-planned and executed AT programs that focus on the vulnerabilities in the Terrorist Planning Cycle can deter and prevent attacks before they ever occur. Though desired, threat intelligence and criminal information is not required for a commander to succeed in protecting the personnel, resources, and facilities on his installation.

Garrison commanders are tasked with the responsibility of protecting installations against terrorist threats. In the struggle to defend against potential terrorist threats, commanders face three truths:

- The threat is real and is not going away.
- There may never be intelligence or criminal information indicating that a potential threat exists until after an attack occurs.
- Terrorists have rejected and will reject an installation as a possible target because of its visible security posture, and the commander will likely never know the installation was even under targeting consideration.

Commanders face enormous pressures trying to balance their responsibility to protect the installation with the competing demands of limited resources and the mobility needs of the base population. The correct use of the right personnel leveraged with existing and emerging technology can create a security posture that prevents terrorist attacks before they are planned. After all, a prevented attack equals victory.

---

1 Associated Press. "Store Clerk Helps Feds Bust 6 in Alleged 'Jihad' Plot to Kill U.S. Soldiers at Ft. Dix." *Fox News*, 8 May 2007. Available at http://www.foxnews.com/story/0,2933,270601,00.html.

2 Isikoff, Michael, and Hosenball, Mark. "The Suspects Who Got Away." *Newsweek*, 5 October 2007. Available at http://www.newsweek.com/id/42244/output/print.

3 Global Security. "MQ-1B Armed Predator." 6 October 2007. Available at http://www.globalsecurity.org/intell/systems/armed-predator.htm.

4 Warrick, Joby, and Wright, Robin. "Unilateral Strike Called a Model for U.S. Operations in Pakistan." *Washington Post*, 19 February 2008. Available at http://www.washingtonpost.com/wp-dyn/content/article/2008/02/18/AR2008021802500.html.

5 MSNBC News Service. "Cheney Unhurt After Deadly Blast at Afghan Base." *MSNBC*, 27 February 2007. Available at http://www.msnbc.msn.com/id/17355517.

6 Caudill, Shannon, Lt Col. "Lessons Learned: The Fort Dix Six." *The Guardian*, Winter 2007.

7 *Marines Magazine*. November 1993. Photo available at http://www.beirut-memorial.org/history/index.html.

8 Office of the Press Secretary. "Fact Sheet: The Terrorist Threat to the US Homeland." *White House*, July 2007. Available at www.whitehouse.gov/news/releases/2007/07/20070717-2.html.

9 McConnell, J. Michael. "Annual Threat Assessment of the Director of National Intelligence." *Office of the Director of National Intelligence*, 5 February 2008. Available at http://www.dni.gov/testimonies/20080205_testimony.pdf.

10 US Army Training and Doctrine Command. "A Military Guide to Terrorism in the Twenty-First Century." 15 August 2007. Available at http://www.fas.org/irp/threat/terrorism/index.html.

11 Dershowitz, Alan M. *Why Terrorism Works*. 2002. New Haven, CT: Yale University Press.


Know the Enemy
US Army TRADOC
TRADOC G2
Training Support Package
159-T-0001
A Military Guide to
Terrorism
in the Twenty-First Century
TSP
New
US ARMY TRADOC
KNOW THE ENEMY
THREATS TERRORISM TEAM
TRISA
NEVER FORGET
WE are at WAR!
on
TERRORISM
Terrorism in COE
Motivations
Behaviors
Organization
Targeting US Forces
Patterns and Trends
Foreseeable Future
Learning Activities
Use the TRADOC G2
Terrorism Handbook Series
US Army TRADOC G2
TRISA-Threats WOT Poster No. 6A-08
https://dcsint-threats.leavenworth.army.mil
(Source: DoD Photo)

Notes from the War on Terror

Overcoming the ideology of hate and terror

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

"This is a very cowardly action being carried out in the home of God, where the people come to offer their prayers. But fearless and ignorant people are carrying out these suicide attacks, killing innocent people inside a holy and respected place. This is totally against our religion of Islam to blow himself up in the mosque."

Muhammed Hussain Andiwal
Provincial Afghan police chief
New York Times
February 2008

"Al Qaeda and its Taliban allies did all they could to prevent and then to disrupt the exercise. They killed some 300 candidates, election officers, and party activists. Their sinister slogan 'From Box to Box,' meaning that anyone who casts a vote into the ballot box could end up in a coffin, was posted or scribbled on many walls. The terrorists also destroyed at least 12 polling stations and stole several dozen ballot boxes. Still, they failed."

Amir Taheri
Asharq Al-Awsat
22 February 2008

"The killing has taken Hezbollah off guard and is now considered as a serious breach of uneasy truce with Israel. It is a matter of time before the party responds and it has proven that it has the ability and infrastructure to do so. Its retaliation will ignite a new cycle of violence and may lead to a new war between Israel and Hezbollah."

Osama Al Sharif
Arab News
20 February 2008

"The government understands, in Yemen you must compromise to reach a solution. The Americans would like to put us all in jail. But if you do this, 10 men will become 20, 20 will become 100, and then—we will be an army."

Ali Abdullah Saleh
President of Yemen
New York Times
28 January 2008

"The most evil of the traitors [Iraqi Sunni Arabs who form Awakening Councils to resist al Qaeda in Iraq] are those who trade away their religion for the sake of their mortal life ... Our duty is to foil these dangerous schemes, which try to prevent the establishment of an Islamic state in Iraq, which would be a wall of resistance against American schemes to divide Iraq ... We intend to liberate Palestine, the whole of Palestine from (Jordan) river to the sea ... We will not recognize even one inch for Jews in the land of Palestine as other Muslim leaders have."

Osama Bin Laden
AP
30 December 2007

"We doubt al-Zawahiri's sincerity about having a serious dialogue with thinkers and religious and political experts."

Sheikh Kalid al-Mushuh
Spokesman for Saudi Anti-Extremism Campaign
Al-Hayah/OSC
25 December 2007

Notes from the War on Terror

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

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

	Event	Strategic Significance
Negative effects on the GATE	**Charges Dropped Against Iraqi Officials.** An Iraqi court dropped charges in March against two former government officials accused of allowing Shiite death squads to use ambulances and government hospitals to carry out kidnappings and killings. The case has been seen by minority Sunnis in this majority-Shiite country as a major test of the judiciary system, because a Shiite prime minister, Nouri al-Maliki, leads the government.	The reconstruction of Iraq will have to include a fair and just judicial system. Partisan rulings based on religious affiliation undermine the ability to form a functioning government based on the rule of law.
	Sri Lanka: Sri Lanka blast kills 26. A bomb and shooting attack blamed on Tamil separatists ripped through a packed civilian bus in January. The attack killed 25 people and injured 63 others in southeastern Sri Lanka as the government officially withdrew from a tattered cease-fire with the rebels. Officials said the blast came from a 44-pound mine just yards from the road.	President Mahinda Rajapaksa has said he abandoned the cease-fire because it wasn't working and the rebels used it as cover to build up their military strength. At least 5,000 people have been killed since the cease-fire was signed.
Uncertain effects on the GATE	**Violence Leaves Young Iraqis Doubting Clerics.** After almost 5 years of war, many young people in Iraq, exhausted by constant firsthand exposure to the violence of religious extremism, say they have grown disillusioned with religious leaders and skeptical of the faith that they preach.	Despite growing trends to the contrary across the rest of the Middle East, Iraqi youths are beginning to turn their backs on Islam. Most blame religious clerics for the violence and limitations that are placed on them. They are tired of these clerics lying to them and spreading hatred. The US should carefully monitor this recent development and work to ensure that positive opportunities exist for this disillusioned group.
	Al Qaeda in Iraq "Killing Off" Former Allies. (CNN) Video provided to CNN shows an al Qaeda in Iraq firing squad executing one-time allies—fellow Sunni extremists— who were not loyal enough to the terror organization. In the video armed men wearing masks are shown standing behind nine kneeling men, all of whom are wearing blindfolds or hoods with their hands presumably tied behind their backs. The video shows the men being executed.	Current trends continue to show Sunni extremists cooperating with US forces. This new and desperate tactic by al Qaeda in Iraq may keep the Sunnis from cooperating at first but will more likely incite them to turn against al Qaeda faster.
Positive effects on the GATE	**Al Qaeda Leader's Diary Reveals Organization's Decline.** US troops found a diary belonging to an al Qaeda in Iraq leader that has Coalition forces believing the terrorist organization is "on its heels." The diary belongs to Abu Tariq, an al Qaeda emir in control of five battalions within two sectors.	Al Qaeda's numbers are declining thanks to awakening groups such as Concerned Local Citizens. Despite being attacked more frequently, these groups are gaining members every day and are showing top al Qaeda leaders that they are not afraid to take back what al Qaeda has taken.
	Results of a Nationwide Public Opinion Survey of Pakistan before the February 18th Elections. In a dramatic reversal from just a few months ago, Pakistanis have turned against Osama Bin Laden, al Qaeda, and the Taliban. And in an equally stunning turnaround, in advance of Pakistan's upcoming February 18th elections, nearly two-thirds of Pakistanis now intend to vote for the moderate political parties on the ballot.	Pakistanis are telling al Qaeda that they have worn out their welcome. They have come to the conclusion that al Qaeda violates Islam and they want a change for the better.

> Websites

The following list of websites is provided as a supplement to *The Guardian* and a resource for its readers.

> DOD SO/LIC
http://www.defenselink.mil/policy/sections/policy_offices/solic/index.html

> NAVY AT/FP PROGRAM
https://portal.navfac.navy.mil/portal/page?_pageid=181,5560913,181_5560927&_dad=portal&_schema=PORTAL

> USMC AT/FP PROGRAM
http://hqinet001.hqmc.usmc.mil/pp&o/PS/psfp/psfpHome.asp

> US ARMY AT/FP PROGRAM
http://www-tradoc.army.mil/tpubs/regs/r525-13.htm

> USAF AT/FP PROGRAM
http://www.e-publishing.af.mil/shared/media/epubs/AFI10-245.pdf

> ATEP
https://atep.dtic.mil/

> FPED
http://www.fped6.org/

> TSWG
http://www.tswg.gov/

> OPEN SOURCE INTELLIGENCE/PUBLICATIONS
http://www.fas.org/irp/offdocs/index.html

> DOD DIRECTIVES/INSTRUCTIONS
http://www.dtic.mil/whs/directives/

> PSEAG (CAC REQUIRED)
https://fppscop.spawar.navy.mil/forum/zone1/dispatch.cgi/

> LEVEL I AT TRAINING
https://atlevel1.dtic.mil/at/

> FEMA
http://www.fema.gov/

> DHS
http://www.dhs.gov/index.shtm

> *EARLY BIRD*
http://ebird.afis.mil/

If you have a website you would like posted, please contact *guardian@js.pentagon.mil*

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.