Volume 10
Number 3

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

"This is the moment when we must defeat terror and dry up the well of extremism that supports it. This threat is real and we cannot shrink from our responsibility to combat it. If we could create NATO to face down the Soviet Union, we can join in a new and global partnership to dismantle the networks that have struck in Madrid and Amman; in London and Bali; in Washington and New York. If we could win a battle of ideas against the communists, we can stand with the vast majority of Muslims who reject the extremism that leads to hate instead of hope.

This is the moment when we must renew our resolve to rout the terrorists who threaten our security in Afghanistan, and the traffickers who sell drugs on your streets. No one welcomes war. I recognize the enormous difficulties in Afghanistan... For the people of Afghanistan, and for our shared security, the work must be done. America cannot do this alone. The Afghan people need our troops and your troops; our support and your support to defeat the Taliban and al Qaeda, to develop their economy, and to help them rebuild their nation. We have too much at stake to turn back now. "

—President Barack Obama
July 24, 2008

"What is dubbed the war on terror is, in grim reality, a prolonged, world-wide irregular campaign —a struggle between the forces of violent extremism and moderation. In the long-term effort against terrorist networks and other extremists, we know that direct military force will continue to have a role. But we also understand that over the long term, we cannot kill or capture our way to victory. Where possible, kinetic operations should be subordinate to measures to promote better governance, economic programs to spur development, and efforts to address the grievances among the discontented from which the terrorists recruit. It will take the patient accumulation of quiet successes over a long time to discredit and defeat extremist movements and their ideology. As the National Defense Strategy puts it, success will require us to 'tap the full strength of America and its people'—civilian and military, public sector and private."

—Secretary of Defense Robert M. Gates
September 29, 2008

"It's going to be some time before we know all the details behind the Mumbai attacks, perhaps even longer before we completely understand exact motives and goals. But it shouldn't be lost on anyone how a handful of well-trained terrorists using fairly unsophisticated tools in a highly sophisticated manner had at bay an entire city and nearly brought to a boil interstate tensions between two nuclear powers.

This wasn't just an attack on Indians or Americans or Brits or even Jews. It was, rather, an attack on all of us who love the sacred dignity of human life. As we witnessed in our own country seven years ago, the tactic of terrorism can be a deadly strategic weapon."

—Chairman of the Joint Chiefs of Staff ADM Mike Mullen
December 10, 2008

Guardian readers, as you are aware, we have had a change of administration here in Washington, DC. While this may be a period of transition, we must remain ever vigilant and committed to an all-hazards approach to force protection. We must ensure that we never present a static, predictable target to those who wish us or our new government harm.

Confronted with an era of shrinking defense budgets, it is increasingly important for our Antiterrorism Officers and commanders to understand how best to leverage available resources. To assist, the Antiterrorism branch released $42 million (FY08) in Combating Terrorism Readiness Initiative Funds (CbtRIF) for needed force protection initiatives worldwide. As recent events in Mumbai, India, show, the threat of terrorist attacks against soft targets remains a significant challenge. We must not lose sight of the potential for similar attacks here in the United States. As the memory and shock of 9/11 and of the Fort Dix Six fade, both are grim reminders to review, improve, and update your Force Protection Programs.

I encourage you to continue to challenge old assumptions, to submit new ideas, and to document lessons learned on the range of activities that are critical to our force protection efforts. *The Guardian* is an essential tool for sharing successful antiterrorism efforts and interacting with peers on important issues. Our last issue covered topics ranging from DOD law enforcement transformation to antiterrorism program assessments. In this issue, you have responded with a wide range of topics, from successful FOB access procedures to understanding the Jihadist threat. Take advantage of the opportunity to tell your story and to help others benchmark from your success. The Force Protection branch will continue to engage in programs that continue to affect the safety of the warfighter at home and abroad.

After 3 years on the Joint Staff, I will be moving over to the National Guard Bureau in 2009. It has been a pleasure to work with you and to serve our nation at the J-34. I could not be prouder of the many contributions made by our joint team to improve antiterrorism and force protection support to our forces. We have much left to do, and I'm confident my replacement, Brigadier General Jonathan Treacy, will continue to be your advocate and champion on many important issues.

As I close my tenure on the Joint Staff, I'm reminded by Thomas Jefferson's words of the importance of our mission in today's volatile world: "The price of freedom is eternal vigilance." Let this be our mantra as we collectively seek better ways to protect our countrymen. Thank you for your service and dedication to our democracy.

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.

Antiterrorism and Homeland Defense: Progress, Challenges, and Opportunities

By BG Peter Aylward, Deputy Director for Antiterrorism and Homeland Defense (J-34)

Defense of the homeland is the Department of Defense's highest priority with the goal to defeat threats at a safe distance from the homeland.[1]

—Joint Publication 3-27, Homeland Defense

Seven years after 9/11, it's clear that the war against terrorism will be a protracted conflict that places unique demands on the DOD. How we manage post-9/11 expectations is intertwined with how we prioritize the resources available to DOD, with an aim of balancing strategic risk. Institutionally, we have a tendency to fall into our comfort zone when we consider the wider range of activity in which DOD is expected to participate. In many ways, we continue fighting a war with old business models and processes that do not necessarily reflect the new realities of the Long War.

> If we are to meet the myriad challenges around the world in the coming decades, this country must strengthen other important elements of national power both institutionally and financially, and create the capability to integrate and apply all of the elements of national power to problems and challenges abroad.[2]
>
> —Secretary of Defense Robert M. Gates

The old DIME (diplomatic, information, military, economic) construct outlining the elements of national power has been replaced with a new framework, which is easy to remember with the acronym MIDLIFE (military, information, diplomatic, law enforcement, intelligence, finance, and economics).[3] It requires a "full court press" by the entire US government.

A fully integrated, information-sharing, and operational interagency construct raises many daunting challenges. Have we made the human capital investment to institutionally transform our interagency partners to "think strategically"? Have we made the investment in how we grow leaders to operate in this new environment? Have we laid the framework for how we synchronize the elements of national power to provide flexible response options to the National Command for global engagement?

As I reflect on my 3 years as the Joint Staff's Deputy Director for Antiterrorism and Homeland Defense, J-34, I hope to provoke thought and to provide key insights and recommendations on interagency reform as well as changes to policy and programs for force protection (FP), weapons of mass destruction

(WMD), and narcoterrorism. Driven by high public expectations, we need solutions that provide best business practices, especially in light of limited fiscal resources.

Interagency: The Future is Now

> The interagency process which was essentially developed in the 1950s is now broken. It is hopelessly too slow and too lacking in accountability. An integrated system has to be developed which sets metrics and accountability and which reports to the Commander in Chief with the clarity that a global battlefield requires.[4]
>
> —Former Speaker of the House Newt Gingrich

Interagency reform through legislative mandates is necessary. Much like the successful Goldwater-Nichols Act, the federal government must address its interagency approach to civil defense and national security. The Project on National Security Reform, headed by Goldwater-Nichols reformer James Locher, released its 751-page report on national security reform in December 2008. "The terrorist attacks of 9/11, troubled stability operations in Iraq and Afghanistan, and poor response to Hurricane Katrina provide compelling evidence of the inadequacy of current (interagency) arrangements," Locher reported.[5]

Interagency and national security reform are critical to the US government's overall effectiveness in combating new threats like WMD and narcoterrorism. The Project on National Security Reform is pushing for a new National Security Act in the coming year to bring Goldwater-Nichols–like reforms to the rest of the US government and to compel changes that are deeply needed.

Furthermore, as the discretionary funding available to DOD gets squeezed by other statutory programs, we need to take a hard look at how we conduct Joint, Combined, Interagency, and Intergovernmental operations. Is it time to look beyond the Joint Task Force and to embrace the Joint Interagency Task Force as the centerpiece of our formations? If the answer to that question is yes, then what have we done to prepare our leaders and their staffs to operate with our interagency and intergovernmental partners? Should we examine a professional development program that will prepare future leaders to deal with the interagency partners across the spectrum? Should such a program put special emphasis on domestic operations to provide appropriate special-skill and additional skill identifiers?

In addition to organizational reform, another area that needs to be examined is existing budgetary authority. Currently, the overall federal budgetary authority that governs homeland defense and domestic operations does not provide a cohesive, integrated funding strategy to ensure that forces are ready for the full spectrum of homeland defense operations needed to respond to a range of natural and manmade disasters. Instead, the authorities, enshrined in the Economy Act, in the Stafford Act, and in DOD policies, force the Department into a reactive posture and prevent the military from building necessary capabilities.

The Federal Civil Defense Act of 1950, repealed in 1958, provides a model that should be replicated today. The act was designed to thwart sabotage, espionage, and terrorism. It gave the Department authority to prepare, prevent, and deter domestic incidents from asymmetric actors (e.g., Spetznaz, saboteurs) as well as to prepare for response to catastrophic disasters (e.g., nuclear war.) These proactive models gradually morphed into a split between preparedness/mitigation and response/recovery within the response community.

Other funding priorities and the lack of a peer-nation competitor led to the elimination of many preparedness efforts. This problem was further exacerbated by the transition of disaster response from primarily a state responsibility to a federal bill with the adoption of the Stafford Act. That act focused on mitigating effects of both natural and manmade hazards and placed the greatest emphasis on postevent recovery.

Interagency and national security reform are critical to the US government's overall effectiveness in combating new threats like WMD and narcoterrorism. The Project on National Security Reform is pushing for a new National Security Act in the coming year to compel changes that are deeply needed.

A consequence (perhaps unintended) of the repeal of the Federal Civil Defense Act was DOD's loss of statutory authority to prepare for domestic operations. Implementation of the Stafford Act created a situation in which DOD is now mandated under the Economy Act to demand reimbursement for any actions taken to prepare for homeland security operations. In the aftermath of a catastrophic domestic event such as Hurricane Katrina, operating under the full scrutiny of the American and international media, DOD cannot

The 2008 attacks in Mumbai, India, have shown that terrorists change tactics and can easily gain the press coverage they desire with a spectacular, well-planned small arms attack. The threat of terrorist attacks against soft targets remains a significant challenge.

afford to be perceived as unprepared. Currently, the Services fund domestic support with the expectation that they will get reimbursed at a later date.

As funding gets tighter, we need to reexamine the Domestic Emergency Response Fund in an attempt to close the gap between Stafford Act authority and emergency supplementals. The idea is to provide the commanders in the field with the operational flexibility by providing cash flow and a funding bridge as the interagency community sorts out "who's in charge" and "who's paying the bill." The aim is to get on the front end of preparedness and to enable our commanders in the field to respond rapidly. More than at any other time in history, we need to examine these alternatives as other measures of good fiscal stewardship.

Force Protection: Relearning Old Lessons

When Gen James Conway was the J-34, he used to invite ADM Robert Long, US Navy (retired), the leader of the post–Beirut bombing commission, and GEN Wayne Downey, US Army (retired), the head of the post–Khobar Towers bombing analysis team, to Joint Staff antiterrorism training forums to discuss the lessons learned from recent terrorist attacks. A sobering fact is that the two post-incident reports are eerily similar in their findings. The similarity shows that the longer the span of time from a terrorist incident, the more likely we are to repeat the same mistakes and to become complacent.

Even today, we continue to find that more than 60% of vulnerability assessment deficiencies are the result of not following existing guidance and protocols. In other words, commanders are not exercising hands-on and innovative leadership to test and refine the responsiveness of their installations and units for antiterrorism scenarios. Commanders must make FP a priority, address their antiterrorism command and control structure, and appoint and empower a qualified Antiterrorism Officer.

The 2008 attacks in Mumbai, India, and the foiled 2007 attack planned against Fort Dix provide glimpses into the shifting tactics of terrorists. The US government has invested in ways to defeat vehicle-borne improvised explosive devices (IEDs), including improving standoff distances, hardening key buildings, and standing up counter-IED task forces. These efforts have been largely successful in mitigating and deterring attacks with vehicle bombs against US targets.

But, as recent events in India and the United States have shown, terrorists change tactics and can easily gain the press coverage they desire with a spectacular, well-planned small arms attack. The threat of terrorist attacks against soft targets remains a significant challenge. With the large availability of small arms in the United States, we must not lose sight of the potential for similar attacks here. This threat is of particular interest to military installations, as the Services are stretched thin for military police and security forces due to the high demand for law enforcement expertise in the Global War on Terror (GWOT).

At the intersection of small arms availability and security, the FBI found a nexus with a "new" form of terrorism in the Fort Dix plot, in which uniquely involved homegrown terrorists organized, trained, and equipped themselves on their own. They had no formal connection to other terrorist networks but were largely inspired by al Qaeda's ideology and call for jihad against the West.[6] "These homegrown terrorists can prove to be as dangerous as any known group, if not more so. They operate under the radar," commented FBI agent J.P. Weis.[7]

The FBI described the terrorists' efforts as indicative of a rise in small but sophisticated groups that operate autonomously from other established terrorist groups and that are inspired by internet propaganda and terrorist media releases.

How do we counter these new and evolving threats in an era of dwindling resources? We need to examine how we operate. The Joint Staff has made progress in a number of areas to assist the Services and combatant commands in improving FP preparedness. Many of these improvements require no additional resources.

First, vulnerability assessments are one of the most effective tools we have in bolstering our defensive posture against terrorism, but we have too many underway.

Two years ago, we thought that there were between 21 and 27 assessments underway; since then, we have discovered that there are more than 90 vulnerable assessment models underway across DOD. Why should base commanders have to endure similar vulnerability assessments conducted by different teams at sporadic times? We need to reduce the number of vulnerability assessments that base commanders have to endure. We need to establish a base standard, with modules added depending on command-emphasis issues.

Second, we need to do a better job of leveraging biometrically enabled tools, not just in the Central Command (CENTCOM) area of responsibility (AOR) but across all combatant commands.

We are working closely with the Biometrics Task Force to develop an overarching strategy for biometrics, as well as the follow-on DOD Instruction. We are also developing, in coordination with the Army, a draft Capstone concept of operations for expeditionary forensics. This project is the first step in our efforts to establish a coordinated effort to develop a robust integrated battlefield forensics capability for the warfighter.

Third, common access controls for DOD installations—a controversial issue across the Services—is another important capability that J-34 is currently working to solve.

We need to find a solution, beyond colored decals, that ensures robust access control while remaining feasible and affordable on a base-to-fort-to-post basis, particularly for co-use bases and installations.

Fourth, we need to do a better job with how we spend FP dollars. Integrated Unit, Base, and Installation Protection (IUBIP) is another major effort that will affect our overall base defensive posture.

In the biggest sense, the effort provides the business case and foundation for thinking about how DOD FP dollars will be spent as well as for ensuring that all equipment will be plug-and-play or interoperable across the Services. The effort is enormous and affects many diverse parts of DOD. In the end, we hope to have a menu of best-of-breed products based on field experience and of best business practices. With IUBIP, we are forming a common set of tailorable and scalable FP capabilities for the Joint Force in the future years of 2012–2024. Our focus is on recapitalizing resources and delivering vital capabilities to the warfighter based on a prioritized critical infrastructure framework.

Prediction: We Will Be Attacked in the Next 5 Years with WMD

Is the federal government, not just DOD, prepared for terrorist threats in a new century? Have we lost our way when it comes to deterrence? What does it mean to deter today? How do we deter nonstate versus state "bad actors"? In a recent *Joint Force Quarterly* article, ADM Mike Mullen notes that deterrence today is tougher and more complex than in the past.[8] In an era of dwindling resources, synchronization of the elements of national power to achieve desired outcomes or to compel our adversaries to choose alternate courses of action, particularly when it comes to deterring WMD, is sorely needed.

The recently published *National Defense Strategy* (June 2008) reminds us that we face a spectrum of challenges, including WMD.[9] Without question, disruptive technology from rogue nations as well as from former Soviet Union biological and chemical programs creates a potentially volatile and dangerous situation. Power formerly reserved for nation states now has the potential to fall into the hands of terrorists or radical individuals.

It remains questionable whether we can effectively deter individuals or groups from pursuing the power formerly reserved for nation states, particularly when such power could be concentrated in the hands of Islamic jihadists who are willing to die for their cause. In December 2008, a bipartisan commission reported that the United States will likely be attacked with nuclear or biological weapons in the next 5 years.[10]

The very threat of catastrophic terrorism should alter the way we think about roles, missions, and resources. Despite this, the Quadrennial Defense Review recommended 21 capability packages

but did not include consequence management or counter-WMD. As noted by ADM Mullen, "We have done precious little spadework to advance the theory of deterrence."[11] Indeed, since 9/11 we have heard a lot of rhetoric about the importance of being prepared for WMD, the most dangerous threat facing this nation; however, the reality remains that much work needs to be accomplished.

In a 2007 *Wall Street Journal* article, former Secretary of State Alexander Haig wrote: "On 9/11 the monster found us asleep at home and will continue to find us inadequately prepared unless we muster more strength and more wisdom. Unless we break the illusionary democratic mongering, inept handling of our military resources and self-defeating political debates, we are in danger of becoming our own worst enemy."[12] Collectively, we need to continue to challenge the old business processes and business models using good old American ingenuity to solve problems.

Commanders must make FP a priority, address their antiterrorism command and control structure, and appoint and empower a qualified Antiterrorism Officer.

On the one hand, the interagency partners have much to be proud of when it comes to crafting framework strategies that describe how the US government will respond to a range of WMD scenarios. On the other hand, the wide-ranging strategies argue for capabilities that, in the aggregate, do not equal comprehensive response solutions. Still maturing, the interagency effort has made slow but notable headway while tackling some tough issues. This process is ongoing and evolving.

Recognizing that deterrence may fail, it makes sense to dedicate a portion of our resources to craft a comprehensive response program as a hedge against a successful use of WMD by terrorists on our soil. The Katrina lessons underscore that failure to respond in a competent, efficient, and effective manner will undoubtedly have serious political consequences. A number of areas could use some additional work.

In the aftermath of the Oklahoma City bombing, Presidential Decision Directive 39 assigned specific responsibilities to the federal government partners, stating that "The United States shall give the highest priority to developing effective capabilities to detect, prevent, defeat and manage the consequences of nuclear, biological or chemical (NBC) materials or weapons use by terrorists." Now called "Combating Weapons of Mass Destruction," this policy statement was the foundation of the framework within which federal interagency partners planned and executed WMD operations.

Unfortunately, an unintended side effect of the community's thinking was that WMD consequence management became an exclusive responsibility of the Federal Emergency Management Agency (FEMA). Viewing consequence management as support to another federal agency, DOD developed an institutional bias regarding it. Why should DOD spend its limited resources on consequence management when it is the primary responsibility of another federal agency? I would offer two reasons.

First, consider incidents like Beirut and the Khobar Towers bombing, featuring the more nefarious forms of WMD. Do we really expect our federal partners to respond to WMD events on DOD installations? If yes, what capability and capacity do they have and how quickly can they get there?

Second, the National Military Strategy to Combat Weapons of Mass Destruction correctly notes that "we must possess the full range of operational capabilities to protect the United States, US military forces, and partners and allies from the threat or actual use of WMD."[13] Can we successfully deter the threat or actual use of WMD? Can we successfully preempt such an attempt? If not, have we balanced that risk against DOD's ability to respond? At what cost?

> "The most likely catastrophic threats to the US homeland—for example, that of a US city being poisoned or reduced to rubble by a terrorist attack—are more likely to emanate from failing states than from aggressor states. The kinds of capabilities needed to deal with these scenarios cannot be considered exotic distractions or temporary diversions."[14]
>
> —Secretary of Defense Robert M. Gates

With the stand-up of Northern Command (NORTHCOM), the recent assignment of the Chemical, Biological, Radiological/Nuclear, and Explosive (CBRNE) Consequence Management Response Force (CCMRF) package is a major step in developing a capability needed by the United States to respond to future attacks. Yet, as presently designed, there are growing pains and lessons to be learned as the model and CONOPS mature while conducted under various conditions during validation exercises.

Foremost, overcoming the challenges of time and distance under normal and adverse weather conditions will provide clearer insight to better integration of geographically dispersed units that will have to converge in the aftermath of a WMD event and function as a cohesive whole in a chaotic environment.

A section of the US-Mexico border fence near San Diego, California.

The growing levels of violence in Mexico point to an alarming trend that both threatens the sovereignty of the Mexican government and the security of American border states.

A response scenario, for example, could require these small units to integrate in New York City, with the reception, staging, onward movement, and integration (RSOI) location as La Guardia Airport. How would those units arrive from the 57 different sites, conduct RSOI, and then transit effectively across town to the incident site? The deployment and integration plans are in their infancy, and simply traveling across town could well be one of CCMRF's biggest challenges, followed by sustaining its capability to work in a hot zone without a designated replacement unit.

Recognizing that deterrence may fail, it makes sense to dedicate a portion of our resources to craft a comprehensive response program as a hedge against a successful use of WMD by terrorists on our soil.

CCMRF, still in its formative stages, has many challenges that lay ahead. The tactics, techniques, and procedures and the organization itself represent a best guess at what a WMD response might look like. The realities of today's operational environment are characterized by the potential proliferation of WMD, rapidly changing disruptive technologies, and catastrophic manmade and natural events. In an era of dwindling resources, the call has gone out for integration of the Reserve Components into a comprehensive WMD response. The geographic proximity and unique capabilities embedded in these components are vital to fill, and need to complement, the gaps in civil response assets throughout the United States.

When we look for sourcing solutions, we rarely look beyond Title 10 active-duty forces.[15] Arguably, the Request for Forces process needs to provide a full spectrum of options, including all the Reserve Components, with geographically dispersed Reserve Component and National Guard units in either Title 10 or Title 32 roles.[16] Frankly, the American people do not know the difference between the various Service components; all they care about is how quickly the

Services will respond and that they bring the right capability. We need to define the requirement, match it with the appropriate capability, and then fully examine what status provides commanders with the most operational flexibility. Over time, we need to examine integrated Active and Reserve Component units that have full-time Active Guard/Reserve (AGR) or Title 10 core units that are rapidly augmented with detachments, teams, sections, and platoons from across the Reserve Components because of their unique geographic proximity.

A Threat Close to Home: Narcoterrorism

Another area we need to examine is the threat of narcoterrorism. The nexus of drug money and terrorists is a major concern. The growing levels of violence in Mexico point to a growing and alarming trend that both threatens the sovereignty of the Mexican government and the security of American border states. In 2008, the number of deaths related to drug violence more than doubled to nearly 5,400 people in Mexico, with more than 700 killed in Tijuana alone—a major city frequented by American tourists and Servicemen on the border with California.[17] More than 500 Mexican law enforcement officers and soldiers have been killed in the last 2 years, since the Mexican government declared war on illegal drug trafficking.[18]

The spread of lawlessness in Mexico can only contribute to border-region instability and provide a border safe haven for those who wish the United States harm. US security agencies are increasingly focused on the possibility of terrorists using the US–Mexican border as a preferred transit point. In recent years, the CIA has become increasingly alarmed by the possibility that terrorist groups like Hezbollah and al Qaeda will use the Mexican border to gain easy access to the United States.

The CIA's Counter Terrorism Center wrote a 2004 threat paper noting that

> Many alien smuggling networks that facilitate the movement of non-Mexicans have established links to Muslim communities in Mexico. … Non-Mexicans often are more difficult to intercept because they typically pay high-end smugglers a large sum of money to efficiently assist them across the border, rather than haphazardly traverse it on their own.[19]

The growing nexus of crime and terrorism requires a cohesive and seamless federal law enforcement response. Criminals and terrorists attempt to operate in the gray areas produced by bureaucracy, corruption, and legal loopholes. DOD, for instance, lacks a singular executive agent with the vested authority to establish DOD-wide law enforcement policy, to integrate and synchronize DOD law enforcement assets in support of GWOT, and to improve DOD's interagency coordination within the federal law enforcement enterprise. DOD must establish a Principal Staff Assistant (PSA) for law enforcement to fully capitalize on DOD law enforcement expertise in support of the warfighter and improve support to law enforcement as a new element of national power, as outlined in the National Strategy for Combating Terrorism.

US security agencies are increasingly focused on the possibility of terrorists using the US–Mexican border as a preferred transit point. In recent years, the CIA has become increasingly alarmed by the possibility that terrorist groups like Hezbollah and al Qaeda will use the Mexican border to gain easy access to the United States.

Leveraging the new elements of national power, we can begin to get after the terrorists' source of funding. A Deputy Secretary of Defense memo dated 26 April 2006, provides DOD guidance for using counternarcoterrorism (CN) resources to support law enforcement agencies (LEA) conducting counterterrorism activities for fiscal years 2006 and 2007. The memo addresses the growing nexus of drug trafficking organizations and terrorists to smuggle money, people, information, weapons, and substances. This authority was not significantly used but was extended for 2008 and 2009.

DOD needs to review relevant CN policies and to take the following priority actions to address this increasingly volatile threat. The CN Central Transfer Account (CTA) is a single budget line that accounts for all associated CN resources, providing approximately $950 million annually. The Office of the Under Secretary of Defense for Policy (OUSD-P) manages distribution and provides flexibility for CN programs by reprogramming funds to address emerging needs. DOD should examine the existing interagency relationships and expand the range of activity allowed under CTA budgetary authority as well as funding for narcoterrorism applications.

Finally, NORTHCOM's Joint Task Force North (JTF-N) is a JTF HQ designed to facilitate DOD support to LEA efforts to reduce the amount of drugs entering the United States. Authorities are derived from a series of acts and policies, culminating in

a March 2004 NORTHCOM execute order. JTF-N coordinates support, shares information with LEAs, and analyzes threats in the "approaches." JTF-N does not arrest, apprehend, or detain; conduct searches or seizures; collect or retain intelligence on US persons; or direct operations of LEAs. Based on the Joint Interagency Task Force (JIATF) South model, we should examine expanding JTF-N, which operates primarily under Title 10 restrictions. Migrating to the JIATF model is a practical attempt to leverage the wider range of statutory authority that our interagency partners bring to the table, specifically that of the Coast Guard (US Code 14), the Drug Enforcement Agency (US Code 21), and the National Guard (US Code 32).

The Way Ahead

> The missed opportunities to thwart the 9/11 plot were also symptoms of a broader inability to adapt the way the government manages problems to the new challenges of the twenty-first century.[20]
>
> —9/11 Commission Report

The Joint Staff is now undergoing the third and final phase of the Beyond Goldwater-Nichols multiyear effort to explore the next era of defense reform. Its primary goal is to develop an integrated set of practical and actionable recommended reforms for organizing both the US military and national security apparatus to meet 21st century challenges. Much remains to be done to protect the homeland and its military forces from a broad range of threats, particularly WMD, through homeland defense programs, antiterrorism and FP policy, and military support to states and to civilian responders.

DOD and its interagency partners must focus on the "seams" in federal policy, particularly in combating WMD. Along these seams are transnational terrorist groups, including narcoterrorists, who swim in the gray AOR among DOD and the Department of Homeland Security, the Department of Justice, and other agencies. The challenge is for interagency partners to use collective action to shrink the gray areas and to ensure that interagency capabilities are maintained to counter growing FP, WMD, and narcoterrorism threats. The challenges are great, but the costs of failure are greater.

1 *Joint Publication 3-27*, Homeland Defense, 12 July 2007. Available at: http://www.dtic.mil/doctrine/jel/new_pubs/jp3_27.pdf

2 Landon Lecture (Kansas State University, Manhattan, Kansas). Remarks as delivered by Secretary of Defense Robert M. Gates, 26 November 2007.

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

4 Gingrich, Newt. "Lessons from the First Five Years of War: Where Do We Go from Here?" American Enterprise Institute Online [speech], 11 September 2006. Available at: http://www.aei.org/publications/pubID.24891,filter.all/pub_detail.asp

5 "U.S. National Security System Deemed 'Fundamentally at Risk.'" CNN, 3 December 2008. Available at: http://cnnwire.blogs.cnn.com/2008/12/03/us-national-security-system-deemed-fundamentally-at-risk/

6 Alfano, Sean. "Fort Dix Plot Called 'New' Form of Terror." CBS News, 9 May 2007. Available at: http://www.cbsnews.com/stories/2007/05/09/terror/main2778068.shtml

7 Ibid.

8 Mullen, Michael. "From the Chairman: It's Time for a New Deterrence Model." *Joint Forces Quarterly,* 4th quarter 2008. Available at: http://www.ndu.edu/inss/Press/jfq_pages/editions/i51/5.pdf

9 Department of Defense. *National Defense Strategy,* June 2008. Available at: http://www.defenselink.mil/news/2008%20national%20defense%20strategy.pdf

10 Hess, Pamela. "Panel: Bio Attack Likely in Next 5 Years." Associated Press, 2 December 2, 2008.

11 Supra 8

12 Haig, Alexander M., Jr. "Our Own Worst Enemy." *Wall Street Journal,* 10 July 2007. Available at: http://online.wsj.com/article/SB118403572723161796.html?mod=opinion_main_commentaries

13 Department of Defense. *National Military Strategy to Combat Weapons of Mass Destruction,* 13 February 2006. Available at: http://www.defenselink.mil/pdf/NMS-CWMD2006.pdf

14 Gates, Robert M. "A Balanced Strategy: Reprogramming the Pentagon for a New Age," *Foreign Affairs,* January/February 2009. Available at: http://www.foreignaffairs.org/20090101faessay88103/robert-m-gates/how-to-reprogram-the-pentagon.html

15 US Code, Title 10, Armed Forces. Available at: http://uscode.house.gov/download/title_10.shtml

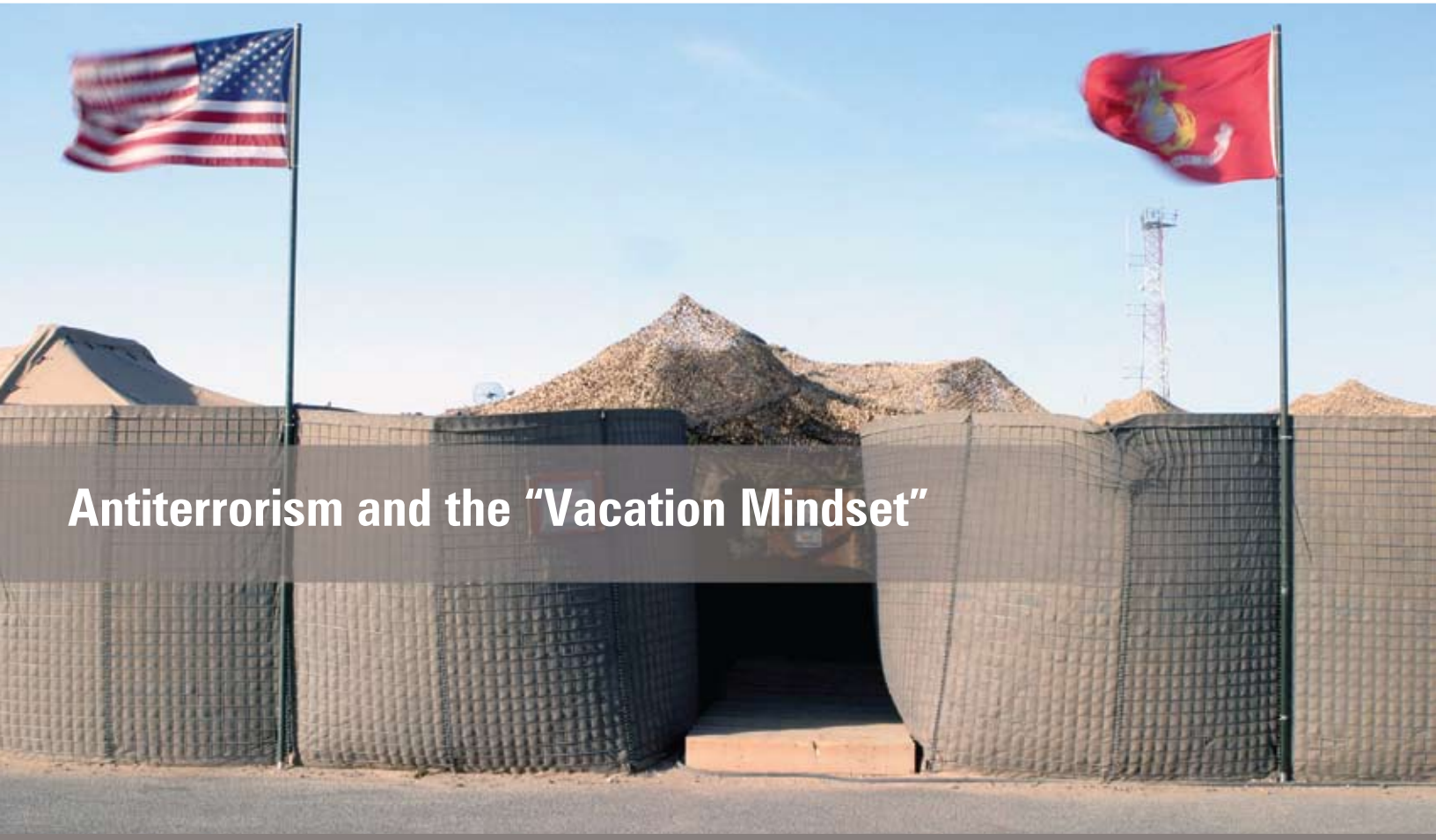
16 US Code, Title 32, National Guard. Available at: http://uscode.house.gov/pdf/2004/2004usc32.pdf

17 Diaz, Lizbeth. "Indiscriminate Drug Killings Sow Terror in Mexico." Reuters, 9 December 2008. Available at: http://www.reuters.com/article/worldnews/idUSTRE4B85OY20081209?pageNumber=1&virtualBrandChannel=10341

18 Ellingwood, Ken. "Two Top State Police Officers Slain in Mexico." *Los Angeles Times,* 4 November 2008. Available at: http://www.latimes.com/news/nationworld/world/la-fg-mexico4-2008nov04,0,6550328.story

19 Gato, Pablo, & Robert Windrem. "Hizballah Builds a Western Base." Telemundo/MSNBC, 9 May 2007. Available at: http://www.msnbc.msn.com/id/17874369/

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



Antiterrorism and the "Vacation Mindset"

By MSG Chuck Jackson, US Army, Special Forces and Ben Nerud, Defense Threat Reduction Agency

Since 9/11, there has been unprecedented emphasis on protecting critical assets from terrorist attacks. This increased emphasis resulted in the formation of a new cabinet-level department, restructuring of our intelligence apparatus, and the creation of new laws, all meant to improve the ability of the United States to protect itself against terrorist attacks. The United States has spent billions of dollars on security systems, employed thousands of people, and dedicated countless hours to developing and implementing programs to protect important assets. Yet numerous reports suggest we are becoming increasingly vulnerable to terrorist attacks.

The sine wave phenomenon of security is often credited as a contributing factor to this increasing vulnerability. The sine wave theory postulates security dramatically increases because of some catalyst—either an attack or the threat of an attack. Later, this security is reduced, eventually falling to a level that existed prior to the catalyst occurring. A good theory, and perhaps valid. However, we become vulnerable to an attack long before any of this theory comes to fruition. We become vulnerable as soon as we allow our protective programs to go on "vacation."

Laurence Gonzales, a researcher and author of *Deep Survival,* published a column in the June issue of *National Geographic Adventure* magazine titled, "The Dangers of the Vacation Mindset."[1] This article describes man's unconscious tendency to conclude that his little corner of the world is safe:

> As human beings, we have big brains that are capable of complex rational thought. But we're also saddled with a lot of hereditary neural equipment. One of those legacy systems tells us whether our behavior is good for our survival. For example, if we do something that rewards us with food or a pleasant feeling, we're far more likely to do it again. We don't have to think about it. It's in our animal nature. In a modern technical culture we're rewarded almost all the time, no matter what dumb things we do. We're clothed, fed, and sheltered, and don't even think about predators. If we need more rewards, we can just reach out and grab them from the refrigerator. The animal part of our brain takes this as clear evidence that our strategy is a good one.

The "vacation mindset" begins with the unintended acceptance of more and more risk, usually in an effort to ease restrictions or to reduce costs; examples of this acceptance include the reliance on random antiterrorism measures (RAMs) instead of adherence to baseline standards. This acceptance generates increased reliance on technology to perform functions that are better suited to be performed by people (i.e., replacing patrols with CCTV or static guards with intrusion detection systems). These risk management decisions are viable, but pushing the boundaries of acceptable risk does nothing to improve our security. As we begin accepting more and more risk and nothing happens, our strategy seems effective and the vacation mindset sets in.

The "vacation mindset" begins with the unintended acceptance of more risk, in an effort to ease restrictions or to reduce costs; examples include the reliance on random antiterrorism measures instead of adherence to baseline standards. This acceptance generates increased reliance on technology to perform functions that are better suited to people (i.e., replacing patrols with CCTV or static guards with intrusion detection systems). As we begin accepting more and more risk and nothing happens, our strategy seems effective and the vacation mindset sets in.

Reliance on technology is increasingly becoming the answer to many security issues. From risk management software to Smart Gates, technology is touted as the solution to our security needs and is often cited as the only means of reducing risk. This overreliance on technology provides a false sense of security. Terrorists invest significant resources learning how to defeat technological security measures, and, in fact, they defeat such measures every day. Dr. Brian A. Jackson, Associate Director, Homeland Security Program, RAND Infrastructure, Safety, and Environment, discussed the interaction between the development and implementation of countermeasures and the terrorist's efforts to defeat them in "Breaching the Fortress Wall: Understanding Terrorist Efforts to Overcome Defensive Technologies"[2]:

> Given the potential for defensive technologies to constrain the capabilities of terrorist groups and limit their operational freedom, these organizations are acutely aware of government efforts to deploy such countermeasures and actively seek ways to evade or counteract them. This measure-countermeasure, move-countermove dynamic is inherent in contests between organizations and, to the extent that the terrorists' efforts are successful, can significantly reduce or eliminate the value of defensive technologies.

The threat has not abated. In a video address in May 2007, Adam Gadahn, aka Azzam the American, stated that al Qaeda intended to attack Americans at home and abroad. More recently, Ayman al-Zawahari answered questions from jihadist forum participants, these responses included many thinly veiled threats of increased terrorist attacks. Recent publications by many government entities have identified al Qaeda as one of the greatest threats to the United States. The only possible conclusion from the data is the intention of attacking US assets, both at home and abroad, is still foremost in the terrorists' minds.

Antiterrorism programs within DOD are primarily passive programs, that is, they stop an attack. Proactive measures are talked about but are rarely implemented or designed to influence the terrorist operational cycle. The result is a stagnant protective program. Yes, we are developing new technology and methods, but those methods merely enhance the same system. They make it a little more efficient. Passive security measures might postpone a terrorist attack, but may not deter it. Furthermore, passive security measures are directly influenced by the vacation mindset, stagnating the security posture of installations and decreasing the effectiveness of the system. Essentially, the attitude becomes "if it works, don't fix it!" Unfortunately, we are faced with a thinking adversary. An analysis of the terrorist attack cycle reveals the dangers of stagnant security programs and the vacation mindset.

The Terrorist Attack Cycle

Initial target selection is based on the terrorist organization's doctrine. In the case of al Qaeda, the ultimate objective is establishing an Islamic state under the rule of a Caliph. What does this mean to us? Targets are not chosen at random. Once a target is selected, it is evaluated to determine the reaction, symbolism, economic impact, and casualties that would be associated with an attack on the target. An additional aspect of the target selection process includes a self-assessment of the terrorist organization's capability to perform the attack. The

Replacing patrols with CCTV or static guards with intrusion detection systems are examples of technology used to perform functions that are better suited to people. This overreliance on technology provides a false sense of security. Terrorists invest significant resources learning how to defeat technological security measures, and, in fact, they defeat such measures every day.

vacation mindset aids the terrorist organization in its capability analysis.

Initial target selection and the beginning of attack planning can take place thousands of miles away, with a laptop computer with an Internet connection. Information placed on the Web to improve efficiency or to enhance business practices may provide exploitable data and could be used to place an asset on a targeting list. A recent technological advancement, for example, is the use of video to provide virtual tours of installations and assets for new personnel and visitors. A simple "welcome to our installation" video posted on the Web might begin by showing a car driving through the main gate, including several wide-angle shots of the gate. Views of barracks, housing, and primary mission assets of the installation complete the virtual tour. From this video, the terrorist can identify access-control procedures, physical security equipment, gate design, standoff, and locations of potential targets. This information allows the terrorist organization to determine whether it has the capability to attack the installation. This type of activity represents the "vacation mindset." Actions that would have been unthinkable immediately after 9/11 are now becoming commonplace.

Understanding targeting preferences and selection processes is vital to proactive security programs. With this understanding comes the ability to limit the availability of relevant open source information that could aid an adversary in selecting a target.

A terrorist organization must conduct surveillance to target an asset. Terrorists performing surveillance are trained to observe the subtleties of the security system, and it is the subtleties that will make the difference. While conducting surveillance on an entry control point, for example, a terrorist observes random cars being thoroughly searched using military working dogs. He watches this for an hour and then the search team leaves. Once the search team departs, the entry control point resumes its normal operation, which is identical to the operations prior to the search team arriving. What has he identified? If military working dogs are observed, wait one hour and continue with the attack plan.

The vacation mindset exists in the belief that RAMs are sufficient to influence an adversary and to deter the attack. In reality, such actions are nothing more than perceived behavioral control.

A more proactive approach is to deny the enemy from observing searches altogether by concealing

security procedures. If the adversary cannot view search procedures, they cannot develop a course of action to defeat them. An additional benefit of this type of proactive countermeasure is it increases the length of time terrorists must perform surveillance. Increased time provides increased opportunity to detect and neutralize or exploit the terrorist cell.

Using target selection information and data collected during surveillance, terrorist organizations develop an attack course of action and procure the required weapons. After performing surveillance, the terrorist organization determines whether it is capable, for example, of attacking the base using a vehicle-borne improvised explosive device (VBIED). This course of action is developed based on the physical and behavioral vulnerabilities witnessed during surveillance of the gate. Through surveillance, the terrorist knows he can place a large device in the trunk of a car, the size determined by the availability of either improvised or conventional explosives, and drive it on base. With the data available, this course of action provides the terrorist with reasonable assurance that he will be able to exploit the access-control system and deliver the weapon to the identified target.

This course of action is viable because the protective system is stagnant. The terrorist knows the security system, both physical and procedural, will not change; that RAMs are performed for short periods, procedures are implemented with the caveat that they cause the least amount of inconvenience; and that staffing will likely never increase. Data collected while performing surveillance months earlier is just as valid on the day of the attack as it was on the day collected. Adaptive and changing security postures, active surveillance denial and detection, and the denial of critical targeting information to the terrorist improve the protection of the target and increase the risk of failure for the terrorist.

Attack courses of action can be developed because of the nonactive nature of countermeasures designed to stop or respond to the attack. Traditional countermeasures perform much like a zone defense in which no one moves until after the ball is thrown. This is the epitome of the vacation mindset in that they fail to recognize the danger of stagnant security programs and the adaptability and innovation of a thinking adversary. Proactive programs question the efficacy of defensive systems; incorporate lessons learned from previous attacks; and, perhaps most importantly, study the adversary and adapt to the terrorists' changing strategy and tactics.

We must transition our protective programs from reactive measures to proactive protection; however, proactive measures can only be implemented when the vacation mindset is changed. Technology will advance our efforts only so far, and our adversary is

STEPS TO ELIMINATING THE VACATION MINDSET

1 Establish a standard-based, zero-tolerance compliance strategy for all security programs.

2 Eliminate the ability for individuals or organizations to arbitrarily accept risk.

3 Develop proactive measures designed to reduce risk by influencing the threat.

Combine all three methods, taking the best from each and creating a holistic approach. Designing our security systems to allow each of these methods to support the others offers the best chance of achieving complete protection.

dedicated to defeating that technology. Technology must be combined with proactive strategies, and those strategies cannot go on vacation.

Eliminating the Vacation Mindset

Several methods can reduce the likelihood of onset of the vacation mindset. First, establish a standard-based, zero-tolerance compliance strategy for all security programs. This strategy will initially result in dramatically improved security, but unless the standards change frequently, protective programs will become stagnant. As the programs stagnate, terrorist organizations will learn how to defeat them.

Second, eliminate the ability for individuals or organizations to arbitrarily accept risk. Each organization would be required to reduce risk to a level that is as low as can reasonably be achieved. This strategy is not risk avoidance; rather, all risk must be addressed and measures must be implemented to reduce vulnerability, criticality, or the threat itself. This strategy eliminates the often-cited excuse of lack of resources and requires decisionmakers to identify compensatory means within their capability to reduce risk.

Third, develop proactive measures designed to reduce risk by influencing the threat. This method requires extensive knowledge of the tactics, techniques, and procedures used by our adversaries and the development of specific, focused measures to counter them. Our protective systems should incorporate proactive measures designed to influence the terrorists' behavior, capability, and ability to develop courses of action. The ultimate goal of proactive antiterrorism programs is to deny terrorists the ability to operate in an area. If terrorists attempt to operate in this environment, the program should be capable of identifying the activity, implementing measures to deny the freedom to operate, and creating a starting point for counterterrorism efforts.

The development of proactive countermeasures begins with determining which aspects of the terrorist targeting process are vulnerable to denial or disruption. This examination is accomplished by integrating intelligence preparation of the operating environment into our planning process and will identify those requirements that are essential to a terrorist attack and susceptible to defeat mechanisms. Once we have identified the vulnerable portions of the terrorist attack cycle, we can design proactive countermeasures to disrupt or deny those requirements. Our security design and standard defense-in-depth countermeasures should limit the availability of information, deny the capability to perform surveillance, reduce the ability to establish cover, and limit the available courses of action.

Perhaps the most reasonable action is to combine all three methods, taking the best from each and creating a holistic approach, backed by standards and requirements, to reduce susceptibility to terrorist attacks. Antiterrorism programs have the ability to integrate both defensive and offensive tactics. Designing our security systems to allow each of these methods to support the others offers the best chance of achieving complete protection.

Conclusions

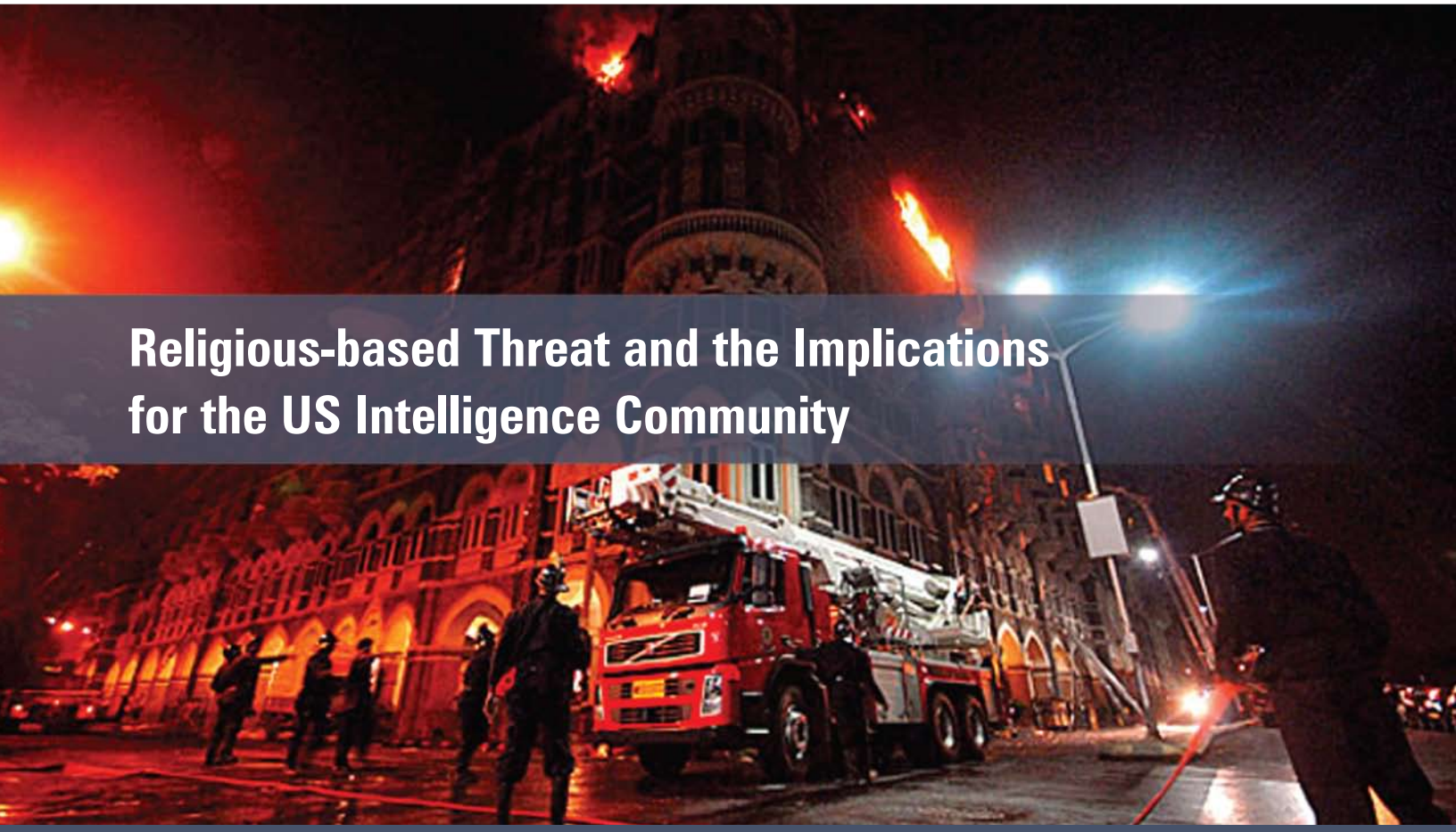
This article may be interpreted as advocating either more security or increased emphasis on antiterrorism programs. Quite the contrary, this article is an attempt to call attention to the stagnancy of our current programs; the almost constant infusion of additional "more of the same" countermeasures; and our reliance, perhaps overreliance, on technology to provide security. When the purpose of antiterrorism programs and, especially, the countermeasures implemented are reevaluated, it seems possible to do more with less because our defensive strategies will shift from passive to proactive protection. No greater deterrent can be achieved than an antiterrorism program that not only defends our installations from an attack but also creates an environment in which terrorists are prevented from even planning the attack.

---

1. Gonzales, Laurence. "The Dangers of the Vacation Mindset," *National Geographic Adventure Magazine,* June 2008. Available at http://ngadventure.typepad.com/blog/2008/05/deep-survival-b.html
2. Jackson, Brian A., Peter Chalk, R. Kim Cragin, Bruce Newsome, John V. Parachini, William Rosenau, Erin M. Simpson, Melanie Sisson, and Donald Temple. *Breaching the Fortress Wall: Understanding Terrorist Efforts to Overcome Defensive Technologies,* RAND Corporation, 2007. Available at http://www.rand.org/pubs/monographs/2007/RAND_MG481.pdf


Coalition Warfare: One TEAM - One FIGHT
NEVER FORGET
WE are at WAR!
on TERRORISM
US ARMY TRADOC
KNOW THE ENEMY
THREAT'S TERRORISM TEAM
TRISA
Use the Army TRADOC G2
Terrorism Handbooks
No.1
TSP
No.1.07
TRISA
US Army
TRADOC Intelligence Support Activity
TRISA WOT Poster No. TG Spec 01A-09
https://dcsint-threats.leavenworth.army.mil
(Source: DOD, Defense Imagery)

Religious-based Threat and the Implications for the US Intelligence Community



On 26 November 2008 in Mumbai, India, a Pakistan-based Islamic terrorist group carried out systematic attacks across the entire city. The assault lasted three days, and left more than 100 dead.

What is called "foreknowledge" cannot be elicited from spirits, nor from gods, nor by analogy with past events, nor from calculations. It must be obtained from the men who know the enemy. —Sun Tzu

For many years, the United States has confronted a growing threat from jihadist organizations. Americans did not acquire a vivid awareness of this threat until the attacks of September 11, 2001. In the past, America's military, law enforcement, and intelligence communities have risen to the challenges posed by new threats, however daunting. We have every reason to think that they can rise to meet this new challenge.

To do so, we must acquire a clear understanding of the complexities and the realities of the jihadist enemy. Because there is still not a common understanding of this reality, we continue to grapple with how best to use our assets to protect American lives and the American way of life. Political correctness has paralyzed the effective development of strategies to confront jihadist terrorism while jihadists have been able to leverage their small numbers to significant advantage.

The mindset of the American intelligence community (IC) still reflects its Cold War founding. In the Cold War, America dealt with a predictable threat assessed in terms of an understood force structure measured in conventional terms of aircraft, ships, or vehicles. Published doctrines and asset deployments of our Cold War enemies were available for study. At that time, the IC focused on sovereign countries with fixed borders and military assets; changes were observable and warned of future intent.

Today's threat of global terrorism confronts America with jihadist and dawa organizations operating outside sovereign terrain. The word *jihad* refers to an active military struggle; *dawa* refers to the invitation to accept Islam, the rejection of which justifies jihad.[1]

Terrorist organizations are diverse and active throughout the world, and their methods vary. Jihadists have no uniforms, standardized systems, military bases, or headquarters. Doctrines with fixed, supposedly divinely ordained requirements motivate group members to fight infidels zealously for the

revival of the Muslim caliphate and the restoration of Islamic law *(sharia)*. The IC must adapt to a determined foe that does not act in conformity with previous models of enemy behavior.

Another challenge for the IC is to remain in constant operational vigilance. The Cold War adversary was available for intelligence study in the absence of direct conflict, which offered the luxury of time to prepare intelligence assessments and analysis. Today's groups of international terrorists are in a constant state of war with America and can strike anywhere, at any time, with any tactic.

unprecedented way.[3] Collecting intelligence on this threat is unprecedented in difficulty, and jihadist groups have shown great ingenuity in responding to known American technological methods of intelligence collection. Successful communication intercepts provide limited information, with more questions than answers.

Human intelligence with a direct link to the personalities and the ideas of an organization is the best way to discover an adversary's intended actions; however, gathering human intelligence against global jihad organizations is fraught with problems.

The mindset of the American intelligence community still reflects its Cold War founding. In the Cold War, the IC focused on sovereign countries with fixed borders and military assets; changes were observable and warned of future intent.

Today's America is confronted with organizations operating outside sovereign terrain. Jihadists have no uniforms, standardized systems, military bases, or headquarters. The IC must adapt to a foe that does not act in conformity with previous models of enemy behavior.

Religious and Ideological Motives

The jihadist enemy's desired end state is the conversion or submission of the West to Islam, and divinely mandated doctrines provide an indefinite timeline. Yet dedicated groups in pursuit of improbable ends may do incalculable damage, even if their ultimate goals are not achieved.

Analysts often dismiss the jihadi's avowed aim, along with jihad ideology, because of its sheer improbability. They often insist that stated jihad aims are merely expressive of other, more practical goals (e.g., reform of autocratic Arab regimes in the Middle East). Furthermore, because the Muslim world currently lacks a coherent central leadership, jihadist and dawa groups compete for power and leadership in a growing jihad movement, giving the illusion of an enemy in disarray.[2]

America denies itself a clear understanding of the enemy because it refuses to focus on the enemy's *stated threat doctrine*. This denial keeps the IC from developing a coherent understanding of the doctrines that unify otherwise diverse jihadist elements. When there was a single adversary, the Soviet Union, supporting regional conflicts for its own interests, the IC could deal with threats as they developed. In contrast, the threat of global jihad demands knowledge of local conflicts throughout the world and their interconnections.

In the aftermath of 9/11, the IC must work cooperatively, sharing information in an

Penetration of religious cultures constructed along close familial and personal ties is nearly impossible, minimizing the ability to procure human intelligence.

In earlier conflicts, a great deal of information about the enemy was available from open sources such as the media and academia, but for jihadist adversaries, the best sources of information are often doctrinal texts of sharia and jihad that are available in English. Although many of these sources are readily available in mosque-associated bookstores and on the Internet, analysts often choose not to incorporate these texts into their analytical models. Hence, the media and other institutions lack detailed information about the enemy and instead rely on often misleading accounts in the popular press. This further convolutes the products of analysts who are overwhelmed by problems they deny themselves the capacity to understand.[4]

Although jihadists continuously plan attacks, it is not clear where or how they plan or with what capabilities. Even if the threat emanates from a country such as Iran, ascertaining intent is difficult in such closed societies with relatively small, discrete leadership circles. Such was the case with the faulty assessments of Saddam Hussein's Iraq.

Our first task as analysts is to reach an understanding of this ideology, despite strong cultural reluctance within the IC and American society in general to probe or to suspect religious beliefs. Yet the jihadist adversary is essentially religious and derives

validity and credibility from the doctrinal teachings of orthodox Islamic law and, particularly, from the law of jihad. Fears of being politically incorrect, of appearing bigoted or offensive in any respect, have compromised the analytical processes associated with threat doctrine development.

Jihadist Threat Doctrine

Jihad is a religious-based, imperialist, military-political ideology that requires adherents to expand Muslim influence throughout the world through persuasion or violence, leaving the followers of jihad in a permanent state of conflict with the world. Jihad is hostile toward any entity not submitting to Islam's perceived superiority.

There is no reason to believe that most of the 1.2 billion Muslims in the world adhere to the militant jihadist narrative as America's enemies, and many Muslims have chosen to limit the meaning of jihad to their own internal spiritual struggles. Significantly, there is no reason to think that the Muslim understanding of jihad is static. Those who now view jihad as an internal struggle may, in the future, change their minds. Likewise, some few who follow the orthodox view of jihad as literal war may also change

Doctrinal Basis of Jihad

Jihadists rely on specific passages of the Koran for the doctrinal bases of their actions, including a few of these passages (emphasis added):

Remember thy Lord inspired the angels with the message: "I am with you: give firmness to the Believers: I will instill terror into the hearts *of the Unbelievers:* Smite ye above their necks *and smite all their fingertips off them. —Koran 8:12*

And those of the People of the Book *who aided them, Allah did take them down from their strongholds and* cast terror into their hearts*, so that some ye slew, and some ye made prisoners. And he made you heirs of their lands, their houses, and their goods,* and of a land which ye had not frequented (before). *And Allah has power over all things. —Koran 33:26–27*

Let not the unbelievers think that they can get the better (of the Godly): they will never frustrate them. Against them make ready your strength of the utmost of your power, including steeds of war to strike terror into (the hearts of) *the enemies of Allah and your enemies,* and others besides, whom ye may not know, but whom Allah doth know."
—Koran 8:56–60

Soon shall We cast terror into the hearts *of the Unbelievers. —Koran 3:151*

Fighting *is prescribed for you, and ye dislike it. But it is possible that ye dislike a thing which is good for you, and that ye love a thing which is bad for you. But Allah knoweth, and ye know not.*
—Koran 2:216

But when the forbidden months are past, then fight *and slay the pagans wherever ye find them, and seize them and beleaguer them, and lie in wait for them* in every stratagem of war; *but if they repent, and establish regular prayers and practice regular charity, then open the way for them. —Koran 9:5*

Fight *those who believe not in Allah nor the Last Day, nor hold that forbidden which hath been forbidden by Allah and His Apostle, nor acknowledge the religion of truth,* even if they are of the people of the Book, *until they pay the jizya with willing* submission, and feel themselves subdued. *—Koran 9:29*

Analysis of the threat doctrine provides an understanding of what is important to the enemy. The enemy's values and objectives present themselves for analysis and can be integrated into a larger cultural, political, and ethnic framework. Seven years after 9/11, and 26 years after the Hezbollah attack on the Marine barracks in Beirut, Lebanon, we still do not have a tangible baseline for analysts and policymakers. The result is a mishmash of competing paradigms that operate at varying levels of understanding of the threat doctrine, all filtered though wishful thinking that is often at variance with reality.

their minds.[5] Much depends on Western response to jihad provocations. Western weakness, for example, may make "moderate" Muslims believe that jihadists are the wave of the future.

Even if these moderate practitioners are the majority of all Muslims, they do not have the support of the scriptural or legal traditions as taught in the most powerful centers of Islamic learning in the modern world. In the war of ideas in the Muslim world, the jihadist has orthodoxy on his side. We must understand this fact, especially because in many places where Islamic law is either dominant or influential, to depart publicly from orthodox teachings can be dangerous and even deadly.[6]

Americans must see jihad as jihadists see it. To accurately attack the jihadists' will, it is necessary to understand the source of their will: a doctrinal reading of Islamic writings, the example of Muhammad, and an apocalyptic reading of the present. Because jihadists clearly describe Islamic law as the doctrinal basis for their actions, that law becomes the enemy's threat doctrine and a mandatory object for our analysis.

Understanding this threat means understanding that Islamic terrorists derive their fighting passion from a faith subordinate to a divine law requiring jihad until the world is brought under the *Dar al Islam* and from a sense that now, after almost 1,500 years, the time has come for this destiny to be fulfilled. This apocalyptic vision is inspired by both the humiliations of and the potential opened up by technological globalization.

Americans must see jihad as jihadists see it. To accurately attack the jihadists' will, it is necessary to understand the source of their will: a doctrinal reading of Islamic writings, the example of Muhammad, and an apocalyptic reading of the present. Because jihadists clearly describe Islamic law as the doctrinal basis for their actions, *that law* becomes the enemy's threat doctrine and a mandatory object for our analysis. Importantly, this remains true even if the jihadists are wrong about their claims with regard to Islam. In matters apocalyptic, *wrong* does not mean inconsequential.

The jihadist is who he says he is and should be evaluated on that basis. Understanding him requires reading his sources with unconstrained perception of his values and objectives.[7] Analysts also need to go directly to the Koran, specifically to the passages that the enemy expressly relies on to provide the doctrinal basis for his actions (see box, "Doctrinal Basis for Jihad").

The Koran's message to Muslims in these passages is that it is pious behavior to wage war in the name of Allah against non-Muslims. Most of the more violent passages in the Koran, moreover, have greater standing in Islam because of the concept of abrogation.

This concept states that verses revealed later in Muhammad's life abrogate or replace earlier contradictory or variant verses. Thus, the chronologically later violent verses cancel earlier peaceful passages. Moreover, because the "time" has come, these verses take on even greater force. Despite the unlikely prospect of victory, which has in the past depressed such ambitions, jihadi apocalyptic beliefs create such a sense of urgency that even suicidal strategies seem compelling.

Because the IC lacks understanding of these principles and dynamics, the IC cannot correctly interpret the enemy's intentions or actions, or even its plainly stated objectives.[8] As Malik states (emphasis added): "*TERROR* struck into the hearts of the enemies is not only a means; *it is an end in itself.* Once a condition of terror into the opponent's heart is obtained, hardly anything is left to be achieved. It is the point where the means and the end meet and merge. *TERROR is not a means of imposing decision upon the enemy; it is the decision we wish to impose upon him.*"[9]

In addition to problems understanding jihadi warfare, IC has difficulty grasping the "civic" dimension of jihad. Because open warfare is impossible at this early stage (as evidenced by the disastrous consequences of 9/11 for the millennial rule of the Taliban in Afghanistan), a preparatory stage of infiltration of targets is necessary.

The IC needs to become familiar with Islamic principles of *taqiyya, kitman,* and slander. Taqiyya and kitman are Koran-based concepts of dissimulation, including deception by omission (i.e., deliberately leaving out key points to mislead and confuse your enemy). Slander, meaning that a Muslim is forbidden to give information that may incriminate or harm another Muslim, is prohibited in the teachings of Muhammad.[10]

Systematic lying and distortion to the targeted enemy are standard tactics for the jihadists. These tactics allow for the dissemination of two simultaneous messages, one delivered to infidels and a different, parallel message sent to the Muslim world. A classic example was the public statements of Yasser Arafat in English talking about his desire for peace and his calls for jihad and violence to his constituency in Arabic.[11]

The Islamic concept of slander can have profound implications for law enforcement and investigative professionals working within Muslim communities. If an FBI agent performs outreach in the Islamic community, he will operate at whatever level of understanding he has. The imam or the leaders of the community may choose to deceive or to confuse the agent with a minimum of information.

The Muslim Brotherhood disavows violence to Westerners while praising and extolling the use of violence by jihadists when speaking with Muslim audiences. Deliberate and systematic deception and disinformation must be considered standard jihadist tactics. These tactics need to be understood in the framework of an enemy who wants opponents to relax, to lower their defenses, and to suffer defeat without a fight.

The Muslim Brotherhood (MB), for example, engages in this tactic, discussing issues in ways that are pleasing to Western ears. The MB disavows violence to Westerners while praising and extolling the use of violence by jihadists when speaking with Muslim audiences. The MB in the United States has the clear goal of engaging in a systematic jihad against American civilization, as outlined by the document *The General Strategic Goal for the Group (Ikwan) in North America,* written in 1991. In that document, entered into evidence during the discovery process in the terrorism financing case against the Holy Land Foundation for Relief and Development, the group states (emphasis added):

> The process of settlement [of members in the United States] is a *"Civilization-Jihadist Process"* with all that means. The Ikhwan must understand that their work in America is a kind of *grand Jihad in eliminating and destroying the Western civilization from within* and "sabotaging'" its miserable house by their hands and the hands of the believers so that it is eliminated and Allah's religion is made victorious over all other religions. … It is a Muslim's destiny to perform Jihad and work wherever he is.[12]

It should not surprise the West that its enemy should seek to mislead about its intentions, methods, and goals. Deliberate and systematic deception and disinformation must be considered standard jihadist tactics. These tactics need to be understood in the framework of an enemy who wants opponents to relax, to lower their defenses, and to suffer defeat without a fight. The enemy will take a direct approach in the face of weakness and will reverse his approach when he is at a disadvantage.

Attacking the Enemy's Strategy

An adversary working under the veil of religion has distinct advantages when confronting modern controversy-averse societies. Political correctness, multiculturalism, and "denial mindsets" (especially the belief that religion cannot or must not be important in comparison to economic or "nationalist" motives) militate against Western self-defense. There can be no security for the United States and the West until there is a willingness to face reality by confronting the seriousness and gravity of this enemy.

The jihad movement does not fit into accustomed threat models. Other enemies sought tangible, limited objectives, such as land, power, control, or economic advantage. Jihad, by contrast, is a messianic, violent political ideology with no single government as an interlocutor, and, in principle, no limit to the movement's ambitions. Even conquest is only the prelude to a totalitarian program of universal "salvation."

Part of the problem stems from wishful thinking, mistaken assumptions, and cognitive egocentrism. Acknowledging that the foe is driven by a religious ideology of world conquest does not mean that 1.2 billion Muslims adhere to that ideology. But pretending that the jihadists are not so motivated in order to avoid a false assumption seems like a strange way to proceed, especially since the jihadists themselves say that they are driven by a religious compulsion.

Rather than work from a denial driven by false assumptions, the IC needs to empirically explore the relationship between real "moderates," dawa jihadis, and outright jihadis and what jihadis consider "rational" behavior (including suicide and sacrifice of their own people). Without this understanding, America's ability to act will be crippled.

Conclusions

The jihadists are determined to destroy America's free way of life. They will not be wished away or negotiated into any settlement. They will be ruthless in the pursuit of their objectives and, if empowered, they will intimidate or inspire Muslims who would not otherwise support them. Analysts must understand this.

The IC will have to be direct in its assessments. The roots of this ideology must be confronted, and its teachings of hate and intolerance must be exposed. This understanding will not come until the IC is fully able to accept the harsh realities of what jihad is and the will of the enemy who plans to wage it.

The opportunity to secure ourselves against defeat lies in our own hands, but the opportunity of defeating the enemy is provided by the enemy himself.
—Sun Tzu

The author is a Strategic Intelligence analyst in the United States Army Reserve, who holds the rank of Lt Colonel. He has extensive experience with Joint Intelligence issues and has worked with several national security organizations.

Recommended Readings

Bar, Shmuel. *Jihad Ideology in Light of Contemporary Fatwas.* Research Monographs on the Muslim World series. New York: Hudson Institute, 2006.

Bostom, Andrew. *The Legacy of Jihad: Islamic Holy War and the Fate of Non-Muslims.* Amherst, NY: Prometheus Books, 2005.

Cook, David. *Understanding Jihad*. University of California Press, 2005.

Cook, David. *Contemporary Muslim Apocalyptic Literature.* Syracuse , NY: Syracuse University Press, 2005.

Ehrenfeld, Rachel. *Funding Evil: How Terrorism is Financed and How to Stop It.* Chicago: Bonus Books, 2003.

Emerick, Yahiya. *What Islam is All About.* New York: IBTS, 1997.

Ganor, Boaz. *The Counter-Terrorism Puzzle.* Rutgers, New Jersey: Transaction Publishers, 2005.

Ibrahim, Raymond. *The Al Qaeda Reader.* New York: Doubleday, 2006.

Malik, S.K. *The Quranic Concept of War.* Adam Publishers, 1992.

Mannes, Aaron. *Profiles in Terror: The Guide to the Middle East Terrorist Organizations.* Kanham, Maryland: Rowman & Littlefield Publishers, 2004.

Phares, Walid. *Future Jihad.* New York: Palgrave Macmillan, 2005.

Siddiqi, Shamim. *Methodology of Dawaha Ilallah in American Perspective.* New York: Forum for Islamic Work, 1989.

Qutb, Sayyid. *Milestones.* Beirut, Lebanon: Holy Koran Publishing House, 1978.

Umdat al-Salik. *Reliance of the Traveller: A Classic Manual of Sacred Islamic Law.*

Interviews

Zeyno Baran, Eric Brown, and Shmuel Bar, Hudson Institute

David Cook, Rice University

M. Zuhdi Jasser, American Islamic Forum for Democracy

Lorenzo Vidino Fletcher, Tufts University

Douglas Farah and Ron Sandee, NEFA Foundation

Zainab Al-Suwaij, American Islamic Congress

Mark M. Lowenthal, Intelligence and Security Academy

Walid Phares, Foundation for the Defense of Democracies

Matthew Levitt, Washington Institute

Sheikh Dr. Ahmed Subhy Mansour, International Quranic Center

Jim Phillips, Heritage Foundation

Analysts from the Joint Staff, the Defense Intelligence Agency, and the Federal Bureau of Investigation

1 The *Encyclopedia of Islam* provides the following definition of *dawa*: "The *dawa,* in the religious sense is the invitation, addressed to men by Allah and the prophets, to believe in the true religion, Islam. The religion of all the prophets is Islam, and each prophet has his *dawa,* Muhammad's mission was to repeat the call and invitation: it is the *dawat al-Islam* or *dawat al-Rasul*. The Infidels' familiarity with, or ignorance of, this appeal determined the way in which the Muslims should fight against

them. Those to whom the *dawa* had not yet penetrated had to be invited to embrace Islam before fighting could take place … By a natural extension *dawa* also denotes the content of this appeal, the religious law, and the words *dawa, sunna , sharia , din,* are often used interchangeably." H. A. R. Gibb, et al., eds. *Encyclopedia of Islam.* (Leiden: Brill, 1960).

2 On the ideology of jihadist groups, see Walid Phares, *Future Jihad* (New York: Palgrave Macmillan, 2005) and *The War of Ideas* (New York: Palgrave Macmillan, 2007).

3 Interview with an IC analyst.

4 Interview with a Joint Chiefs of Staff (JCS) analyst.

5 Tawfiq Hamid, "The Development of a Jihadi's Mind," *Current Trends in Islamist Ideology,* Vol. 5. Washington, DC: Hudson Institute, 2007.

6 David Cook, *Understanding Jihad.* University of California Press, 2005.

7 Analysts should read primary sources such as Pakistani Brigadier General S.K. Malik's book, *The Quranic Concept of War* (Adam Publishers, 1992); Sheikh Nu Ha Mim Keller's authoritative translation of Umdat al-Salik's *Reliance of the Traveller: A Classic Manual of Sacred Islamic Law* (Beltsville, MD: Amana Publications, 1994); Sayid Qutb's *Milestones* (Beirut, Lebanon: Holy Koran Publishing House, 1978); Shammim Siddiqi's *The Methodology of Dawa in America* (New York: Forum for Islamic Work, 1989); and *The Al Qaeda Reader* (New York: Doubleday, 2006) by Raymond Ibrahim.

8 Cook, *Understanding Jihad.*

9 S.K. Malik, *The Quranic Concept of War.* Adam Publishers, 1992.

10 "The Muslim is the brother of the Muslim. He does not betray him, lie to him, or hang back from coming to his aid." Al-Misri, 'Umdat al-Salik, Book R "Holding One's Tongue," r2.3, r2.6 Slander (Ghiba).

11 Interview with an IC analyst.

12 Government Exhibit No. 003-0085 3:04-CR-240-G; *United States v. Holy Land Foundation, et al. Ikhwan* is the shortened version of the Arabic name of the Muslim Brotherhood.

Security through Credentialing and Access Control

By Lt Col Samuel Elkins, USAF, MNF-I CJ3 Protection

It is essential for military, government, and commercial facilities to have a robust process for knowing who is entering a facility and whether those people should be granted access. The safety and security of every Sailor, Soldier, Airman, Marine, and civilian is linked to the effectiveness of our credentialing system. Therefore, it is incumbent on everyone to have an awareness of how this process affects our work and of our role in ensuring that it remains effective.

The credentialing process includes granting access to an individual, providing badges for those who are granted access, and then continually monitoring those with access. These steps are completed by different agencies that coordinate their efforts to ensure a seamless and effective process.

Knowing how to ensure that only those with proper approval are on the installation and what to do if we suspect that someone should not be at our worksite protects people and resources.

The credentialing process includes granting access to an individual, providing badges for those who are granted access, and then continually monitoring those with access. These steps are completed by different agencies that coordinate their efforts to ensure a seamless and effective process.

It is important for all of us to understand the process of granting access, the purpose of the badge in enhancing security, and the role each of us plays in monitoring this system. This article summarizes these key areas and discusses how the pieces fit together to mitigate threats.

Granting Access

Granting access begins with a determination by a requesting authority that someone needs access or that someone who formally had access needs to have that access renewed. The requesting authority will normally be Coalition Force (CF), DOD, or US Department of State (DOS) personnel who are 0-5/GS-13 or equivalents who act in an advisory role. In some cases, contractors and select Iraqi officials can also be requesting authorities.

Examples of those who may need an MNF-I badge to access CF installations include—

1. Foreign government embassy staff
2. CF military without national identification
3. US contractors including non-CAC cardholders
4. Third Country National (TCN) contractors including CAC card holders
5. Local Nationals (LNs) working or residing on any CF installation.

The requesting authority is responsible for answering all inquiries associated with the application. An application is submitted for final approval to the installation commander for access to CF installations (see Figure 1). The person for whom access is requested may be required to submit biometric data, which can include finger and palm prints, iris scans, and facial mapping photos, if other suitable credentials are not already available.

MNF-I Badge Application

• Individual Applicant must fill out personal data, sign and date the application. They must provide supporting documentation to validate their identity and other supporting information.

• Applications are maintained and secured by coalition personnel and not accessible to others. Databases used to track the status of applications do not include addresses.

• Applicants are expected to provide valid accurate information to support potential interview process.

• If a renewal, turn in a copy of the front and back of the old badge with the application.

Figure 1. Application Process

The person for whom access is requested may be required to submit biometric data, which can include iris scans, finger and palm prints, and facial mapping photos, if other suitable credentials are not available.

Biometric data is entered into the Biometric Identification System for Access (BISA). This enrollment system is located at approximately 40 MNF-I locations and is available to all CF installations in theater. BISA information can also be used in other background checks and interviews, if deemed necessary. This information has assisted in—

- Detention and interrogation of subjects who have suspected relationships with terrorist organizations
- Detention and subsequent eviction from Iraq of contractors who illegally entered Iraq
- Finding numerous databases matches that resulted in barment from MNF-I installations.

The data is checked against various network databases to determine whether sensitive and high-interest information exists that may affect the decision to provide access to an installation or, in some cases, to revoke access. This data is then stored so that agencies with a need to know can access and use the data to verify the credentials of the people accessing their installations.

Figure 2. Sample Badge (front and back)

The following process is used to obtain a badge for access to installations and other locations in Iraq:

1. A Sponsor (i.e., requesting authority) completes an application and submits it to the badging office, which screens the application for completeness.

2. A Control Number is assigned to the application, which is used to track the progression of the badge. (The Sponsor should record this number.)

3. The applicant's name is submitted to Task Force Counterintelligence Coordinating Authority (TFCICA) for background checks. Blue or green badges are sent to C2X.

4. All applications requiring access to multiple sites "IRAQ WIDE" are sent, along with a letter of justification, to MNF-I CJ3 Protection for clearance.

5. Locally Employed Persons (LEPs) screening is a semiannual requirement for LN translators and is a yearly requirement for all other LNs. TCNs are subject to TFCICA checks. The commander can waive this requirement (not recommended) if there is a backlog of LEP interviews.

6. Fingerprints, iris scan, and photo are taken and entered into BISA. The Biometric Automated Toolset (BAT) is an alternate method for capturing these data.

7. The biometric data and the application are sent to the Biometric Fusion Center in West Virginia to be formatted for badge printing.

8. The badge is printed and is sent to a local Badge Office for pickup.

9. The Badge Office verifies that the badge is correct, and the person receiving the badge must be properly identified prior to issuance. Individual badge owners must be verified in person prior to receiving the badge.

The Badge Office verifies that the badge is correct, and the person receiving the badge must be properly identified prior to issuance. Individual badge owners must be verified in person prior to receiving the badge.

TYPES OF BADGES

BADGE TYPE & COLOR	AUTHORIZED BADGE HOLDER	ESCORT PRIVILEGE
BLUE	Coalition Partners: The Highest Level Iraqi Officials, UN SRSG	Yes
GREEN	High-Level Iraqi Officials; Selected UN, Military, and Non-Coalition Embassy staff	Yes
BROWN	Coalition and NTM-I Contractors	Yes
YELLOW	Mid-Level Iraqi Officials; Selected PSD, UN, Military, and Non-Coalition Embassy, Select Western Media	Yes
ORANGE	Low-Level Iraqi Officials and Employees; Selected PSD, UN, Military, and Contractor Leaders	No
RED	Non-Coalition Contractors and Generally Unvetted TCNs/LNs, Non-Western Media, and LN Media Staff	No
LN RESIDENTS	Local National Residents and Employees	Limited
BLACK/Temporary	Visitors	No

Table 3: Badge Types

The Badging System

The badging system improves security by providing a means of identifying and screening those who attempt to gain access to approved locations. A standardized access badge system simplifies recognition and reduces confusion at entry control points (ECPs) and bases.

After the proper approval and checks are accomplished, the person entering the installation will need to have a badge, unless she has a press card, a passport, or other documentation that can be used to gain access to a facility for shorter periods of time or for special situations. In such cases, the person will be instructed to report to a badging office with the necessary identification and the approved paperwork to obtain a badge.

The type of badge provided is based on the mission and the status of the individual (see table 3, above). In general, everyone will display some form of identification to gain access to an installation.

The above table provides a general list of the types of badges and descriptions of the people who will be wearing them. The right column identifies whether the badge holder can escort others into the location. A high-level Iraqi official, for example, can escort contractors or family members with black visitor badges when they enter an installation; however, a contractor with a red badge must not be allowed on an installation without an escort.

The badge color provides the guards or other observers with the information to know where and what kind of access the badge holder is permitted.

It determines the lanes of traffic the badge holder is allowed to drive in and whether he is personally exempt from different types of personal or vehicle searches when entering compounds. The badge color also determines whether the holder is required to carry a weapons card.

Those involved in the monitoring of installation access must be aware of all of this information.

Figure 2 shows the back and the front of badges used to monitor access requirements.

The left side of Figure 2 shows the front of the badge, with colors displaying the names of locations. A badge holder can only have access to a displayed site if she is being escorted by someone with escort authority for that site, as described in the table on the previous page. Some badge holders have IRAQ WIDE access and are allowed access to all forward operating bases (FOBs), as necessary. The hologram on each badge helps mitigate counterfeiting activities.

The photo and the name provides screeners with the ability to match the badge with the holder and to crosscheck other identification. Underneath the picture and name is a biometric chip. The chip stores biometric data that can be used to verify identification using BISA portals. The black strip adjacent to the chip identifies privileges that are available to the badge holder (e.g., D: DFAC; G: gym; B: billeting; P: PX; M: MWR; H: hospital). Directly under the black strip is the badge expiration date and, under that, the badge number.

The back of the badge, shown in the far right side of Figure 2, provides descriptive personal data: gender, date of birth, eye color, hair color, height, weight, date of issue of the badge, and levels of access. The levels of access indicate whether the holder is subject to a personal or must hold a weapons card, and can escort others. Additionally, the vertical lines on the right side of the back provide information on the issuing location, the employer, the sponsor's name, and the application number for the badge.

The badging system improves security by providing a means of identifying and screening those who attempt to gain access to approved locations. A standardized access badge system simplifies recognition and reduces confusion at entry control points (ECPs) and bases.

Monitoring Access

All badge holders are responsible for securing and displaying badges properly when entering an installation. Badges are displayed in the front middle torso region between the shoulders and the hips.

Everyone is responsible for verifying that only those who require access are allowed to enter an installation, but some personnel have more direct responsibility. The guards checking badges at the ECPs, for example, must understand what to look for in allowing access. These screeners are trained to detect false IDs, and they have the daunting task of trying to do that within a few seconds for large numbers of people and for a variety of documents on a daily basis.

Newer, cost-reader-authenticators can add a high degree of automation and accuracy to the secure access control process. They are available in a variety of physical configurations and can automatically read and verify biometric data. They extract image fields such as photos as well as data fields, whether from text, barcodes, magnetic stripes, or embedded chips. The extracted data can be vetted against external watch lists without compromising privacy.

Conclusions

Everyone at an installation has a responsibility for security. Report a person without a badge or proper identification to the chain of command or to other proper authorities. If a person is walking around in an unauthorized area or without a required escort, he should be detained and reported to the proper authorities.

Commanders are encouraged to invite members of the Badge Access Control team to Commanders Calls or for informal meetings. The MNF-I CJ3 Protection staff has created examples that can be used to improve everyone's situational awareness of this system. Additionally, CDs that provide a broad knowledge of biometric systems are also available. Awareness on everyone's part will ensure that the credentialing system is effective for installation security.

Detention Operations in the Global War on Terror

CW4 (R) L. J. Powlen III, Senior Analyst, Logos Technologies, Inc

Currently, detainee operations exist in an environment of competing missions among the primary entities involved: Detention Operations (DETOPS), human intelligence (HUMINT) collection, and law enforcement activities (LEA). Detainee operations in the Global War on Terror (GWOT) require a partnership approach.

Detainees must be conditioned to cooperate with both the guard force and the interviewers. This cooperation can best be accomplished through a system of incentives and rewards.

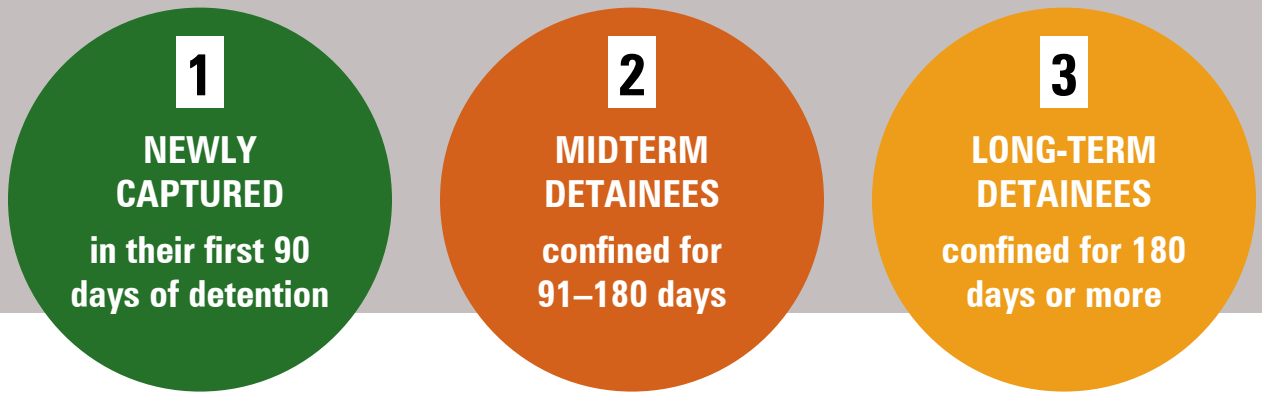
What needs to exist is a team environment in which the needs of all participating agencies are addressed in a mutually supportive partnership pact. DETOPS, Psychological Operations (PSYOPS), Behavioral Science Consultation (BSC), medical activities (MED), psychological and psychiatric treatment (PSYCH), rehabilitation activities (REHAB), HUMINT collection, and LEA should work together to control the behavior of the detainees from a security aspect and to shape peer expectations within the detained population to facilitate cooperation during information gathering operations.

For the purposes of this discussion, detainees who are in their first 72 hours of detention and who are subject to Battlefield Interrogation Tactics (BIT) will not be addressed. This discussion will be limited to those who have been placed in regional or theater detention facilities and in long-term detention facilities.

To fully address all aspects of detainee operations, it is necessary to divide the detained population into three groups and to address each group individually. The first group of detainees consists of those who are "newly captured," that is, in their first 90 days of detention, during which the primary focus is the collection of actionable tactical or operational intelligence. The second group consists of those who are in "midterm" detention, confined for 91–180 days. The third group consists of those who are in "long-term" detention, confined for 180 days or more.

CLASSIFYING THE DETAINED POPULATION

To fully address all aspects of detainee operations, it is necessary to divide the detained population into three groups and to address each group individually.



Managing Detainee Behavior

For all three categories of detainees, security is always an overarching goal; the primary reason for detention will vary by group. In this regard, it must always be stressed that outside the sphere of the interview booth, the guard force has absolute control of the detainees. All entities involved can maintain control without overt displays of authority.

The power of the interviewers, whether Military Intelligence (MI) or LEA, stems from their ability to leverage the guards for detainee privileges. Interviewers should never give a detainee anything in the booth to take back to his cell. The interviewers can allow the detainee to review the material in the booth to determine whether or not the material meets the detainee's needs, but all items should be delivered and removed by the guard force.

The guiding philosophy should be that a detainee who is cooperative with the guards but is not cooperative with the interview process is not a cooperative detainee. The converse also applies: A detainee who is cooperative with interviewers but not with the guard force is also not a cooperative detainee. These two examples demonstrate a detainee who is playing Americans against Americans, and that can never be allowed to happen. Only those detainees who cooperate with the guard force and with the interview process should be given privileges or rewards.

All parties must remain focused on the primary goal, which is security, meaning compliant, cooperative detainees. Security must always be a collaborative process in which all US forces present a united, mutually supportive front.

Newly Captured Detainees

A wide range of behaviors can be expected from newly captured detainees, from complete passive compliance to acting out and disruptive behaviors. It is the responsibility of both the interviewers and the guard force to mold the detainee's behavior. Another factor will be the detainee's peer expectation for behavior; this will be addressed in detail later in this paper. Detainees must be conditioned to cooperate with both the guard force and the interviewers. This cooperation can best be accomplished through a system of incentives and rewards.

An incentive is something that is provided to encourage favorable future behavior; a reward is something that reinforces past and present compliant behavior. During this period of detention, the primary focus has to be acquisition of actionable tactical or operational intelligence. Because the detainee's behavior is being modified, the guard force will need to be tolerant regarding the use of incentives by the interviewers while the detainee is socialized into the confined environment. While incentives may be extended at the interviewer's discretion to a detainee who is mildly noncompliant with the guard force, rewards can only be given to detainees who are cooperative with both the guards and the interviewers.

At this point in detention, the guard force should not unilaterally provide or remove any incentives or rewards without consulting the interviewer. Because the situation across GWOT varies greatly, each detention facility, in consultation with MI, LEA, PSYOPS, and BSC, should develop a list of available

incentives and rewards with agreed upon criteria for their application. The participation of PSYOPS and BSC is critical for shaping peer expectations among the detained population throughout the entire detention cycle.

Although widely sought, disincentives and punishments should be avoided. Everything that is afforded the detainee is an incentive. Examples include not being put in isolation, having a sleeping mat or a blanket, and being allowed to participate in group prayer. Such conditions are provided as incentives for future cooperative behavior; in the absence of cooperative behavior, the incentive should be removed.

behavior through use of the relationship-based interview protocol, which is not detailed in this paper.

At this point, the detainee will have formed a *wasta,* or network, with other detainees. At this stage, it is crucial that the guard force report behaviors to the Facility Intelligence cell or, in the cell's absence, to the BSC. Continued evaluation and monitoring of the detainee's behavior will be necessary to determine the evolution of noncooperative influences, such as escape committees, organized resistance, or movements among the detainees to encourage noncompliant behavior. Through the use of cell moves and linguistic isolation, these behaviors can be controlled within the detainee population.

The development and successful implementation of educational and vocational programs for these detainees is critical for maintaining a compliant and cooperative detained population.

A Camp Delta recreation and exercise area at Guantanamo Bay, Cuba.

Midterm Detainees

As a general rule, after 90 days in detention, any actionable, tactical, or operational intelligence that the detainee possessed should have been either exploited or rendered useless by the passage of time. At this point, the primary focus should be on developing the criminal case against the detainee, if any exists. The detainee should be fully indoctrinated into the rules of the facility and should be subject to peer expectations.

The guard force may take unilateral action to remove incentives or rewards, and should inform the investigator working with the detainee as soon as practical if this is done, but may not unilaterally apply incentives or rewards. For his part, the investigator will still be a great influence in shaping the detainee's

Long-Term Detainees

By now, decisions should have been made regarding whether or not the detainee has any strategic intelligence value that requires further exploitation and whether or not the detainee will continue to be investigated for violations of law that will be prosecuted in a designated venue. Those detainees who do not retain MI or LEA value become the sole interest of the guard force.

The guard force may unilaterally apply or remove incentives and rewards to these detainees without consultation with MI or LEA. Consultation, however, should continue with both PSYOPS and BSC to determine long-range consequences of actions by the guard force and to ensure the continuation of positive peer expectations for behavior. For those detainees who remain of interest to either MI or LEA, the guard

force should have the ability to unilaterally remove incentives or rewards with notification to personnel working with the detainee; however, the application of rewards and incentives by the guard force must only be done after consultation with the personnel working with the detainee.

The biggest challenge will be for the guard force to keep the detainees engaged so that they do not lapse into hopelessness or begin to foment dissent. This effort will be primarily supported by PSYOPS, BSC, MED, REHAB, and PSYCH. Developing programs that keep the detainees occupied and stimulated is of the utmost importance. Such programs may include vocational training, literacy initiatives, and establishment of a detainee governing council that will be responsible for maintaining orderly behavior among the detainees and for engaging in dialogue with the facility command group regarding program ideas and grievances.

The ability for the detainees to air grievances and to receive due consideration from the command group in a controlled manner is paramount for diffusing disruptions and organized noncompliant behavior among the detainees.

PSYOPS

Throughout the detention cycle, the function of PSYOPS is to assist in creating an atmosphere in which the detainees are encouraged to cooperate with the interview process and with the guard force. The area of focus changes as detainees progress through the process, and PSYOPS products must be geared toward each focus. PSYOPS is also critical for REHAB and release programs to ensure that detainees leave confinement with a pro-US sentiment.

For PSYOPS to function properly, all entities involved with the detainees must be required to report behavioral information to the Facility Intelligence cell, which is responsible for fusing the information and for providing analytical products to support the various missions occurring in the facility. BSC is also critical in a consultant role at all points during the cycle. Those assigned to BSC duties should be psychologists with additional specialty training in the area of detained individuals and behavioral consultation. All should be certified in survival, evasion, resistance, and escape. Their roles support interview operations and detainee management operations.

BSC and PSYOPS have the greatest influence in developing detainee peer expectations. Through the consistent application of incentives and rewards and the use of PSYOPS products, an expectation can be created among the detainees that engenders cooperation with both the guard force and the interviewers. Once institutionalized, these expectations will be transferred to new detainees as they are socialized into the detention facility. Peer expectations can reduce the amount of active participation needed by the guard force and by interviewers in shaping detainee behavior because the detainee's peers will do it.

Through the use of peer expectations, those who do not comply are more likely to be suppressed by their social sphere and those who refuse to comply will be pointed out by the detainees to the guard force as they seek to maintain the cooperative environment. BSC and PSYOPS are the experts in the area of managing behavior and should carry great influence in this area. Personnel assigned to BSC cannot be involved in the treatment of detainees; they must only be used as behavior consultants.

MED/PSYCH

MED and PSYCH specialists are only involved with the detainees in the medical or the psychologic or psychiatric areas of treatment. These specialists cannot participate in BSC and cannot provide advice on interview operations. They are charged with the health of the detained population, and it is incumbent on them to report health issues and concerns to the facility command group.

MED and PSYCH specialists should not be completely isolated from the guard force and others who work in the facility. Frequently, guards or interview personnel will seek to have a detainee receive medical treatment. Confirmation that treatment was received should be shared with the referring parties. It is also essential that MED and PSYCH personnel identify malingering detainees who may be using this tactic as a form of noncompliant behavior. Instances of malingering should be reported to the Facility Intelligence cell.

REHAB

REHAB personnel are psychologists, sociologists, occupational specialists, and teachers whose primary efforts will be focused on long-term detainees. They will assist with developing the attitudes of detainees being released and in developing programs for those detainees who will remain in detention for an extended period. The development and successful implementation of educational and vocational programs for these detainees is critical for maintaining a compliant and cooperative detained population.

In addition to the standard REHAB package, consideration must be given to conducting religious rehabilitation. Based on the very successful model currently employed by Singapore, Dr. Rohan Gunaratna and BG (Ret) Russell D. Howard are working on developing a program that should be implemented by the Department of Defense in all theaters in which Islamic militants are detained. The Strategic Islamic Communications Program concept

has an 85 per cent success rate in Singapore and could be used—

- By trained PSYOPS personnel in a counterpropaganda campaign
- By trained Islamic clerics in prisons, in camps, and in other areas where Muslim extremists are incarcerated
- In a simplified form in military service schools and for predeployment training
- As part of counterterrorism courses at the undergraduate and graduate levels.

The program is currently being funded by the US Military Academy at West Point, New York, while it is in development, and it is key to dissuading released detainees from returning to the battlefield. If properly applied, the program would also greatly enhance security of detainee operations and strategic and operational information gathering.

Conclusions

Detainee operations in GWOT require the establishment of collaborative, complementary partnerships among all of the entities involved in these operations. While the focus on the mission of one entity or the other changes throughout the detention cycle, it is critical that all involved provide a united front to groom individual detainees and to develop positive peer expectations in the detained population that will enhance information gathering and security operations.

Decontamination Operations in a Mass Casualty Scenario

By Michael L. Snyder and Thomas J. Sobieski

Michael L. Snyder is a Homeland Security Advisor with Battelle Memorial Institute. Thomas J. Sobieski provides contract support (Battelle Memorial Institute) to the Joint staff, Force Structure, Resources, and Assessment (J8), Joint Requirements Office for Chemical, Biological, Radiological, and Nuclear Defense.

At 10 a.m. on May 10, 2007, in the northeast corner of metropolitan Indianapolis, near the suburb of Lawrence, a terrorist group smuggled in and detonated a nuclear device. The local, state, and federal governments were presented with many complex challenges as a result of this catastrophic event. Among the most challenging tasks was the need to quickly and completely decontaminate large numbers of the population. . . .

Thus begins the scenario for exercise Ardent Sentry 2007 (AS07). Why was such an exercise needed? Indeed, the DOD is capable of providing decontamination in support of civil authorities. However, effective employment of DOD decontamination capabilities requires a full understanding of the special circumstances of a homeland event and the doctrinal differences between battlefield decontamination operations and defense support to civil authorities (DSCA).

This article, sponsored by the Joint Requirements Office for Chemical, Biological, Radiological, and Nuclear Defense (JRO CBRND), focuses on two perspectives of the DOD decontamination mission for planning considerations: the differences between decontamination conducted in a DSCA environment and that done by DOD units in their traditional wartime role. The article also examines additional considerations on mass decontamination tasks due to the DSCA environment; the challenges associated with decontamination in a DSCA environment; the impact of DSCA on decontamination tasks; and some specific observations about managing the civilian population, controlling runoff, and dealing with personal effects. It further highlights the need for better understanding by DOD planners and units regarding the unique challenges of supporting civilian authorities with decontamination.

Background

Exercise Ardent Sentry 2007 was designated by the Chairman of the Joint Chiefs of Staff, sponsored by US Northern Command (USNORTHCOM), and supported by US Joint Forces Command. Based on Department of Homeland Security (DHS) National Planning Scenario #1 (Nuclear Detonation—10-kiloton Improvised Nuclear Device), AS07 primarily focused on exercising the USNORTHCOM ability to execute DOD chemical, biological, radiological, nuclear, and high-yield explosive (CBRNE) response plans at the operational level. For the first time, AS07 included a separate but simultaneous field training exercise designed to allow selected DOD units to train with civilian counterparts.

Since 2004, the JRO CBRND has been providing CBRN and consequence management subject matter experts to support the combatant commands' and their subordinates' training and exercise programs. The office has also partnered with several non-DOD government agencies to enhance their knowledge of DSCA procedures.

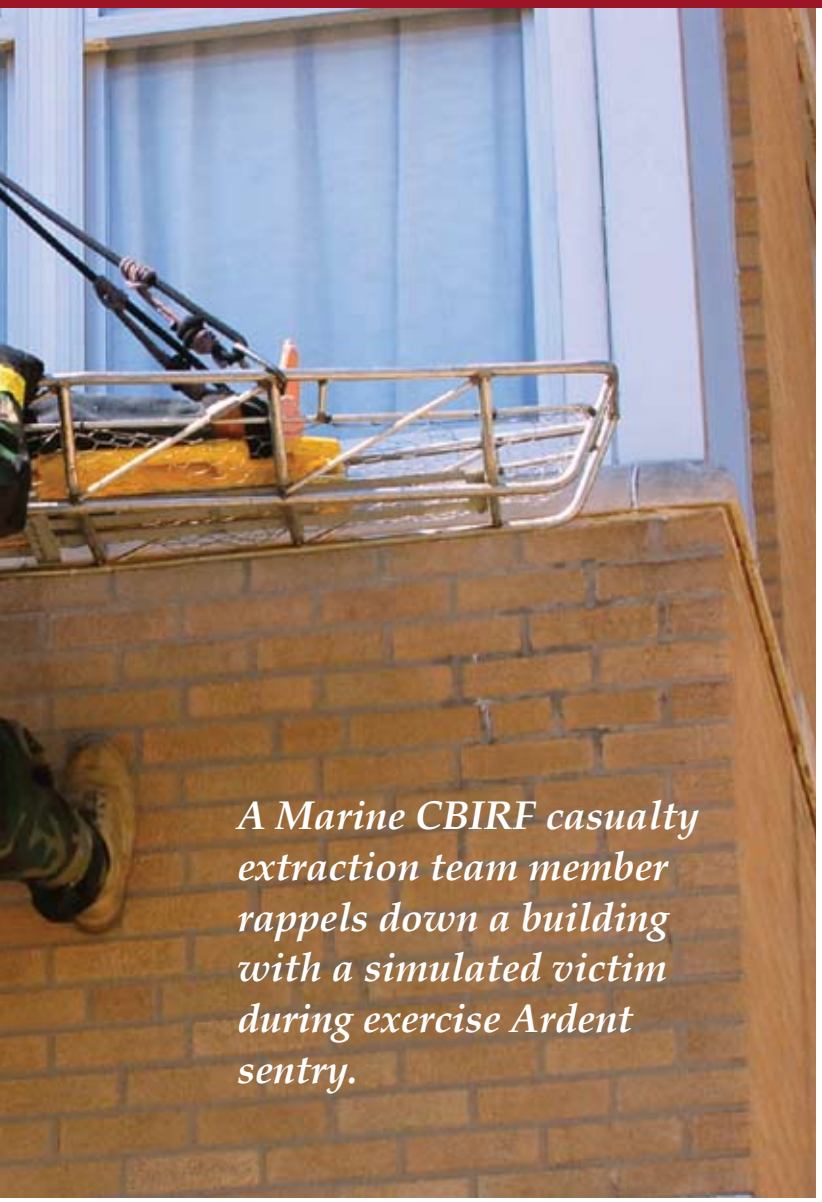
In the months leading up to AS07, the JRO CBRND provided USNORTHCOM and USJFCOM with technical assistance in developing the effects of the nuclear detonation for the exercise and observed battle staff operating procedures at selected command and control locations. Exercise development included collaborating with exercise planners from the Indiana Department of Homeland Security to build the documents and scenario inputs needed to drive the DOD response to the federal requests for assistance. Participants recognized during the planning process and exercise execution that further discussion of the above two perspectives of DOD decontamination would benefit the CBRNE response community and emergency responders in general.

The exercise was conducted May 10–17, 2007. The simulated nuclear detonation was a no-notice terrorist event in the northeast corner of metropolitan Indianapolis. The scenario used scripted weather, census data from 2000, and computer modeling. It was determined that the 10-kiloton surface burst created casualties estimated at 15,000 dead and 21,000 injured. The injured included those affected by the blast, thermal radiation, prompt radiation, and subsequent radioactive fallout.

The detonation and subsequent effects resulted in the declaration of an incident of national significance, the appointment of a principal federal official by DHS, and a subsequent Presidential disaster declaration. Per the National Response Plan (NRP), which was in effect at the time of the exercise but has since been replaced by the National Response Framework, DHS and Federal Emergency Management Agency (FEMA) Region V established a joint field office (JFO) at Camp Atterbury, 43 miles south of Indianapolis. The defense coordinating officer and defense coordinating element from FEMA Region V joined the JFO as part of the coordinating staff. Joint Task Force–Civil Support was deployed to Camp Atterbury to provide command and control over all DOD forces deployed (real world and notionally) to support the local, state, and federal response. Elements of the DOD CBRNE Consequence Management Response Force were also deployed to conduct operations in concert with first responders from Marion County, Indiana, the Indiana Department of Homeland Security, elements from the Indiana National Guard CBRNE Enhanced Response Force Package, and civil support teams. This field training exercise was conducted at the Muscatatuck Urban Training Center, 25 miles southeast of Camp Atterbury.

Decontamination in DSCA Environments

In a terrorist use of weapons of mass destruction (WMD) scenario, DOD is ready to assist the local, state, and federal response efforts. DOD fulfills



A Marine CBIRF casualty extraction team member rappels down a building with a simulated victim during exercise Ardent sentry.

its DSCA mission by responding to requests for federal assistance in accordance with the NRP and DOD policy and guidance. The NRP provides the coordinating framework for support under the Robert T. Stafford Disaster Relief and Emergency Assistance Act[1] and the Economy Act.[2] Within the NRP, DOD is a support agency to all 15 emergency support functions and a cooperating agency to the majority of NRP support and incident annexes. Pursuant to the above, when requested and in concert with other federal agencies, DOD supports the primary agency by providing the manpower and equipment necessary to meet the needs of the responding local and state officials.[3]

In a large-scale catastrophic event, where local, state, and regional capabilities are overwhelmed, the federal government, with DHS as the lead agency, assists local and state efforts in mitigating effects. To accomplish this, DHS may request support from Title 10 DOD forces, activated Reserves, and possibly federalized National Guard. Orchestrating DOD capabilities in collaboration with other existing capabilities is the function of the JFO.

In the AS07 scenario, DOD decontamination capabilities were used (notionally) either to augment or provide relief in place for decontamination operations initially started by local first responders and National Guard units in state Active duty or Title 32 status. This highlights the need for DOD decontamination units to learn and understand how civilian first responders approach expedient mass decontamination operations.

The pre-9/11 focus on responding to and remediating hazardous material spills demonstrated a capable and thorough decontamination process. These procedures and systems, however, were equipment- and manpower-intensive and had various but limited throughput capacities (usually 50–100 people per hour). By comparison, the current decontamination throughput capabilities of DOD units, such as the Marine Corps Chemical/Biological Incident Response Force and Army Chemical Decontamination units, vary between 250 and 400 troops per hour.[4]

Recognizing the need to decontaminate much greater numbers, civilian first responders developed methods using currently available equipment. Two of the more common approaches are the Emergency Decontamination Corridor System (EDCS) and Ladder Pipe Decontamination System (LDS). Both have been documented in publications by the US Army Soldier and Biological Chemical Command[5] (SBCCOM) and the Chemical, Biological, Radiological, and Nuclear Defense Information Analysis Center (CBRNIAC).

In January 2007, SBCCOM published Guidelines for Mass Casualty Decontamination during a Terrorist Chemical Agent Incident. Although the guidelines review these capabilities in respect to a chemical event, they offer several principles of decontamination that also apply to a nuclear detonation scenario:

- Expect a 5:1 ratio of unaffected to affected casualties.
- Decontaminate as soon as possible.
- Disrobing is decontamination: top to bottom, more is better.
- Water flushing generally is the best mass decontamination method.
- After known exposure to a liquid agent, first responders must self-decontaminate as soon as possible to avoid serious effects.

Drawing on the innovation of various fire departments, section 4.4 of the SBCCOM guideline also provides excellent schematics, photographs, and procedures for mass decontamination via the EDCS and LDS and commonly used first responder equipment.

Similarly, CBRNIAC cites two products: the *Emergency Decontamination Corridor and Ladder Pipe Decontamination Systems* (CR–04–12), published in May 2004, and *Best Practices and Guidelines for Mass Personnel Decontamination* (SOAR–04–11), published in June 2003. CR–04–12 is a laminated card that provides site layout diagrams for each system and quick reminders on the advantages and disadvantages of each.

- Determining who needs to be decontaminated.
- Multisite operations.
- Integration of decontamination operations with other plans.
- Disposition of runoff.
- Disposition of personal effects.
- Accountability.
- Crowd control.

The CBRNE expert needs to be keenly aware of the full context in which DOD decontamination capabilities will be employed in a DSCA environment. Incorporating the above considerations into the staff preplanning and command guidelines will strengthen the execution of mass decontamination operations.

The DHS Lessons Learned Information Sharing Web site (www.LLIS.gov) contains an archive of best practices from all jurisdictions of interest to the response community at large.

Similar to the SBCCOM publication, SOAR 03–10 focuses on responding to and decontaminating victims due to chemical or biological incidents. Its sections on general decontamination principles, setups, and managing incident sites are useful for a nuclear scenario as well. These systems primarily use equipment common to fire departments (including those at DOD installations), but not to DOD decontamination units.

This disparity in capability within DOD is to be expected as installation fire department personnel are trained and equipped much like their civilian counterparts and routinely collaborate with them through mutual assistance/aid compacts (as directed through DOD instructions/guidelines). DOD decontamination units, on the other hand, are equipped and trained for the warfighting mission. These facts highlight the need for all elements of the possible DOD response community to become familiar with the equipment and procedures of civilian expedient mass decontamination to fulfill their expected supporting roles according to the NRP.

Impact of DSCA

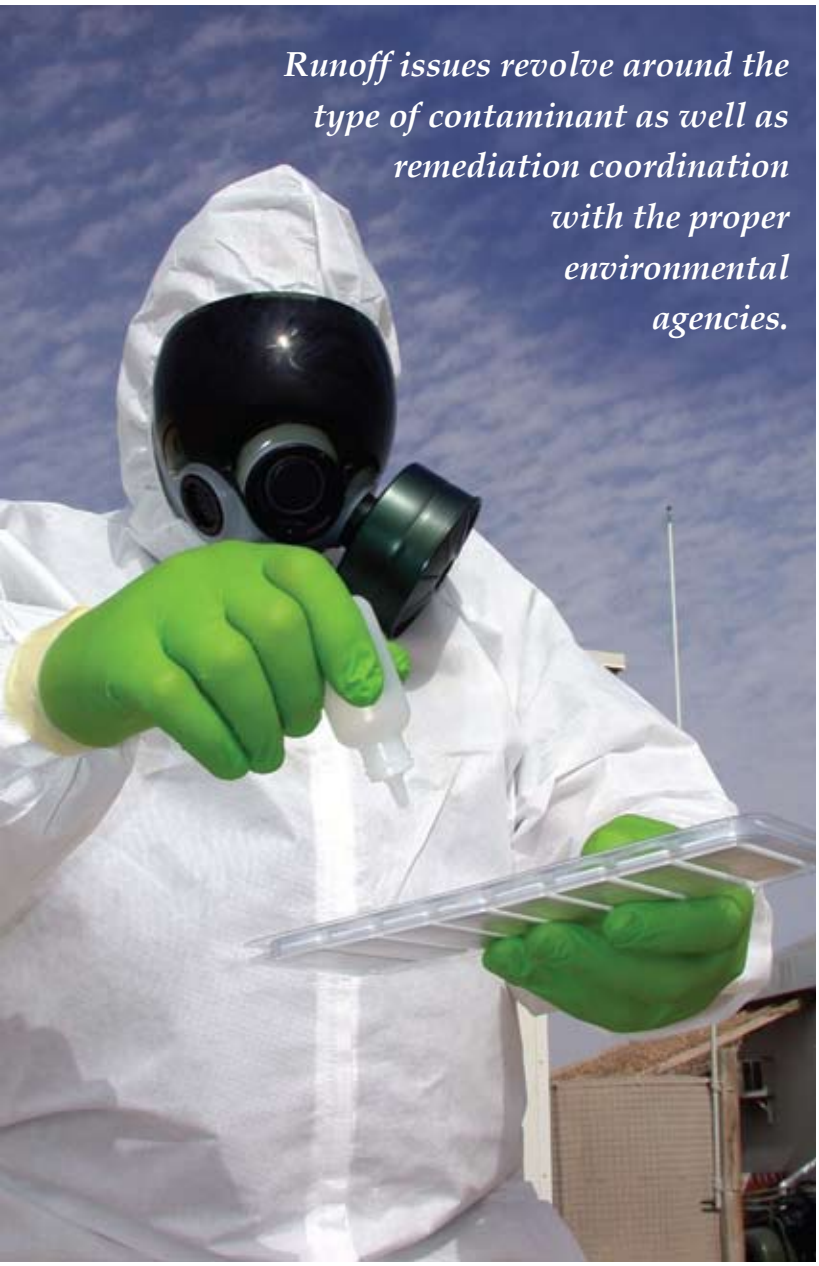
While developing the scenario in conjunction with representatives from the Indiana Department of Homeland Security Training Division and City of Indianapolis Department of Public Safety, it was learned that decontamination efforts in the DSCA environment require special considerations by military CBRN planners in the following areas:

Other information sources of best practices to amplify and support these considerations include the DHS Lessons Learned Information Sharing Web site (www.LLIS.gov), which contains an archive of best practices from all jurisdictions of interest to the response community at large. One such citation, "Radiological Dispersal Device Incident Response Planning: Decontamination," provides insights into the topical discussions presented here.

Determining Decontamination

In the AS07 scenario, modeling estimated that a total of 21,000 citizens were within the area defined as the evacuation zone due to the fallout created by the nuclear detonation. Some of these citizens would be evacuated immediately, while those further downwind might shelter in place and be evacuated later.

It is reasonable to assume that not everyone within the evacuation zone would be contaminated. Identifying those who are "clean" would greatly reduce the resources needed and expended. This prescreening process is likely to be complicated by several factors in a no-notice event. For example, many victims or potential victims would have self-evacuated, creating the issue of how to communicate to them, locate them, treat them, and deal with any cross-contamination precipitated by their evacuation. Additionally, first responders, some of whom would be victims themselves or become victims due to exposure, would arrive late and be uncoordinated due



to communications being degraded by electromagnetic pulse and system overloading.

Multisite Operations

To respond to the magnitude of need, several mass decontamination sites probably would be established around the plume perimeter. While DOD is not the primary agency responsible for coordinating the operations of the multiple sites, having military leaders prepared to provide support and/or relief to any operation or even take over full operation of a particular site would improve and maintain the efficiency of the process. Knowledge of the locations, access routes, and capabilities on each site would expedite the response to requests for support by civil authorities.

Integrating Operations

Decontamination operations must be integrated into the whole mitigation/recovery process. Successful decontamination operations include planning initial medical triage and follow-on medical care, as well as providing subsequent transport, clothing, food, and shelter to all those who process through prescreening. From a medical standpoint, establishing ambulatory and nonambulatory decontamination lines is just one aspect of the process. Consideration needs to be given to how close to the decontamination area triage facilities and transportation staging areas should be established so wind shifts do not threaten operations. Provision of food and water needs to be planned for those awaiting transportation, as do trash collection and the consolidation and disposal of contaminated clothing and personal effects. Coordination with ESF 8 (Public Health and Medical Services) and the American Red Cross on pickup/transport is recommended in order to prevent overcrowding at the decontamination site.

Runoff

The need to process large numbers through the decontamination line makes containment of the runoff a challenge. Conventional hazardous material decontamination operations contain runoff to prevent contamination of the environment. Runoff issues revolve around the type of contaminant as well as remediation coordination with the proper environmental agencies. A hard surface with the proper grade to reduce cross-contamination is essential to containing the runoff. EDCS and LDS operate as high volume/low pressure systems and generate significant amounts of runoff.

Proper location selection and configuration are crucial to enabling continuous decontamination operations, as well as to reducing the amount of postdecontamination remediation that needs to occur. In the DSCA environment, CBRNE staff officers must consider environmental impacts when planning and executing decontamination operations. Numerous federal and state laws may impact the decisions of CBRNE planners. *First Responders' Liability to Mass Decontamination Runoff,* published by the Environmental Protection Agency in July 2000, provides an excellent synopsis of the issue and has links to more detailed information.[6]

Personal Effects

The need to decontaminate large numbers of people creates the need to deal with volumes of personal effects that will require final disposition as victims process through the decontamination line.

Jurisdictional decisions referencing the disposition of personal effects will need to be addressed within JFO planning. What is to be done with licenses, credit cards, and other personal identity items will need to be determined as prescribed by local protocols. Additional protocols must be in place for the screening/disposition of vehicles.

Accountability

In every event, ascertaining the disposition of all affected people is a major concern. A nuclear detonation scenario of this magnitude would most certainly be a worst-case scenario, particularly due to the large numbers of displaced residents seeking decontamination. Complicating the need to track people through evacuation, decontamination, transport, and followup medical care is the fact that they may have also been stripped of any identification. In the initial chaos of a no-notice event, such protocols may not have been in place in the rush to meet other priorities. In any case, typical DOD decontamination procedures do not address this task but may be expected to support it in a DSCA response.

Crowd Control

Keeping large groups orderly is essential for effective mass decontamination operations. Local law enforcement would vector victims to the various mass decontamination sites established upwind of the blast and outside the projected plume path. Communicating to the victims the necessity to move through the decontamination processes in an efficient manner would be a challenge. While Title 10 forces are prevented from performing law enforcement duties in accordance with the Posse Comitatus Act, the planning and operation of a mass decontamination station must address the need for crowd control and coordination for support from civilian law enforcement.

The procedures and capabilities to conduct mass decontamination have undergone dramatic changes in recent years. Although the Department of Defense is not the lead agency responsible for coordinating the overall decontamination effort in a catastrophic scenario such as a nuclear detonation, it will most likely be called upon to establish its own mass decontamination sites or to augment operations that were previously established by local/state first responders.

This creates the need to understand the operational employment concepts and equipment that may be used by civilian first responders such as the Emergency Decontamination Corridor System and Ladder Pipe Decontamination System. Additionally, practicing the task of actually having to decontaminate thousands of people is not often done; therefore, periodic review of mass decontamination plans with special consideration of the aforementioned areas allows planners to incorporate new policies, procedures, and equipment. We train not just to train; we train because we are reminded that someday, we may have to execute this scenario for real.

Although the Department of Defense is not the lead agency responsible for coordinating the overall decontamination effort in a catastrophic scenario such as a nuclear detonation, it will most likely be called upon to establish its own mass decontamination sites or to augment operations that were previously established by local/state first responders.

1 Public Law 93–288, Title 42, U.S. Code, Section 5121, et seq.

2 Title 31, U.S. Code, Section 1535.

3 U.S. Northern Command Revised Contingency Plan 2501 for Defense Support of Civil Authorities, dated 11 April 2006, describes the manner in which DOD forces provide that support.

4 Data gleaned from Chemical/Biological Incident Response Force organizational brief and statements made by CBRNE Consequence Management Response Force personnel at the commanders' conference hosted by Joint Task Force–Civil Support, Fort Monroe, Virginia, 28–30 August 2007.

5 In 2003, the U.S. Army Soldier and Biological Chemical Command was renamed the Natick Soldier Research Development and Engineering Center under U.S. Army Research and Development Command.

6 Available at: www.epa.gov/OEM/docs/chem/onepage.pdf

Notes from the War on Terror

Overcoming the ideology of hate and terror

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

"These are sensitive moments. The situation is serious; let us not fool ourselves ... when the people in India feel this is 9/11 for India."

Shah Mehmood Qureshi
Pakistan Foreign Minister
Reuters News
29 November 2008

"The Congress calls upon Pakistan to honor its commitment and prevent the use of its territory for commission of acts of terrorism against India."

Manmohan Singh
Indian Prime Minister
Reuters News
29 November 2008

"There is perhaps a [gap] that exists and we will work to sort this out. There is a systemic failure which needs to be taken stock of. We are fully conscious of it and the debate. The point is it is a serious issue ... a serious matter of security."

Admiral Sureesh Mehta
India's Navy chief
Reuters News
2 December 2008

"The problem with terrorism is that information is useful but it is not always something that you can prevent."

Condoleeza Rice
US Secretary of State
Reuters News
2 December 2008

"Money is the lifeblood of terrorism. The jury's decision demonstrates that US citizens will not tolerate those who provide financial support to terrorist organizations."

Richard B. Roper
United States Attorney
New York Times
24 November 2008

"The international community should give us a timeline of how long or how far the 'war on terrorism' will go. If we don't have a clear idea of how long it will be, the Afghan government has no choice but to seek political solutions [such as] starting to talk to Taliban and those opposing the government."

Hamid Karzai
President of Afghanistan
Al-Jazeera News
25 November 2008

"Hezbollah has three times the ability it had before the second Lebanon war [July 2006] and now has 42,000 missiles in its possession, as opposed to the 14,000 it had before the war. It has missiles that can reach the towns of Ashkelon, Beersheba and Dimona [in the South]."

Ehud Barak
Israeli Defense Minister
BBC World News
24 November 2008

India By Peter Lewis - Australia, Politicalcartoons.com

By Paresh Nash – The Khaleej Times, UAE

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	**Deadly Mumbai Attacks Kill 183.** Residents of Mumbai are in mourning after a series of attacks around the city left at least 183 people dead.	Late Wednesday night, Mumbai, India found itself the target of a ferocious terrorist attack. Ten young gunmen entered Mumbai in small inflatable boats on Wednesday night, carrying bags filled with weapons and ammunition, and spread out to nine locations to begin their attacks. Lobbing grenades and firing their weapons, they entered hotels, a railway station and several other buildings, killing scores and wounding even more in a 60-hour-long siege. Based in part on the confessions of the only terrorist captured alive—Azam Amir Kasav (aka Ajmal Qasab), Indian officials say that the 10 gunmen involved, were all members of Lashkar-e-Taiba, a Pakistani militant group with links to the disputed Himalayan region of Kashmir—though Pakistan officially denies any involvement. According to recent reports, the 10 attackers were responsible for the deaths of 183 people, including 22 foreigners, and 240 wounded. While mourners of the victims attended to their loved ones, and people all over the world held vigils, a Muslim graveyard in Mumbai refused to bury the nine dead gunmen, saying that they were not true followers of the Islamic faith.
	Cadets Among 36 Killed in Iraq Blasts. Bombers targeting Iraqi and US security forces cut a deadly swath across Iraq yesterday, killing as many as 36 people, including 15 police cadets slain at a police academy in Baghdad.	The day's killings pointed up the volatility in Iraq as it heads toward two milestones: provincial elections on 31 January and the pullback of US combat troops from cities and towns by 30 June. The attacks show the challenges awaiting Iraqi security forces when Americans draw down. In the northern city of Mosul, a car bomb targeting a patrol by US and Iraqi security forces blew up shortly before noon. US officials said nine Iraqis, including the bomber, were killed. Four American troops and two Iraqi national policemen were wounded, said a military statement. Iraqi officials in Mosul put the death toll at 15.
Uncertain effects	**"Systemic Failure" Led to Mumbai Attacks.** The Indian navy said a "systemic failure" of security and intelligence services led to the Islamist militant attacks in Mumbai that killed 183 people.	India's police, coast guard, and intelligence communities are pointing fingers over whether information existed that could have been acted on to prevent the 3-day rampage in the financial hub. Intelligence sources said they had issued a series of warnings of a possible attack on Mumbai by sea in the months leading up to last week's strike. The latest, warning that the "sea wing" of Pakistani-based militant group Lashkar-e-Taiba was planning to attack, was issued just 8 days before. Many Indians have expressed anger at apparent intelligence lapses and a slow reaction by security forces to the attacks against Mumbai's two best-known luxury hotels and other landmarks in the city of 18 million.
Positive effects on the GATE	**New Chemical Ali Death Sentence.** An Iraqi court has sentenced to death Ali Hassan al-Majid, also known as Chemical Ali, for his role in crushing a Shia uprising in 1991.	It is the second death sentence passed on Majid, a cousin of Saddam Hussein. The court also condemned a senior Baath Party official, Abdulghani Abdul Ghafour, to hang for the same crime. In February, Majid was condemned to hang for genocide over the killing of 100,000 people during the 1988 Anfal campaign against Iraq's Kurds. The latest verdicts were issued after a trial that heard harrowing testimony of how the Iraqi army crushed the rebellion by Iraq's Shia community. The uprising followed Saddam Hussein's defeat by US-led forces in the first Gulf War in 1991. Witnesses told of mass executions and family members being thrown from helicopters. Ten other defendants received sentences ranging from 15 years to life in prison. It is estimated that as many as 100,000 people were killed as troops carried out massacres around the Shia holy cities of Najaf and Karbala, and shelled towns and villages across southern Iraq in the campaign.

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.