Winter 2007
Volume 9
Number 3

The Guardian

The Source for Antiterrorism Information

In This Issue

3 VaraT: Vulnerability Assessment Reporting and Analysis Tool

6 Choosing Words Carefully: Language to Help Fight Islamic Terrorism

9 ISAF Biometrics

17 EOD/LIC Technologies: Weaponized Bot Rolls into Battle

21 31 Wins, 6 Losses, and 1 Tie: The ABA Journal's Scorecard of the Justice Department's Legal War Against al Qaeda

24 Lessons Learned: The Fort Dix Six

28 Notes from the War on Terror

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

The Pentagon, Room MB917
Washington, DC 20318

Report Documentation Page

Form Approved
OMB No. 0704-0188

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE **2007**	2. REPORT TYPE	3. DATES COVERED **00-00-2007 to 00-00-2007**
4. TITLE AND SUBTITLE **The Guardian. Volume 9, Number 3, Winter 2007**		5a. CONTRACT NUMBER
		5b. GRANT NUMBER
		5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)		5d. PROJECT NUMBER
		5e. TASK NUMBER
		5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Deputy Directorate for Antiterrorism/Homeland Defense,Antiterrorism/Force Protection Division,The Pentagon, Room MB917,Washington,DC,20318**		8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)		10. SPONSOR/MONITOR'S ACRONYM(S)
		11. SPONSOR/MONITOR'S REPORT NUMBER(S)
12. DISTRIBUTION/AVAILABILITY STATEMENT **Approved for public release; distribution unlimited**		
13. SUPPLEMENTARY NOTES		
14. ABSTRACT		
15. SUBJECT TERMS		

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**31**	

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std Z39-18

"In this war, we're on the offensive against the enemy—and that's the only way to be. We'll fight them in foreign lands so we don't have to face them here in America. We'll pursue the terrorists across the world. We'll take every lawful and effective measure to protect ourselves here at home. In an age when terrorist networks and terrorist states are seeking weapons of mass destruction, we must be ready to defend our nation against every possible avenue of attack."

—President George W. Bush
23 October 2007

"These two Americans [William Buckley, Central Intelligence Agency station chief in Beirut, Lebanon, and LtCol William Higgins] were murdered by the same Hezbollah-linked extremists who killed hundreds of Americans in 1983 at the Marine barracks and US embassy in Beirut. It is important to remember that until the morning of September 11, 2001, Hezbollah had been responsible for the deaths of more Americans, our countrymen, than any other terrorist group in the world.

Now we must deal with an even more deadly threat. Since al Qaeda attacked America nearly 6 years ago, our armed forces have been tasked with removing hostile regimes and booting out terrorist networks in Iraq and Afghanistan; initially quick military successes that in both cases have led to protracted stability and reconstruction campaigns against brutal and adaptive insurgencies."

—Secretary of Defense Robert Gates
18 July 2007

"It takes me to two aspects of terrorism: one in Iraq and one in Afghanistan. There's been discussion recently in the last few days about the health of al Qaeda in Iraq. And they're clearly not as capable as they were. They've suffered a lot of losses in Iraq over the period of the last many months or a year or so. But they are still there, they're still dangerous and by no means are they going away. Nor can we take them for granted.

As that translates to whether that creates more [terrorists] or not, I honestly don't know. Where they are? I honestly don't know that. Clearly, I do worry, have for a long time, about this war creating many, many more converts over time. But I just don't have a good feel for that.

Secondly, in Afghanistan with the Taliban—again, it's still a very lethal, capable force that I worry about. But we also had some success against them over the course of this year. And I'm encouraged by that success in terms of our focused efforts to kill as many of them as we possibly can. And in the long run, if an organization starts losing, then it might—I guess my hope would be that there wouldn't be droves continuing to sign up.

But I'm clearly not here to say that the tide has turned in either place or that they're defeated in either place. But we've had considerable success in both places, and I'm encouraged by that. We still have an awful lot of work to do."

—Chairman of the Joint Chiefs of Staff ADM Mike Mullen in an interview with the *New York Times*
19 October 2007

Guardian readers, I am requesting your assistance in evaluating this magazine. Please spare a few minutes of your time to go to http://guardianfeedback.xservices.com, rate the effectiveness of *The Guardian,* and give me some suggestions on ways to improve it. I know your inputs can help me make this magazine a better "all hazards" tool.

Since the last edition of *The Guardian,* several major terrorist efforts have been disrupted, most notably the Islamic Jihad Union plot in Germany. These arrests and the recent convictions from the Madrid train bombing serve as a reminder of the nature of the threat and the role of both law enforcement and society in fighting violent extremism. While it may be easier to understand the threat when it emanates from another country plagued by internal societal ills, it is more difficult to comprehend the origin of indigenous plots.

There are three hard-core facts to keep in your crosscheck. First, the danger posed by insurgents and terrorists is ever-present as these groups adapt and adjust in an effort to get at us. Second, the implied *must* task for every commander is to protect forces. Third, we, as a nation, need to make the hard preparations to fight this enemy in the homeland. The danger is evident in the enemy's use of improvised explosive devices, snipers, and ambushes against our Soldiers, Sailors, Airmen, and Marines downrange. Not so evident, perhaps, but on our horizon nonetheless, is the manifestation of this threat on our soil. Our law enforcement partners have actively taken on this threat, and DOD has a significant part to play as well. In the recent interagency national-level exercise, military units executed consequence management and force protection missions in response to a series of radiological dispersal device attacks against the United States. The exercise experience posits some important questions for you and your unit. Most of our CONUS force protection efforts counter the design-basis threat—but are *you,* at the unit and installation level, ready to respond to these kinds of incidents? As we ensure our installations are prepared, are *you* prepared when you are off duty and off post? Do *you* have a personal AT plan for you and your family?

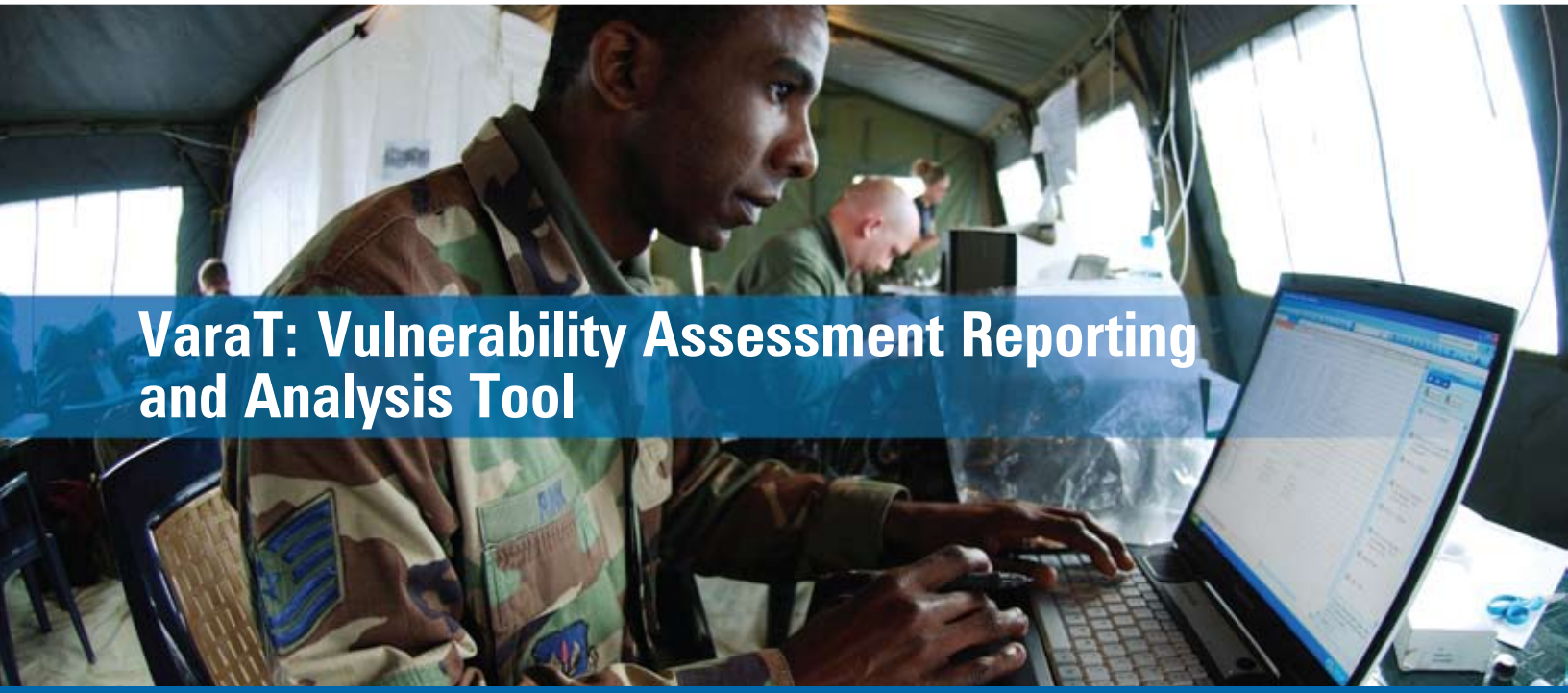
Lastly, I want to make sure that you, as AT and FP professionals, are getting the help you need from the J-34. If you require assistance in CbTRIF, Higher Headquarter Assessments, DOD AT Policy, Training (Level I-IV), Law Enforcement, Biometrics, Forensics, or MANPAD defense, please contact me or my staff, and we will be sure to get you the answer to your questions as well as the right help you need.

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

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

SUBMITTING NEWS & ARTICLES

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



VaraT: Vulnerability Assessment Reporting and Analysis Tool

By Caroline Neely and Peggy McCarthy, DTRA OP-CSAS

Caroline Neely and Peggy McCarthy are analysts assigned to the DTRA Combat Support Assessments Division, Support Branch. They have been working with JSIVA teams and conducting analysis on JSIVA data since 1998.

Strategic Concept for Entry Control Operations

The number of vulnerability assessments (VAs) conducted throughout the DOD has increased tremendously since the inception of the AT/FP program in 1997. The result is a large collection of VA observations highlighting ways in which US installations are at risk of potential terrorist attacks. As the amount of data has increased, the need has arisen to look at this body of information in a meaningful way. In order to accomplish that, VA observations need to be collected in a standardized format.

The Vulnerability Assessment Reporting and Analysis Tool (VaraT) is a new software application designed to assist assessors in the reporting process. It also provides policymakers with the ability to perform cross-organizational analysis on all VAs, including Joint Staff Integrated Vulnerability Assessments (JSIVAs), Higher Headquarters assessments, Service and combatant command VAs, and assessment data from a variety of other DOD organizations. VaraT will allow each organization to build its own unique assessment model and report structure. At the heart of VaraT is an analytic ontology that allows organizations to map their unique assessment models to a central data structure. This approach will help decisionmakers get a more in-depth and accurate picture of the overall DOD AT/FP posture.

How Can VaraT Help?

VaraT can assist organizations in a number of ways. First, it will facilitate the creation of standardized assessment reports through collaborative tools, intuitive data-entry screens, and timesaving job aids. Second, once reports are completed, VaraT assists organizations in uploading their data into the Core Vulnerability Assessment Management Program (CVAMP). Instead of Antiterrorism Officers (ATOs) having to retype all VA report observations into CVAMP, the file produced by VaraT can be uploaded automatically. Finally, VaraT provides organizations with additional trend analysis functionality. Using robust search engine and flexible reporting tools, VaraT offers novice and experienced analysts a variety of analytical capabilities to create products that are customized to fit each organization's needs.

VaraT is a new software application designed to assist assessors in the reporting process.

Background

Since 1998, JSIVA teams have been using JIS (JSIVA Information System) software that facilitates the report-writing process and puts information into a searchable database for analysis. JIS was originally designed to meet the needs of the JSIVA teams and support their assessment and report-writing process; however, a multitude of other organizations also began to use JIS. As a result, technical limitations of

the software became apparent because JIS could not be modified without additional cost to meet the needs of alternative assessment methodologies. The ability to put VA data into a database format and produce a final report was still needed. In addition, in 2005, JIS functionality increased when it allowed users to create an XML file allowing reports to be directly uploaded into CVAMP.

In 2007, leadership at the Joint Staff and the Defense Threat Reduction Agency (DTRA) decided it would be beneficial to replace the antiquated JIS software with a more flexible and analytically powerful application that would complement the risk management capabilities already present in CVAMP. The new software, called VaraT, would be built on a more modern technology stack than JIS and would allow users to customize the frameworks of their assessments while maintaining a common data-capture construct. This structure would allow for analysis among the various assessment types. The more assessment teams use VaraT to produce their reports, the richer the analytic products are for gauging the health of the AT/FP program DOD-wide.

The more assessment teams use VaraT to produce their reports, the richer the analytic products are for gauging the health of the AT/FP program DOD-wide.

How Was VaraT Developed?

The VaraT development process was a collaborative endeavor between government subject matter experts and the contractor team of Analytic Services (ANSER) and Leftbrain, Inc. ANSER analysts assisted JIS users for almost 9 years and had unique insight into the prevalent user complaints from that legacy system. Moreover, ANSER analysts have conducted trend analysis on JSIVA data since the program's inception and have an intimate understanding of the nature of the VA data and its information management life cycle.

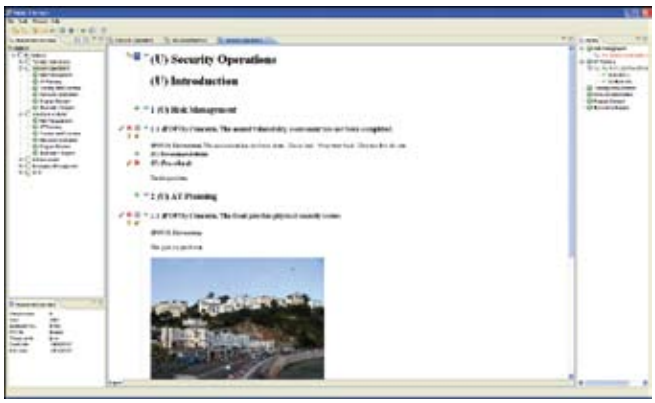
The development team elicited requirements from the user community in a number of ways, including an electronic survey, workshops, and interviews with assessors within the DTRA and other Services and combatant commands. The team tried to reach out to as much of the antiterrorism community as possible in order to understand the needs of the users. Using this in-depth understanding and compilation of inputs gathered from the user community, the VaraT development team created a prototype application. The prototype was reviewed by a smaller user group, and their inputs were incorporated into the final version of the software. In addition, conference room pilots were performed by assessment teams to test the functionality of VaraT in a simulated assessment environment. The result is an application that meets the varied needs of the AT/FP user community.

The VaraT Software Suite

The VaraT software suite is comprised of two components: a desktop application and a web application. The desktop application, known as VaraT Remote, allows assessors to collect data and produce the final report. Using the latest technology, VaraT Remote provides an improved user experience over the JIS application by offering more word processing-like functionality and more report views. The application also offers customizable views for each user to adjust to his or her preferences.

The key functional capabilities of VaraT Remote are—

- **Writing the report:** VaraT Remote is the primary application used to write and produce an assessment final report. Design for this aspect of the software focused on making the experience closer to writing in a word processing program than in a database and took advantage of the timesavers offered by a database-driven application. For example, VaraT Remote allows users to build a library of frequently used observations, called "My Favorites," that can easily be added into the report in which they are currently working. The VaraT Remote screen is composed of a series of adjustable panels and collapsible text to provide the assessor with a variety of ways to navigate and view the assessment report.



VaraT Remote

- **Consolidating team member inputs:** One of the most challenging aspects of producing a report with more than one author is figuring out a way to combine each author's section and keep track of revisions and versions of the document. VaraT offers a user-friendly solution to this obstacle in both the desktop and web applications. Using an iPod-like synchronization technology, users can export their data to a data transfer medium such as a thumb drive or CD. When the user inserts the medium into a computer, VaraT recognizes data to be imported, and an auto-run feature prompts the user to accept or reject the import.

In this way, data can be seamlessly transferred among multiple members of an assessment team. The same technology is also used to transfer updated configuration files from VaraT Web to VaraT Remote. For example, a change in the report model could be exported from VaraT Web onto a CD. Any VaraT user could put the CD into a computer's CD drive and select "OK" during the auto-run process, and that computer would be automatically updated.

VaraT Web is a web-based application residing on the SIPRNET, which is the central warehouse of VA information. It is also the application that allows organizations to create unique assessment models, maintain user information and other control data, and take advantage of the online editing workflow process. Most importantly, VaraT Web provides analysts with the tools they need to take a more accurate and in-depth look at VA data.

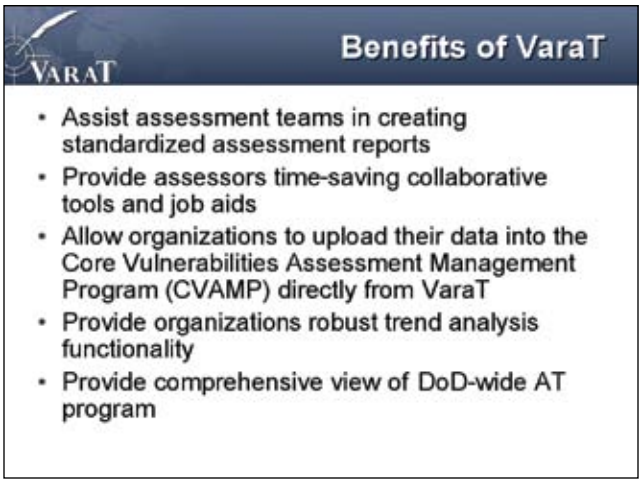
The key functional capabilities of VaraT Web are—

- **Creating assessment models:** The creation of an assessment model in VaraT includes the ability to select organization-specific logos, report introductions, annexes and subannexes, and analysis criteria. Users can also choose to perform an observation-based assessment, such as a JSIVA, or a checklist-based assessment similar to the Joint Staff's Higher Headquarters assessments. In addition to the reporting flexibility, the model allows organizations to create their own categories for analysis. In this approach, organizations map their own analysis categories, such as benchmarks and standards, to the VaraT master list. This mapping allows organizations to do their own analysis while, at the same time, allowing the Joint Staff to perform cross-organizational analysis using the master ontology. The ability to create models is limited to system administrators and can be propagated to the assessors' machines on which VaraT Remote is installed.
- **Editing workflow:** When the report has been completed by an assessment team, VaraT Web provides users with a customizable, collaborative environment in which the editing workflow process can auto-generate e-mail reminders and track the status of the report until it is ready for distribution.
- **Analyzing assessment information:** A goal of VaraT is to provide organizations with the ability to perform their own analysis on data collected during their assessments. In addition, VaraT provides DOD leadership with the ability to perform cross-organizational analysis by using an ontological approach to database design. VaraT provides organizations with the ability to add their own unique categories for analyzing their data but requires them to link the additions to the master VaraT categorization. This requirement ensures that the disparate assessment processes can still offer a "big picture" of the AT/FP program.

VaraT also offers multiple types of analysis reporting options, from text reports to charts and tables. Basic users can select from a list of predetermined and frequently used analysis reports. The system also offers more advanced users the ability to customize reports to meet their unique analysis needs. All of the data from VaraT reports can be easily exported into applications within Microsoft Office.

VaraT Web provides analysts with the tools they need to take a more accurate and in-depth look at Vulnerability Assessment data.

VaraT is designed to assist assessors in the reporting process and provide policymakers with the ability to perform cross-organizational analysis on all VAs.



This application will help decisionmakers get a more in-depth and accurate picture of the AT/FP program in terms of areas of responsibility as well as an overall DOD view.

Technical Requirements

Installation of VaraT requires a current-model laptop or desktop computer with 1 GB RAM and 2 GB free disk space, Windows XP, and Office 2003.

How Can I Get VaraT?

VaraT is government-owned software and can be obtained at no cost to government organizations. For more information on how to obtain VaraT, e-mail ATFPHelp@dtra.mil.

Choosing Words Carefully: Language to Help Fight Islamic Terrorism

By Douglas E. Streusand, PhD and LTC Harry D. Tunnell IV, USA,
National Defense University Center for Strategic Communications

This article was originally published by the National Defense University.

The United States must do more to communicate its message. Reflecting on Bin Ladin's success in reaching Muslim audiences, Richard Holbrooke wondered, "How can a man in a cave outcommunicate the world's leading communications society?"[1]

Use Precise Terms Precisely

The answer to Mr. Holbrooke's question is an unsophisticated one: Bin Ladin speaks in a language that his Muslim listeners understand. We, on the other hand, simply do not comprehend the meaning of many words that we use to describe the enemy. American leaders misuse language to such a degree that they unintentionally wind up promoting the ideology of the groups the United States is fighting.[2] We cannot win widespread support throughout the Muslim world if we use terms that, to them, define the behavior of our enemies as moral. Because the Global War on Terrorism—or more precisely the war against Islamic totalitarian terrorism—includes a war of ideas, leaders, journalists, authors, and speakers must use the most accurate terms to describe those ideas.

The responsibility for precision in expression rests with anyone who believes in the need to share information candidly. But for those unfamiliar with Islamic doctrine, history, and tradition, it may often be necessary to rely on scholars or other experts about the Islamic world to provide one with the necessary guidance to help convey the message correctly. Muslims will ultimately determine whether the ideology of al Qaeda, its affiliates, franchisees, and fellow travelers represents authentic Islam or not, but the West can have enormous influence on their decisions. Furthermore, it is important to make sure that the civilian community in the United States and that of our allies and coalition partners accurately understands the nature of the enemy that we are fighting. Unfortunately, Western governments, intellectuals, and journalists commonly use words that inadvertently (or sometimes deliberately) authenticate the doctrines of our enemy as truly Islamic. Correcting this vocabulary is a necessary step to educate the wide-ranging groups who are affected by the war; to discredit those who either passively or actively, wittingly or unwittingly, support Islamic totalitarian terrorism; and to reveal the truly insidious nature of our enemy.

What Are We Really Saying?

This essay discusses the most egregious and dangerous misuses of language regarding Islamic totalitarian terrorists; a comprehensive study would require a book. We begin with the word *jihad*, which literally means striving, and generally occurs as part of the expression, *jihad fi sabil illah*, striving in the path of God. Striving in the path of God is a duty of all Muslims. Calling our enemies *jihadis* and their movement a global jihad thus indicates that we recognize their doctrines and actions as being in the path of God and, for Muslims, legitimate. In short, we explicitly designate ourselves as the enemies of Islam.

Muslims have debated the meaning and application of the concept of jihad for centuries. Our application of the term to the actions of our enemies puts us on

their side of the debate. We need not concern ourselves with the identification of the original or legally correct meaning of the term; individual Muslims will make up their own minds. As Professor Streusand has previously written, "Classical texts speak only to, not for, contemporary Muslims." It is also important to note that opposing jihad, a basic principle of Islam, violates a classical text of our own. The United States Constitution denies our government the ability to prohibit the free exercise of religion; consequently, we should never use a term, such as jihad, that misstates our current and historical position on religion.

Mujahid (plural *mujahidin* or *mujahideen*): One who participates in jihad, and frequently translated in the American media as "holy warrior." The use of this term designates the activity of the enemy as jihad and thus legitimizes it. It was quite proper for us to describe the warriors who resisted the Soviet invasion of Afghanistan as mujahidin, many of whom are now our allies in Afghanistan. To extend the term to our current enemies dishonors our allies as well as authenticates our opponents as warriors for Islam. Even to a Western audience it can lend a sense of nobility to an otherwise ignoble enemy.

Caliphate (*khlilafa* [or *khilafa*]): This term literally means successor and came to refer to the successors of the Prophet Muhammad as the political leaders of the Muslim community. Sunni Muslims traditionally regard the era of the first four caliphs (632–661) as an era of just rule. Accepting our enemies' description of their goal as the restoration of a historical caliphate again validates an aspect of their ideology. Al Qaeda's caliphate would not mean the re-establishment of any historical regime; it would be a global totalitarian state. Anyone who needs a preview of how such a state would act merely has to review the conduct of the Taliban in Afghanistan before September 11, 2001.

Allah: The word Allah in Arabic means the God—nothing more, nothing less. It is not specifically Muslim; Arabic-speaking Christians and Jews also use it. In English, Allah should be translated as God, not transliterated. While translation emphasizes the common heritage of Judaism, Christianity, and Islam (the three faiths that identify their God as the God of Abraham), it does not imply that the Abrahamic faiths share identical concepts of God. Even though some Muslims use Allah rather than God in English, the practice exaggerates the divisions among Judaism, Christianity, and Islam.[3]

Because the Global War on Terrorism—or more precisely the war against Islamic totalitarian terrorism—includes a war of ideas, leaders, journalists, authors, and speakers must use the most accurate terms to describe those ideas.

What Are the Right Words for the Job?

Now that a few unsuitable word choices have been addressed, it is time to begin to identify the proper expressions to use whenever discussing the global Islamic totalitarian terrorist movement. Many of these terms will be unfamiliar to Westerners, but not to most Muslim audiences. Only those who actively, passively, or even unwittingly support al Qaeda's (and similar groups') professed goals would find the terms, and their use by non-Muslims, offensive.

To refute challenges to the new context surrounding these expressions, any user of these terms must be able to define the words in order to defend their accuracy and the appropriateness of their use. Otherwise, anyone who dares to define the enemy using its own Islamic language can be challenged by a variety of "pundits" who still see the struggle in terms of religion or poverty rather than political ideology; who despise Western society, capitalism, or democracy; or who oppose the war for any other reason.

Hirabah: This word, which is derived from the Arabic root that refers to war or combat, means sinful warfare; warfare contrary to Islamic law. There is ample legal justification for applying this term to Islamic totalitarian terrorists and no moral ambiguity in its connotation. We should describe the Islamic totalitarian movement as the global hirabah, not the global jihad.[4]

Mufsid (*moofsid*): This word refers to an evil or corrupt person; the plural is *mufsidun.* We call our enemies mufsidun, not jihadis, for two reasons. Again, there is no moral ambiguity, and the specific denotation of corruption carries enormous weight in most of the Islamic world.

Fitna, fattan: Fitna literally means temptation or trial but has come to refer to discord and strife among Muslims; a fattan is a tempter or subversive. Applying these terms to our enemies and their works condemns their current activities as divisive and harmful.[5] It also identifies them with movements and individuals in Islamic history with negative reputations such as the assassins of the Caliph

Calling our enemies jihadis and their movement a global jihad indicates that we recognize their doctrines and actions as being in the path of God and, for Muslims, legitimate. We should describe the Islamic totalitarian movement as the global hirabah, not the global jihad.

`Uthman in 656, who created the first fissure in the political unity of the Muslim community.

Totalitarian: Calling our enemies totalitarian serves several purposes. There is no such thing as a benign totalitarianism. Totalitarianism is a Western invention, and it appeared in the Islamic world as a result of Western influence (first fascist, then Marxist–Leninist). It is also in direct contrast to the idea that the enemy would actually establish a caliphate if they defeat the United States, our allies and coalition partners.

Not the Last Word, Just the Beginning

This essay is neither definitive nor complete. It is only the beginning of a "primer" of the terminology used to describe Islamic totalitarian movements. There should be far more discussion about the right words to use to describe the variety of threats posed by transnational terrorists—Islamic groups and others. This article, we hope, will help jumpstart the discourse.

Notwithstanding the fact that this article is a small beginning, the terms proposed herein should become an indispensable part of the vocabulary of America's leaders, reporters, and friends immediately. The wrong terms promote the idea that terrorist elements represent legitimate Islamic concepts, which in turn might aid in the enemy recruitment of disenfranchised Muslims because we have identified to them a seemingly "traditional" outlet through which they can voice their dissatisfaction. It is essential to use the right language to address worldwide problems so that various audiences—which include the American Muslim community—understand the full scope of the problem and are intellectually able to identify with potential solutions that are reasonable and ethical.

This paper offers word choices not just for public officials and correspondents but even students in the classroom and others studying terrorism. In fact, anyone who is interested in current events should have some familiarity with these words as well as the concepts and new dialogue they represent. We must use the right turn of phrase whenever attempting to inform and educate; language is a key component for us to be able to, in a way that makes sense to any audience, ask for assistance or demand action that will help defeat the scourge of Islamic totalitarian terrorism.

---

1 National Commission on Terrorist Attacks Upon the United States. *The 9/11 Commission Report.* W.W. Norton & Co., New York, undated, p. 377.

2 The 9/11 Commission's own report is guilty of this by using *jihad* (and other variations of the term such as *jihadists*) throughout. Jihad, discussed more in detail later, does not have a negative connotation for most Muslims—even when combined with descriptions of terrorist purpose or action.

3 See Daniel Pipes, "Is Allah God?," *FrontPage Magazine*, June 28, 2005, at http://www.frontpagemag.com/Articles/ReadArticle.asp?ID=18577

4 James Guirard of the TrueSpeak Institute explains the reasons for using the term *hirabah* rather than *jihad* in "Terrorism: Hirabah versus Jihad: Rescuing Jihad from the al Qaeda Blasphemy," *American Muslim,* July–August 2003, available at http://www.theamericanmuslim.org/tam.php/features/articles/terrorism_hirabah_versus_jihad_rescuing_jihad_from_the_al_qaeda_blasphemy
Guirard's approach underlies this entire article.

5 For example, the former leader of al Qaeda in Iraq, Abu Musab al-Zarqawi, stated that Shiites are *rafada,* or rejecters of Islam. The Salafist Sunni terrorist groups, the most well known of which is al Qaeda, do not recognize other traditional Islamic sects as acceptable or as Muslims. Use of rafada is from Fouad Ajami, "Heart of Darkness," *Wall Street Journal,* September 28, 2005, p. 16, as cited in the online version of *The Early Bird,* available at www.us.army.mil/suite/earlybird/sep2005/e20050928393978.html, accessed September 28, 2005. The al Qaeda attack of civilian weddings at three hotels in Amman, Jordan, on November 9, 2005, is another case in point of terrorist attempts to promote discord among Muslims. The attacks killed 57 people and wounded 115, the majority of whom were Jordanian and Palestinian. Direct attacks by al Qaeda in Iraq against Shiite holy sites throughout Iraq continue as of February 28, 2006. [Editor's note: Attacks against Shiite holy sites in Iraq continue, with the last major attack occurring in June 2007 in Samarra.]

This article is available online as part of the US Army Professional Writing Collection, at www.army.mil/professionalwriting/volumes/volume4/july_2006/7_06_4.html

ISAF Biometrics

By Todd Chappell

Todd Chappell is a senior policy analyst within the Joint Staff J-3, Deputy Directorate for Antiterrorism and Homeland Defense. He previously served as chief of Counter IED intelligence and biometric program support within the North American Treaty Organization's (NATO's) Supreme Headquarters Allied Powers Europe (SHAPE) J-2.

February 2007 marked a significant step forward in the Global War on Terror: By the end of that month, the International Security Assistance Force (ISAF) in Afghanistan, led by the North Atlantic Treaty Organization (NATO), had fielded US biometric equipment called the Biometric Automated Toolset (BAT) and the Handheld Interagency Identification Detection Equipment (HIIDE) as part of ISAF force protection and overall security efforts. The provision of US equipment and biometric data to allies epitomizes information sharing, facilitates clear identification of threats, and sets the stage for the greater international fight against transnational criminal and terrorist networks. Recognizing the significance of the effort, the United States should provide dedicated support to ensure continued effectiveness and momentum until NATO can field its own system.

Background and Fielding Issues

The interim provision of US equipment to ISAF is straightforward: The loan will extend until NATO develops comparable capability, estimated for sometime in 2008. The initiative emerged in late 2006 from a Supreme Headquarters Allied Powers Europe (SHAPE) request of visiting US defense intelligence officials. After validating requirements with senior ISAF staff in December 2006, SHAPE worked with representatives from Joint Forces Command Brunnsum, US Central Command (CENTCOM), Combined Joint Task Force (CJTF) 76, CJTF 82, and the Biometrics Task Force to get the equipment and training in place in Afghanistan. ISAF issued execution guidance and arranged for representatives from all major ISAF locations in Kabul, Afghanistan, to attend training at Kabul International Airport in February. The training itself was routine yet spectacular in that US field support engineers taught more than 30 representatives from 10 allied nations how to employ the BAT. Within days, systems were in place and using data from a central ISAF database.

Months later, using both BAT and HIIDE, ISAF allies have enrolled over 3,700 people and identified potential individual threats, including foreign nationals previously identified in Iraq and others who had been barred from entry to other US or ISAF locations. Success is a tribute to the hardworking ISAF, CENTCOM, and CJTF 82 representatives and their

leadership who see the value of the initiative, not only in short-term force protection efforts, but also in the transnational fight ahead.

The effort is not without shortfalls or criticism on both sides of the Atlantic. Early on, some observers opined that the effort would not work or would not pass the cost–benefit comparison. Others wanted to develop comprehensive NATO doctrine to guide the initiative before fielding any equipment. Similarly, some observers sought to develop an independent NATO system that, among other issues, would avoid any perceived connection to US intelligence or detainee systems. Still others argued that any biometric effort violates European privacy laws or some combination of European Union (EU) requirements for transnational application of EU laws. Those comments, although never echoed by senior leadership or supported in official legal reviews, continually delayed staffing efforts. Having been addressed over time in many forums, those concerns became quieter by June 2007 as common understanding and appreciation of the concept grew.

Other issues have also affected biometric success within ISAF. The lack of dedicated manpower restricts the ability to train and expand the ISAF BAT/HIIDE reach, which remains at least 3 months behind original fielding plans. The agreement between SHAPE and the United States held that US support would be provided, as available, from assets already in Afghanistan. Although not staffed to support ISAF, CENTCOM and CJTF 82 both provide superior support within this framework. With renewed emphasis on the US biometrics program in Afghanistan, the availability of US support for ISAF efforts has decreased. Similarly, steady allied troop rotations complicate planning and overall support requirements. Further, although formal biometric training will support the future NATO biometric system, the effort to train ISAF personnel at Fort Huachuca, Arizona, has also been repeatedly delayed by conflicting ISAF priorities and agendas. NATO has not been able to initiate biometric familiarity training for forces before entering theater; the first such training was scheduled for fall/winter 2007. Consequently, troops arrive in Afghanistan having heard little of the capability or its applications.

Conflicting expectations of allied and US personnel also slow the development process. The US military has used biometrics as a military tool for over four years and has developed many policies and expectations; conversely, NATO just finished its first six months of biometric experience. NATO is just now encountering issues that the United States worked through in 2003 and 2004. Biometric networking requirements are one example. Long-standing NATO information technology policies restrict equipment that can be connected to the network. Those policies have restricted BAT connectivity and have forced ISAF to rely on manpower-intensive "air gap" synchronization of biometric data across locations. The issue is not insurmountable: Efforts are underway to achieve connectivity but must be worked through the NATO process over time. Although the lack of networking hinders data exchange and utilization of the full BAT capability, the access-control benefits of BAT/HIIDE are a significant improvement to overall ISAF force protection, even in stand-alone mode, and merit continued fielding and support. American analysts often view the networking as a critical component of the effort, whereas ISAF considers the basic capability of localized individual identification as significant because fake, shared, or stolen ISAF identification cards or fraudulent Tazkera cards are no longer a large concern and opportunities for large-scale insider attacks have been mitigated.

The provision of US equipment and biometric data to allies epitomizes information sharing, facilitates clear identification of threats, and sets the stage for the greater international fight against transnational criminal and terrorist networks.

The "stand-alone versus networking" debate delays efforts by confusing priorities. Undoubtedly, the system will be more effective once it is networked across all locations and sharing information in real time. Until ISAF is comfortable with and capable of expanding this role, the systems provide positive value in a stand-alone mode and collect data that will be useful when the systems are eventually networked. ISAF's deployment of a compatible system is a significant capability that should not be delayed or overlooked while waiting for some future network capability.

An informal expectation exists within some US ranks that NATO and ISAF should adopt US policies and processes based on the US experience. NATO and ISAF welcome the US experience with biometric systems and rely on American expertise to support the systems; however, the systems and processes in use at ISAF must reflect ISAF and NATO capabilities, expectations, and policies. In NATO, the United States is just one of 26 equal partners, and NATO policies remain a reflection of all 26 nations.

US Marine Corps Lance Cpl. Brian Gamble, from India Battery, 2nd Battalion, 10th Marine Regiment, uses a biometrics automated tool set to renew a man's identification badge in Al Nuammia, Iraq, June 20, 2007. [http://www.defenselink.mil]

Information Sharing

Information sharing is a basic requirement for effective alliances. Logically, in order to develop a cohesive strategy, alliance members should operate from similar assumptions and outlooks. Along this line of thought, Jamie Shea, Director of Policy Planning in the Office of the Secretary General at NATO, cites better intelligence sharing as a requirement for the future of NATO and as a way to make political deliberations more effective.[1]

While some observers were seemingly impressed by the cost and scope of the United States' voluntary contribution of biometric equipment and support, the provision of the US biometric database and data to ISAF is the epitome of information sharing. The United States provided a database that included innumerable files of raw data concerning people who constitute potential threats in the War on Terror. The information will remain NATO property and actually resides in the hands of allies who participate in ISAF operations. Significant to the exchange, the United States provided the files as entered by US technicians when created, without significant scrutiny or revision.

Information-sharing requirements of the modern era demand this level of detail and trust as opposed to the traditional exchange of polished intelligence that has been re-tuned and scrubbed so often that the substance and timeliness of the issue are lost. This instance of biometric data sharing is not only a testament to US leaders and their far-reaching vision, but also a tribute to the faith that the US maintains in its enlisted and noncommissioned officer corps. Every BAT operator is now, essentially, involved in the international exchange of information. Beyond the provision of equipment, the quality and scope of the raw information provided demonstrate that the United States is unequivocally dedicated to the well-being of its allies and partners.

Threat Identification

Biometrics will help clarify who the enemy is in Afghanistan by providing links among activities and allowing the Afghan government and allied forces to focus on genuine problems. This capability is critical, because although many observers give a knowing nod to the myriad tribal, clan, criminal, regional, economic, social, cultural, religious, and national factors that

influence Afghanistan politics, few seemingly understand their actual significance. Consequently, large volumes of threat activity in Afghanistan continue to be attributed to the Taliban when the Taliban, or even al Qaeda or Hezb e Islami Gilbuddin (HIG), had little or nothing to do with the efforts.

Connecting geographically separate attacks, such as improvised explosive device (IED) attacks, to individual people will also be significant in qualifying the threat.

Distinguishing who is responsible for activity is critical if the government of Afghanistan is expected to address root causes of violence and achieve broader stability and security across the country. The individual motivations for attacks, whether by subelements of a Hotak clan, by regional warlords, by criminal opportunists, or by government representatives seeking greater influence, must be identified so that they can be addressed. The capability of pinpointing responsibility for actions without racial or regional generalizations will be the ultimate test of legitimacy for a central government charged with overseeing such a patchwork of interests. Any broader categorization of the enemy as "Taliban" is usually the result of convenience, analytical apathy, or ignorance, and undermines the mission. As the use of fingerprints moves investigations in the United States from discussions of organized crime to individual people and specific networks, biometrics will help to refine analysis and reduce opportunities to attribute threat activity incorrectly.

Although some people argue that the term Taliban is just a category of threat, they fail to recognize the political significance that the term conveys. The word Taliban is derived from the word for student, Talib, and is associated with those studying Islam. As such, it is a positive term for some people, especially Pashtun in the south and east. As a movement, the Taliban under Mullah Omar essentially saved much of Afghanistan from factional violence during the 1990s and was credited with bringing stability to at least the southern part of the country. The Taliban subsequently oversaw large swaths of the country for years, so many families, clans, villages, and regions have some affiliation or connection to the Taliban label overall. In spite of this connection, which was necessary for daily life, there was little support for the overall ideological structure. As demonstrated in 2001–2002, Afghans quickly rallied to oust the Taliban governance.

In the current environment, those old connections to the Taliban label remain through tribal, family, or regional fact and are superimposed on local competition for resources, power, and influence, not to mention the preexisting family, criminal, or tribal rivalries. Mullah Omar has little or no influence on these micro localized issues. Overattribution of terrorist activity to the Taliban as some grand strategic notion in these diverse regions gives the organization more influence and legitimacy than Mullah Omar could otherwise imagine. Surely certain few people in the outlying areas would benefit from Omar's return, but most of the country would quickly be seeking relief as it was in 2001. Premature categorization of localized groups and issues as Taliban obfuscates the true nature of the threats and virtually forces the regional groups into an irreconcilable category where the only remaining option is to side with the Taliban in order to maintain leader authority or group identity.

This regional orientation of Afghanistan has been well documented over the centuries. Historical accounts, from Alexander, the British, and even the Soviets, repeatedly reveal an opposition of fierce warriors who are characterized by haphazard organization, personal motives, and conflicting agendas. Salient issues and control changed over each mountain pass or even on opposite sides of the same village. This characterization remains true today. Although Omar cobbled together his confederation of power more than a decade ago, its current composition is anything but monolithic. Key uniting Taliban leaders are dead or in hiding. In spite of grandiose statements, Omar has actual command and control over few forces and lacks influence at a tactical level. Aspiring warlords, thriving in the chaos, benefit from having feet in all camps and even notional ties to the Taliban, but have little obligation to the former leader who remains safely hidden. The concept that large numbers of outsiders descend on small villages and get broad support based on ideological or political motives is possible but not at the frequency and magnitude often described. The idea that Afghans can only be 'for us or against us' is naive. In order to truly identify the threats to ISAF and the Afghan government, the individual and localized issues have to be considered outside of any Taliban label.

Reflective of Afghan history, residents in any region are already beholden to local power brokers who provide their services in exchange for some incentive. Vanda Felbab-Brown brilliantly describes this evolution of alliances of convenience and self-interest in the Afghan opium trade in her essay, "From Sanctuaries to Protostates."[2] Although she describes the thugs involved as "Taliban," it requires few intermittent supporters to wave a notional Taliban

standard. The motivation behind attacks is clearly not ideological, and a tangible link to Omar is virtually nonexistent. Indeed, Omar's death will have as little impact on overall Afghan violence as other recent, high-profile Taliban deaths. Regional and individual interests remain the impetus for violence.

From a Western point of view, this reality emerges in the effort to describe an overall Taliban order of battle. The effort has only produced a cluttered graph of bubbles, which some deride as "blobology," indicating tentative enemy numbers and locations. The ineffectiveness of blobology is revealed when allied forces kill large numbers of so-called Taliban in the area but the numbers in the blobs do not change. Large numbers of unlawful enemy combatants acting in opposition to the Afghan government or allied forces could have been killed. They may have been attacking ISAF or Afghan forces as mercenaries, in support of fellow tribesmen or employers, or against a perceived occupation force. That typically makes them justifiably dead, but that does not make them Taliban. As mentioned above, once generalized as Taliban, their motivation is obscured and reconciliation becomes more difficult. Afghan President Karzai's effort to reconcile with certain Taliban elements is commendable. It would be facilitated by ending the use of the broad Scarlet Letter T(aliban) label. Similar broad categories, such as opposing militant forces or insurgents, are not synonymous with Taliban, but prove equally useless because they essentially postulate a common enemy and neglect the influence of tribal, clan, criminal, regional, economic, social, and cultural motivations.

As the use of fingerprints moves investigations in the United States from discussions of organized crime to individual people and specific networks, biometrics will help to refine analysis and reduce opportunities to attribute threat activity incorrectly. Biometrics are key in this environment because they identify a specific person.

Biometrics are key in this environment because they identify a specific person. A person is not a category; he or she personifies race, tribe, clan, and regional factors. Just as police officers do not stop an investigation when they find a connection to organized crime, forces in Afghanistan should not be content to attribute activity to the Taliban. Biometrics, using international technical standards, makes the identification repeatable across locations, regardless of potentially different analytical attributions. The information is also available almost immediately at the tactical level, where it is needed most and has the most direct impact.[3] Biometric data will allow forces to address the particular threat and not just the category of threat. The discussion of whether a person moved from Kandahar to Kabul is no longer theoretical; biometric operations can show that the movement occurred by displaying dates and times the person was biometrically identified in both locations. A biometric collection will likely document individual traits, perhaps including tribal, clan, criminal, regional, economic, and cultural details. Any subsequent detection of this person will have this information as a baseline. Biometrics will put a face on the person and ultimately restrict the propensity to categorize the threat as the Taliban boogeyman.

Mao Zedong said that guerilla fighters must "swim like fish in the sea"; biometrics can pick out the troublemaking fish. As described in a review by Giles Kyser, Matt Keegan, and Samuel Musa, this capability is a force multiplier that will mitigate friendly force deficiencies in demographic or language familiarity and restrict insurgent gains from changing locations. It increases situational awareness, especially at the critical time when forces are in direct contact with the person providing the biometric sample.[4] As awareness and system usage grow, the impact will be as decisive for military operations in the current irregular environment as basic fingerprinting was for law enforcement when the practice was adopted. Because this impact is not an immediate result from the introduction of a single system but the cumulative effect of systematic use over time, the early provision of biometric equipment and data throughout the alliance becomes significant. The longer the capability is in use, the more effective it proves.

As shown in daily television dramas, biometric efforts not only link perpetrators to attacks but also link attacks to other acts. This level of detail, as it grows with corresponding understanding of biometric roles, will allow ISAF forces to apply precise terminology and responsibility for action and share the information effectively with those who need it, including the governments of Afghanistan and Pakistan. As Donald Bolduc and Mike Erwin described in their *Special Warfare* article, "The Anatomy of an Insurgency: An Enemy Organizational Analysis," it is important to recognize the role and position that a person plays in an insurgency. Bolduc and Erwin describe leaders, supporters, fighters, and facilitators and provide examples of the elements of each category.[5] Biometrics will help to place people into those categories based on where or how the biometrics are collected. Understanding a person's role allows the use of different tools to influence that person. Connecting geographically separate

US Army Soldiers from Headquarters, Headquarters Company, 2nd Battalion, 8th Cavalry Regiment, 1st Brigade Combat Team, 1st Cavalry Division use the biometrics automated tool set system to obtain information on volunteers for the civilian infrastructure security in Hor Al Bosh, Iraq, Oct. 16, 2007. *[http://www.defenselink.mil]*

attacks, such as improvised explosive device (IED) attacks, to individual people will also be significant in qualifying the threat. In turn, this capability will allow the government of Afghanistan and its allies to address individual, group, or regional grievances more precisely. Although the war will still be equated to looking for needles in a haystack, the needles will have threads strung among them that highlight their positions. Regardless of ethnic background, regional affiliation, or personal interest, people who rely on the Taliban threat to conduct their activities will be revealed.

Long-Term Utility

As Mike Innes pointed out in his book, *Denial of Sanctuary,* in spite of the post-9/11 attention placed on eliminating terrorist sanctuaries, terrorist and organized criminal groups continue to operate effectively across "the spectrum of rogue states, failed states, and perfectly healthy democracies."[6] They do not wear uniforms or generally distinguish themselves except in their attacks, after which they disappear back into the population. This anonymity allows them to continue operations, even in close proximity to police or counterinsurgency forces. Biometrics are a critical step in eliminating the terrorist's advantage of anonymity.

NATO and its partners are involved in ongoing operations on three continents and the Mediterranean Sea, near the nexus of known criminal and terrorist activities (i.e., Afghanistan, Sudan, and the Balkans). They probably interact routinely with many people who are associated with terrorist threats or criminal activity and have already been identified by allies. Biometric applications will help identify links across those regions. A simple example could include the identification of someone fired from a NATO base in the Balkans who is subsequently hired in ISAF or Sudan. As a standard tool, biometrics will facilitate the sharing of information across commands and national boundaries. A NATO country should not hire a local worker in one of these operations if that person has previously proven unreliable or dangerous elsewhere. Simple identification would not necessarily indicate criminality, but would at least remove anonymity with regard to threat activity. As more people, threat or not, are identified traveling among the operating locations, different travel routes and mechanisms will also be illuminated. This information will facilitate more effective security and stability operations overall.

Application of the technology can also be expanded to other international issues. Biometrics are used to register children in the United States in case of kidnapping. Similar applications can help to mitigate human smuggling or support refugee migration analysis. Biometric features are already utilized in some national identification systems. Assuming the technology will be transferred to other nations, such as Afghanistan, Pakistan, and Lebanon, it will also highlight the movement of people, whether from a stated refugee camp or across a legal border checkpoint, and the timing of that movement. This

information will significantly empower all involved organizations and provide support for their efforts and actions.

Increased precision of information and operational effectiveness will translate into a reduction in the reliance on large troop formations and allow for more specialized review of issues. Consequently, instead of forces saturating an area, a fewer number of specialists can rely on the biometric information to conduct precise operations, thereby affecting fewer people and achieving greater stability and local support. Biometric matches will help identify who should receive added attention and how to focus that attention, whether it is a pre-employment screening interview or detection following an attack. Ultimately, individual troublemakers will be spotted and isolated earlier.

As a standard tool, biometrics will facilitate the sharing of information across commands and national boundaries.

Conclusion

The provision of biometric equipment and data to ISAF forces is a positive step in both tactical and strategic terms. Biometrics will help to clarify immediate threats by removing the ability to hide in plain sight. The technology also better positions NATO and allied forces for the asymmetric challenges posed by transnational terrorist organizations. Although the technology has great promise, significant steps must be taken to achieve full implementation, including the formulation of policy and procedures for information collection and sharing that will be acceptable across the alliance. With acceptance and familiarity, the capability will prove effective not only in keeping military forces safe, but in keeping member nations and citizens safe as well.

The ISAF biometric program proved its utility within days by identifying local workers who had lied about previous interaction with the alliance; however, continued utility depends on both the comprehensiveness and accuracy of the database. Database maintenance will require personnel to train, support, and maintain the systems within existing processes. Synergies will be found as the database grows and reporting accuracy is increased.

Although NATO has positively received biometrics within ISAF, use of biometrics is not a foregone conclusion. Only 6 of 26 NATO members have achieved the goal of 2 percent of gross domestic product allocated to national defense budgets.[7] Any substantial investment in technical programs must be based on merit and will compete with the spectrum of emerging military topics, from missile defense and advanced weapons systems to basic computer networks and databases. Because of its far-reaching effects and proven utility, biometrics will compete well in this environment, but it must still compete. The United States, as a leader of the ISAF biometric program, should consider providing additional dedicated personnel or support to ensure that the program continues to be effective.

Working with multiple allies' timelines will require patience. The program may not achieve immediate goals or adopt US policies directly, but the overall progress of the program remains in the interest of NATO and the United States. It will be worth the effort: Although the United States can achieve a high level of success with a national biometric system, only international coordination will achieve the ultimate potential offered by biometrics in the fight against transnational terrorists and criminals.

---

1 Shea, J. A NATO for the 21st Century: Toward a New Strategic Concept. *The Fletcher Forum of World Affairs,* Vol. 31, No. 2, Summer 2007, p. 50.

2 Felbab-Brown, V. From Sanctuaries to Protostates. In Denial of Sanctuary (Michael Innes, ed.), *Praeger Security International,* Westport, CT, 2007, pp. 153–166.

3 Howcroft, J. R. Technology, Intelligence, and Trust. *Joint Forces Quarterly,* Vol. 46, Third Quarter 2007, p. 20.

4 Kyser, G., M. Keegan, and S. A. Musa. Applying Law Enforcement Technology to Counterinsurgency Operations. *Joint Forces Quarterly*, Vol. 46, Third Quarter 2007, pp. 32–38.

5 Bolduc, D., and M. Erwin. The Anatomy of an Insurgency: An Enemy Organizational Analysis. *Special Warfare,* Vol. 20, July–August 2007, pp. 14–17.

6 Innes, M. (Ed.). Denial of Sanctuary. *Praeger Security International,* Westport, CT, 2007, p. 13.

7 See Shea, p. 51.

(*Source*: DoD Photo)

EOD/LIC Technologies: Weaponized Bot Rolls into Battle

By Kelly Rose, ManTech SETA Support to TSWG

The Combating Terrorism Technical Support Office (CTTSO) leverages technical expertise, operational objectives, and interagency-sponsor funding in its work with over 100 government agencies, state and local governments, law enforcement organizations, and national first responders. This collective approach to resource and information sharing positions the CTTSO to gather front-line requirements that support multiple users—a distinct advantage in combating terrorism.

As a program office under the Assistant Secretary of Defense for Special Operations, Low-Intensity Conflict, and Interdependent Capabilities (SO/LIC&IC), CTTSO is uniquely positioned to contribute to the success of the Global War on Terror. CTTSO takes operational requirements from warfighters and first responders; incorporates policy objectives that flow down from the Department of Defense; and marshals the technical expertise of its program managers, subject matter experts, and developers to provide capabilities that are fieldable and sustainable over the long war. This balance of political direction, operational relevance, and technical expertise has enabled CTTSO to respond with agility and speed to changing requirements.

In 1999, the CTTSO was assigned program management oversight for the Technical Support Working Group (TSWG). Since then, the Explosive Ordnance Disposal/Low-Intensity Conflict (EOD/LIC) and Irregular Warfare Support programs were added to further expand the CTTSO's response capabilities in combating terrorism.

Operators demonstrate the functions of SWORDS.

EOD/LIC Background

CTTSO's EOD/LIC program has been bringing new technology to EOD and Special Operations since 1990. EOD/LIC is an Advanced Technology Demonstration Program designed for the rapid prototyping of fieldable systems.

Because of the ever-growing threat of improvised explosive devices (IEDs) and other makeshift weapons aimed at US Forces in Operation ENDURING FREEDOM in Afghanistan and in Operation IRAQI FREEDOM, the need for new technological tools to combat such threats grows every day. Current operations require extensive use of EOD personnel to deal with the threat from IEDs and the potential for encountering an array of conventional explosive munitions discovered and confiscated in this hostile environment.

Two SWORDS in theater

Combating Threats to US Forces

During these recent conflicts, EOD personnel have also been tasked with investigating pre- and post-blast explosives and IEDs using limited supplies as necessitated by rough terrain and foot travel. Those limitations led to the requirement for compact, lightweight, multipurpose tools, such as robotic systems, that can be rapidly fielded in response to emerging threats. Remote-controlled robotic systems, or "bots," are being designed to do the jobs that pose the greatest risk to EOD operators. The bots primarily conduct reconnaissance and street patrols. An operator controlling the system may send it into a busy neighborhood infested with insurgents to detect, identify, and neutralize targets before forces on foot follow to patrol the area. Such a weapon recently deployed into theater is the Special Weapon Observation Reconnaissance and Direct-Action System (SWORDS).

SWORDS Development

Unmanned ground vehicles are used extensively to locate booby traps, ambushes, and IEDs. Despite the advances of those ground vehicles, US Forces still require innovative systems using preexisting technology. The robots are needed to function remotely in order to investigate threats and keep US Forces out of harm's way. As a result, the SWORDS program was initiated in 2004 by the US Army's Armament Research, Development, and Engineering Center. CTTSO became involved when the Army expressed interest in upgrading SWORDS with a modified system to meet specific Special Forces requirements. Initially, SWORDS evolved from the Foster–Miller TALON robot. TALON is a military-grade robot commonly used for EOD missions that require small, lightweight, and mobile remote-controlled robots. The bot is powerful, rugged, and speedy for its size. Its unique features made it an ideal candidate to become SWORDS 1.0.

Subsequently, CTTSO funded and managed the upgrade of SWORDS to create version 1.5 and add enhancements to version 2.0, which features a foundation developed specifically for specialized deployment in high-risk combat missions. SWORDS is the first weaponized robotic platform to be sent into theater, and developers anticipate great success; user feedback is still expected.

SWORDS 1.5 is composed of a weapons system mounted on the standard TALON chassis, and SWORDS 2.0 is mounted on a completely redesigned chassis. SWORDS is armed, remotely controlled, and integrated with features like the Tele-present Rapid Aiming Platform and multiple video cameras. The CTTSO EOD/LIC program upgrade outfitted the setup with an effective foundation for added stability, effectiveness, and reliability. The SWORDS setup is interchangeable with multiple weapons, but currently can only be mounted with the M249 Squad Automatic Weapon, M240 machine gun, or Barrett .50 caliber rifle for armed reconnaissance missions. The SWORDS vehicle weight with the M249 is 196 pounds, and the top speed is approximately 5 miles per hour. The system is also equipped with video cameras of varying intensity for recording, infrared, and zoom capabilities to assist in scouting missions. SWORDS operates in

SWORDS is equipped with more than just a weapon; cameras enable the operator to investigate suspicious threats remotely.

A conceptual image of SWORDS engaging the enemy.

SWORDS—ready for deployment.

multiple environments including sand, snow, and rain. The system is not autonomous; it is manipulated by an operator controlling a small, portable console/terminal known as the operator control system (enclosed in a pelican case) to remotely direct the device and fire its weapons.

This remotely operated system improves the safety of deployed Joint Service EOD and Special Forces units as they conduct reconnaissance, perimeter security operations, and surveillance operations. SWORDS also provides sniper capability and improves the safety of US Forces disembarking from their armored vehicles during patrols. Ultimately, the robot will extend the standoff distance between US Forces and the enemy.

SWORDS Testing and Deployment

In 2006, SWORDS underwent and successfully completed safety certification testing, an operational assessment, and further capability assessments at Aberdeen Proving Ground, Maryland, in preparation for its deployment abroad. SWORDS also underwent user training and evaluation with Special Forces in theater.

In the summer of 2007, the EOD/LIC-upgraded SWORDS became the first armed robot to deploy in Iraq. As a result of the success of SWORDS in the field, the Army has solicited a future upgrade for additional robots.

With SWORDS, developers hope that advanced technology operated near-autonomously will act as a deterrent to terrorists who threaten US forces. These systems have the potential to save lives by using advanced telerobotics to move armed forces out of harm's way. Additionally, future systems may be a force multiplier to supplement already extensive US forces, not just in theater but in combat zones all over the world.

For more information on SWORDS and the upgrade program at CTTSO, please contact the EOD/LIC program at EODLICWeb@eodlic.cttso.gov.

Information on the Armament Research Development and Engineering Center is available at http://www.pica.army.mil/PicatinnyPublic/organizations/ardec/index.asp.

JCOB Force Protection Handbook

http://www.train.army.mil | https://atep.dtic.mil

The Joint Contingency Operations Base (JCOB) Force Protection Handbook has just been published. It is intended for protecting modular battalion-sized units (tent systems) engaged in Security, Stability, Transition, and Reconstruction operations. It is available for download at http://www.train.army.mil and https://atep.dtic.mil.

> Questions?
Contact the JCOB/JFOB development team at jfob@erdc.usace.army.mil.

31 Wins, 6 Losses, and 1 Tie

The *ABA Journal's* scorecard of the Justice Department's legal war against al Qaeda

By Edward A. Adams

This article is reprinted from the September 2007 edition of the American Bar Association Journal.

How well is the US Department of Justice faring in its legal war against al Qaeda and its former state sponsor, the Taliban?

To find out, we reviewed DOJ's *Counterterrorism White Paper*, issued in June 2006, and subsequent court documents. The 68-page white paper, listing dozens of terrorism-related cases, is arguably the department's most comprehensive public accounting of its terrorism successes and failures since 9/11. It includes what DOJ considered the major pending cases at that time. Below are the 38 defendants who were charged since 9/11 with fighting for, providing material support to, or financing al Qaeda or the Taliban and whose cases have been disposed of by a US District Court as of late July 2007. Many of the cases remain on appeal.

Since 9/11, Justice Department officials have repeatedly said they will use minor charges to convict individuals they believe are terrorists—much as gangster Al Capone was convicted of tax evasion—in an effort to thwart another attack. But absent a conviction on terrorism charges, it is impossible to say for sure that those individuals are terrorists since, as DOJ officials also often say, defendants are presumed innocent until proven guilty.

Consequently, the following chart evaluates the strength of the government's cases, not whether the defendants were terrorists. It scores each case based on whether the government proved—either by a defendant's plea or a conviction after a trial—the indictment's charges of supporting al Qaeda or the Taliban. The cases are listed in chronological order based on when legal proceedings began.

DEFENDANT	DATE CASE BEGAN, COURT	FACTS	OUTCOME
Zacarias Moussaoui	December 2001 Eastern District of Virginia	Admitted al Qaeda member who pleaded guilty to planning to fly a plane into the White House. After a 2-month trial, a lone juror saved him from being sentenced to death. Sentence: Life in prison.	Win
Richard Reid	December 2001 District of Massahusetts	Pleaded guilty to trying to detonate a bomb in his shoe on an American Airlines flight over the Atlantic. Sentence: Life in prison.	Win
John Walker Lindh	January 2002 Eastern District of Virginia	Pleaded guilty to fighting in support of the Taliban. Sentence: 20 years.	Win
Jose Padilla	May 2002 District of South Carolina	US citizen who allegedly planned to explode a "dirty bomb" in the US for al Qaeda. Held as an enemy combatant. Sought a habeas hearing in federal court. He won in the District Court and lost in the 4th US Circuit Court of Appeals at Richmond, Virginia. Days before the government had to respond to Padilla's US Supreme Court motion for cert, he was charged by a federal grand jury in a plot to wage jihad overseas. The dirty bomb allegations are not part of the criminal charges. At deadline, his trial was underway in Miami.	Loss
Yaser Hamdi	June 2002 Eastern District of Virginia	US citizen picked up on battlefield in Afghanistan was held as an enemy combatant. Sought a habeas hearing in federal court. After the Supreme Court found he was entitled to a hearing by a "neutral decision-maker," the government released him to freedom in Saudi Arabia.	Loss
James Ujaama	August 2002 Western District of Washington	Charged with conspiracy to set up an al Qaeda training camp in Bly, Oregon. Pleaded guilty to helping a person travel to an al Qaeda training camp in Afghanistan and providing money to the Taliban. Sentence: 2 years.	Win
Lackawanna Six	September 2002 Western District of New York	Pleaded guilty to training in an al Qaeda camp in Afghanistan before 9/11. Sentences ranged from 7 to 10 years.	6 Wins
Enaam Arnaout	September 2002 Northern District of Illinois	Head of the charitable Benevolence International Foundation was charged with raising money for al Qaeda. Pleaded guilty to fraudulent diversion of charitable donations to promote overseas combatants in organizations other than al Qaeda. Sentence: 11 years.	Loss
Portland Seven	October 2002 District of Oregon	Six defendants pleaded guilty to attempting to travel to Afghanistan to fight with the Taliban. Seventh reportedly died in Pakistan. Sentences ranged from 3 to 18 years.	6 Wins
Drugs for Missiles Co-conspirators	October 2002 Southern District of California	Three men pleaded guilty to conspiring to provide material support to al Qaeda; they planned to trade drugs for Stinger missiles. Sentences: Approximately 5 years.	3 Wins
Brooklyn Terror Financiers	January 2003 Eastern District of New York	Two men arrested in an undercover operation; they offered to transfer $2 million to jihadists. Convicted of providing material support to al Qaeda. Sentences: 75 and 45 years.	2 Wins

DEFENDANT	DATE CASE BEGAN, COURT	FACTS	OUTCOME
Iyman Faris	April 2003 Eastern District of Virginia	Ohio truck driver pleaded guilty to casing the Brooklyn Bridge for al Qaeda. Sentence: 20 years.	Win
Masoud Khan	June 2003 Eastern District of Virginia	Convicted of conspiracy to contribute services to the Taliban by visiting a training camp in Pakistan, but acquitted of conspiracy to provide material support to al Qaeda. Sentence: Life in prison.	Tie
Randall Royer	June 2003 Eastern District of Virginia	Charges that he aided al Qaeda and the Taliban were dropped when he pleaded guilty to abetting the discharge of a firearm during a crime of violence. Sentence: 20 years.	Loss
Sabri Benkahla	June 2003 Eastern District of Virginia	Acquitted after a bench trial of supplying services to the Taliban. Convicted in a second trial of lying to a grand jury about his training with a Pakistani militant group. Sentence: 10 years.	Loss
Uzair Paracha	August 2003 Southern District of New York	Convicted of providing material support to al Qaeda by obtaining immigration documents that would permit an al Qaeda associate to enter the United States to blow up gas stations. Sentence: 30 years.	Win
Mohammed Junaid Babar	May 2004 Southern District of New York	New York taxi driver/student pleaded guilty to providing goods to al Qaeda and briefly running a jihad training camp in Pakistan. Testified in the UK in 2006 against a group of UK residents of Pakistani descent charged with plotting to mount attacks in Britain using explosives made out of fertilizer. Sentence: Not disclosed.	Win
Ali al-Timimi	September 2004 Eastern District of Virginia	Convicted of urging followers in Northern Virginia to fight for the Taliban in the days after 9/11. Sentence: Life in prison.	Win
Mohammad Qureshi	October 2004 Western District of Louisiana	Convicted of lying to federal agents about providing $30,000 to an al Qaeda member involved in the bombing of United States embassies in Kenya and Tanzania. Sentence: 4 years.	Win
Ahmed Abu Ali	February 2005 Eastern District of Virginia	US citizen convicted of joining an al Qaeda cell in Saudia Arabia, as well as plotting to mount attacks in the US and assassinate President Bush. Sentence: 30 years.	Win
Ronald Grecula	May 2005 Southern District of Texas	Pleaded guilty to attempting to build and sell a bomb to an undercover officer he believed was a member of al Qaeda. Sentence: 5 years.	Win
Rafiq Sabir and Tarik Shah	May 2005 Southern District of New York	Charged with telling undercover agent they would provide al Qaeda with martial arts training and medical assistance. Shah pleaded guilty. Sabir was convicted by a jury. Neither has been sentenced.	2 Wins
The Hayats	June 2005 Eastern District of California	A jury found Hamid Hayat guilty of training in an al Qaeda camp in Pakistan. A separate terrorism trial against his father, Umer, ended in a deadlocked jury. Umer pleaded guilty to a lesser offense and was sentenced to time served. Hamid faces up to 39 years in prison; at deadline, he was scheduled to be sentenced Aug. 10.	1 Win, 1 Loss

Lessons Learned: The Fort Dix Six

By Lt Col Shannon W. Caudill, Joint Staff J-3, Deputy Directorate for Antiterrorism/Homeland Defense, Action Officer, Antiterrorism Interagency Coordination

Six homegrown, foreign-born, self-radicalized extremists were arrested in May 2006 for plotting to attack soldiers at Fort Dix, New Jersey—a military installation used largely to train Army reservists bound for duty in Afghanistan, Bosnia, Iraq, and Kosovo. "Today we dodged a bullet. In fact, when you look at the type of weapons that this group was trying to purchase, we may have dodged a lot of bullets," commented FBI Agent-in-Charge J.P. Weis.[1] The arrest of these suspected terrorists marks an important chapter in homeland antiterrorism efforts from which many lessons can be learned.

The FBI described the efforts of these terrorists as indicative of a rise in small but sophisticated groups operating autonomously from other, established terrorist groups.

The attack was foiled when the men filmed themselves conducting firearms training and took the footage to a video store to put onto a DVD. The recording also showed the men calling for jihad, or holy war, against the United States and shouting "God is great" in Arabic. Concerned about the images, the store owner contacted the FBI, which began an investigation. Investigators infiltrated the group using an informant and secretly recorded the defendants during different stages of their training and targeting cycle.

A New Form of Terrorism

The FBI described the Fort Dix plot as a "brand-new form of terrorism" because it involved terrorists who lived and worked in the United States, organized on their own, had no formal connection to other terrorist networks, and were largely inspired by al Qaeda's ideology and call for jihad against the West.[2] "These homegrown terrorists can prove to be as dangerous as any known group, if not more so. They operate under the radar," commented the FBI's Weis.[3] The FBI described the efforts of these terrorists as indicative of a rise in small but sophisticated groups operating autonomously from other, established terrorist groups.

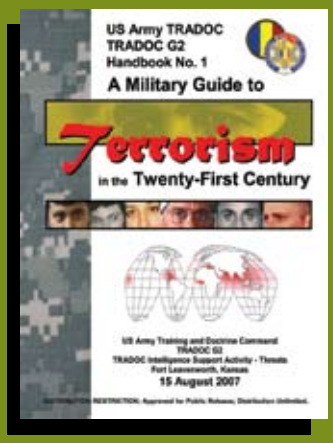
The alleged terrorists were all men in their twenties from the former Yugoslavia and the Middle East:

- **Mohamad Ibrahim Shnewer, 22, of Cherry Hill, New Jersey.** Shnewer was born in Jordan and is a naturalized US citizen. He was employed as a taxicab driver in Philadelphia.
- **Eljvir Duka, 23, Shain Duka, 26, and Dritan Duka, 28; all of Cherry Hill, New Jersey.** All are brothers who were born in the former Yugoslavia and were illegal residents in the United States. They operated several roofing businesses.
- **Serdar Tatar, 23, of Philadelphia, Pennsylvania. Tatar was born in Turkey.** He was a legal resident in the United States. He was a 7-Eleven convenience store employee in Philadelphia.
- **Agron Abdullahu, 24, of Buena Vista Township, New Jersey.** Abdullahu was born in the former Yugoslavia and was a legal resident in the United States. He was employed at a Shop-Rite Supermarket.

The Targets

Largely underreported is the fact that the perpetrators discussed a total of nine potential US military targets in the US homeland. According to the indictment, the group surveilled five installations: Dover Air Force Base, Delaware; Fort Dix, New Jersey; Fort Monmouth, New Jersey; Lakehurst Naval Air Station, New Jersey; and the US Coast Guard building, Philadelphia.[4] The conspirators also discussed attacking Naval Station Philadelphia and the "nearby air force base," which likely refers to McGuire Air Force Base, located adjacent to Fort Dix in New Jersey.[5] As they narrowed their focus on Fort Dix, they discussed attacking critical infrastructure including the base electrical grid to "cause a power outage and allow for an easier attack of the military personnel there."[6]

The group also discussed future plans for high-profile targets, including attacking the Army-Navy game participants in naval billeting or potentially at the game itself held at Lincoln Field in Philadelphia. They also discussed the possibility of sinking US naval vessels while docked at the Port of Philadelphia.



Antiterrorism officers and senior leaders must be aware of the indicators of terrorist surveillance and its role in target selection. **A Military Guide to Terrorism in the Twenty-First Century** *is a great source of information.*

Why Fort Dix? Examining the Terrorist Targeting Cycle

The group chose five potential targets for surveillance, and often videotaped the perimeters of the bases. For example, the conspirators surveilled Dover Air Force Base security operations and physical security and determined it "was too difficult of a target because of its high security."

The group eventually selected Fort Dix as its primary target because one member had access to the base through his father's pizza delivery business. Serdar Tatar's father owned Super Mario's restaurant, which made deliveries to both Fort Dix and McGuire Air Force Base. Significantly, Tatar was able to acquire a map of Fort Dix, labeled "Cantonment Area Fort Dix, N.J.," which helped the conspirators target personnel and facilities. The group also believed that the massing of Soldiers during training events would provide easy targets because they gained intelligence that the Soldiers often trained without ammunition. They estimated that a group of six or seven people could kill 100 unarmed Soldiers. One conspirator commented, "My intent is to hit a heavy concentration of soldiers"—a prospect that seemed possible at Fort Dix based on surveillance.[7] Their goals were "to kill as many American soldiers as possible" and to procure mortars, rocket-propelled grenades, and machine guns.[8]

Attacking unarmed personnel in a training environment is not a new idea. On 9 October 2002, one US Marine was killed and another was wounded after two gunmen infiltrated a military training exercise on Failaka Island in the Persian Gulf off Kuwait City.[9] Two Kuwaiti radicals, deemed terrorists by the Kuwaiti government, used AK-47 automatic rifles to attack Marines who were training with blank rounds. On a smaller scale, the Failaka Island attack parallels the plan of the Fort Dix conspirators.

Conclusion

The preliminary lessons learned from the foiled Fort Dix attack should be fodder for discussion at force protection, threat working groups, and the various levels of antiterrorism training. Leaders must examine similarities between their base and the threat posed to Fort Dix. There is no doubt that military installations in the continental United States will be targeted again. The Fort Dix Six provide a wake-up call for a new and evolving threat; self-radicalized individuals who are inspired, but not directly connected to, established terrorist groups. Such groups can operate autonomously, drawing information and training from the internet and other homegrown radicals. FBI Agent-in-Charge Weis noted the following about the Fort Dix Six:

"We had a group that was forming a platoon to take on an army. They identified their target, they did their reconnaissance. They had maps. And they were in the process of buying weapons. Luckily, we were able to stop that.[11]"

Complacency is the enemy. A robust antiterrorism program is the key to provide challenging base security procedures and continuously improving the installation's force protection and security contingency footing. Without it, a base is relying merely on luck to protect itself from future dangers.

The Fort Dix Six: Lessons Learned

Much more information may be learned during the trial of these conspirators, which is scheduled to start on 15 January 2008. Lawyers are reviewing nearly 200 hours of recorded conversations and 20 hours of videotapes. Some preliminary lessons about homeland security can be learned from the Fort Dix plot:

- **Terrorist planning cycle:** Terrorists, even novice terrorists, follow some form of template for target selection and planning. Antiterrorism officers and senior leaders must be aware of the indicators of terrorist surveillance and its role in target selection. *A Military Guide to Terrorism in the Twenty-First Century* is a great source of information.[10]
- **"The Dover Effect":** The security image of facilities and personnel that a base projects to the public matters. The conspirators were clearly impressed with security at Dover Air Force Base and decided not to attack it as a result. Random antiterrorism measures (RAMs) play a key role in deterring targeting by making base security less predictable. One thing is certain: If a base projects an image of low security, it will move to the top of the terrorist target list.
- **Critical Infrastructure Protection (CIP):** The targeting of Fort Dix infrastructure points to the importance of the CIP program. The destruction of critical infrastructure nodes can lead to a complete mission failure or an exploitable vulnerability during a terrorist attack.
- **Base access:** One defendant knew Fort Dix "like the back of his hand" because he had delivered pizza there and acquired a map. Vetting vendors and commercial business operations prior to giving them base access is an important consideration. Future programs like the Defense Biometric Identification System (DBIDS) will improve base access control, visitor registration, and accountability of critical installation equipment.
- **Joint Staff Integrated Vulnerability Assessments (JSIVA):** Fort Dix had a JSIVA in June 2005. Every JSIVA includes an assessment of potential terrorist operations that may be conducted against an installation—a valuable resource in maintaining vigilance and antiterrorism program standards. JSIVAs, other higher headquarters assessments, and local evaluations must be used as a benchmark for installation success and progress in improving its antiterrorism program.
- **Force protection of massed personnel in a training environment:** The Fort Dix scenario points to the need for force protection of personnel who are training in an unarmed environment. Personnel massed for training present a target of opportunity that must be protected. Installations must take steps to ensure a defense capability for massed personnel.

---

1 MSNBC. "Six Held on Terror Conspiracy Charges in New Jersey." *MSNBC,* 8 May 2007, available at http://www.msnbc.msn.com/id/18549005/from/ET

2 CBS News. "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

3 Ibid.

4 US District Court, District of New Jersey. United States of America vs. Dritan Kuka, 7 May 2007, available at http://www.usdoj.gov/usao/nj/press/files/pdffiles/DukaDritanComplaint.pdf

5–8 Ibid.

9 Schmitt, E. "Threats And Responses: Skirmish; US Marine Is Killed in Kuwait As Gunmen Strike Training Site." *New York Times,* 9 October 2002, available at http://query.nytimes.com/gst/fullpage.html?res=9505E6D91E3BF93AA35753C1A9649C8B63&n=Top/Reference/Times%20Topics/Organizations/M/Marine%20Corps

10 US Army, *A Military Guide to Terrorism in the Twenty-First Century,* TRADOC DCSINT Handbook No. 1, Version 3.0, August 15, 2005, available at: http://www.au.af.mil/au/awc/awcgate/army/guidterr

11 Parry, W. "Store Clerk Key to Fort Dix Plot Arrests." *ABC News,* 9 May 2007, available at http://abcnews.go.com/US/WireStory?id=3154608&page=1

(Source: DoD Photo)

Notes from the War on Terror

Overcoming the ideology of hate and terror

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

"Either we have in the next ten years 80 million productive young people … or we have 80 million radical extremists in the Middle East."

Mohammed Al Gergawi
Cabinet Affairs Minister, United Arab Emirates
Financial Times
28 September 2007

[Saudi youth have become] "a tool in the hands of foreign forces that manipulate them in the name of jihad, whilst fulfilling their shameful goals and objectives in foul operations that are far removed from religion so that our youth have become a commodity to be bought and sold … I advise caution to those with financial means so that their money does not end up harming Muslims."

Saudi Grand Mufti Sheikh Abdulaziz al-Sheikh
Asharq Alawsat
2 October 2007

"While moderates and reformers represent America's natural core allies in the region, extra steps should be taken to include social conservatives as we engage in dialogue across the Islamic world. Conservatives are the swing voters in this critical effort. They may seem to represent the most convenient potential allies for the radical militant extremists, but in fact they must play a crucial role if al Qaeda and other radicals are to be marginalized … Excluding nonmilitant conservatives from the process will only alienate them further … We should be prepared to enter into dialogue with any group that is willing to both renounce violence and respect a diversity of views. When we lump such groups together with radicals and refuse to engage with them because of Islamist ideology, we then aid our true foes."

Peter Singer and Hady Amr
"Restoring America's Good Name: Improving Strategic Communications with the Islamic World"
"In the Same Light as Slavery": Building a Global Antiterrorist Consensus
NDU, 2006

"These days, the jihadi organizations of all types inflict many disasters that might speed up their end. The most important of these disasters is combining jihad and authority. The al Qaeda organization has fallen into this trap when it declared the Islamic State of Iraq in the Al-Anbar region … Combining jihad and authority at the same time is like mixing water and oil; it is an impossible process. Authority is a heavy burden, and administering the day-to-day affairs of the people is a process that is both exhausting and costly, and that needs tools and expertise jihadis do not have, and even if they had them, they would not be allowed to use them."

Abd-al-Bari Atwan
Al-Quds al-Arabi/OCS
24 October 2007

"The brotherhood of faith is the bond that unites Muslims; not affiliation to the tribe, or the country, or the organization … The interests of the Ummah surpass the interests of the state … My brother fighters in Iraq … you have done well in carrying out one of the greatest duties that few people could carry out; namely, the duty of repelling the enemy. Some of you, however, have been late in carrying out another duty, which is also one of the greatest duties; namely, the duty of unifying your ranks as God … wants … The Muslims are waiting for you all to be united under one banner to uphold right."

Osama Bin Laden
Al-Jazeera/OSC
22 October 2007

"Muslims must acknowledge and take responsibility for the manipulation of historical grievances—as Osama Bin Laden's latest message clearly shows … The sad fact is that more Muslims today are dying at the hands of Muslims than by acts of Israelis, Americans, or any other perceived enemies—whether it's from almost weekly suicide bombings in Pakistan, intra-Palestinian fighting, or sectarian violence in Iraq. History shows external influences have certainly been brutal in all those areas, but a clearer focus on the present could help Muslims realize it is not all about 'us versus them,' but also 'us versus us.'"

Mona Eltahawy
Middle East Online
29 October 2007

Notes from the War on Terror

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

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

	Event	Strategic Significance
Negative effects on the GATE	**UK: AQ Said to be Expanding in Iraq and Africa.** Domestic Intelligence (MI5) head Jonathan Evans said the "AQ brand" had expanded in Iraq, Algeria, and parts of east Africa and now posed a threat to the United Kingdom. UK-based extremists were connected to networks in other countries and were trying to recruit children to carry out terror attacks. Evans said AQ was plotting attacks against the United Kingdom from bases in Pakistan and that security services were monitoring at least 2,000 known extremists in the United Kingdom. He also suggested that possibly 2,000 more were not yet known to officials.	A warning against complacency, but also perhaps an effort to build support for tougher counterterrorism laws.
	Libya/AQ: LIFG Merges with AQ. Al Qaeda No. 2 Ayman al-Zawahiri said the Libyan Islamic Fighting Group (LIFG) has merged with AQ, according to an audiotape message on the Internet. Al-Zawahiri referred to Libyan leader Muammar Gaddafi as "an enemy of Islam," and also called on Palestinian Fatah and al-Aqsa Brigade members to overthrow President Mahmoud Abbas.	AQ is trying to achieve a propaganda boost from asserting a connection with the terrorist LIFG, which reportedly does not have many followers and has not been active lately. LIFG, which originated in the 1990s, reportedly poses no threat to Gaddafi's regime but may try to emulate the AQIM terrorists in Algeria, targeting security forces, economic infrastructure, foreign interests, and innocent civilians.
	Thailand: Insurgents Targeting Civilians. In a new report, Human Rights Watch said ethnic Malay insurgents are killing or mutilating a growing number of Buddhist and Muslim civilians in their attempt to establish a separate Islamic state in southern Thailand. The report said that insurgents had carried out more than 3,000 attacks on civilians between January 2004 and July 2007, and 500 attacks on military personnel. Eighty-nine percent of almost 2,500 people killed were civilians, and at least 29 victims were beheaded and mutilated. Schools, community centers, and Buddhist temples were being targeted to undermine Thai control in the southern region.	The report documents that the insurgents are mainly (and deliberately) attacking civilians to drive Buddhists from the Muslim-majority southern provinces and undermine Thai government control. The insurgents have never expressed remorse for deliberately targeting civilians.
Positive effects on the GATE	**Italy/UK/France/Portugal: Raids Target 20 Suspected Terrorists.** Police arrested at least 20 people in an antiterrorism operation led by Italian authorities. Italian police reportedly said that the arrested people, mostly Tunisian nationals, were setting up a "Salafist jihadi" network that recruited and assisted prospective suicide bombers in Iraq and Afghanistan. Italian police said they also seized poisons and equipment for explosive devices.	The Italian Interior Minister claimed the joint police action has decapitated a foreign terrorist network sending combatants to Iraq and Afghanistan.
	Al Qaeda: Anger at the Messenger. On a recent audiotape, bin Laden criticized divisions among Iraqi militants, pleaded for unity, and admitted mistakes. Many media commentators viewed this performance as a confession of weakness and an acknowledgement of fissures within AQ. Some AQ sympathizers have criticized al-Jazeera TV for allegedly manipulating the broadcast to make bin Laden and AQ look weak.	The harsh criticism of al-Jazeera TV suggests that bin Laden's performance may have demoralized some of his followers, who refuse to accept his analysis and recommendations.
	Saudi Arabia: Grand Mufti Warns Against Joining Jihad Abroad. Sheikh Abdulaziz al-Sheikh, Saudi Grand Mufti and one of Sunni Islam's leading religious authorities, issued a fatwa warning young men against traveling abroad to fight jihad. Abdulaziz said such "zealous" young men were being exploited by "outside forces" for "shameful goals," according to media reports. The Mufti reportedly added that participation in a jihad that was not condoned by the appropriate religious authorities was a "violation of the foundations of Sharia."	The Mufti has warned before against violent extremists "corrupting" Saudi youth; in fact, he issued a fatwa against suicide operations prior to 9/11. His latest fatwa, directed at clerics who promote violent global jihad, undermined those who claimed that their participation as combatants in foreign jihad was sanctioned by appropriate religious authorities.

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