Counterterrorism Activities of the FBI:

At Home and Abroad

Case Studies in National Security Transformation
Number 8
M.E. (Spike) Bowman

Sponsored by the Office of the Deputy Assistant Secretary of Defense
Forces Transformation and Resources

Prepared by the Center for Technology and National Security Policy

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
2007		**00-00-2007 to 00-00-2007**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Counterterrorism Activities of the FBI: At Home and Abroad	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) **National Defense University,Center for Technology and National Security Policy,Fort Lesley J. McNair,Washington,DC,20319**	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	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**Same as Report (SAR)**	**19**	

The views expressed in this article are those of the authors and do not reflect the official policy or position of the National Defense University, the Department of Defense or the U.S. Government. All information and sources for this paper were drawn from unclassified materials.

M. E. (Spike) Bowman is Deputy Director, National Counterintelligence Executive. Previously he was a Senior Research Fellow at the Center for Technology and National Security Policy. He is retired from the Senior Executive Service, Federal Bureau of Investigation where he served successively as Deputy General Counsel (National Security Law) Senior Counsel and Director, Intelligence Issues and Policy Group (National Security Branch). He is a former intelligence officer and specialist in national security law with extensive experience in espionage and terrorism investigations. In addition to national security experience he is a retired U.S. Navy Captain who has served as Head of International Law at the Naval War College, as a diplomat at the U.S. Embassy in Rome, Italy and as Chief of Litigation for the U.S. Navy. Mr. Bowman is a graduate of Willamette University (B.A.), the University of Wisconsin (M.A.), the University of Idaho (J.D., *Cum Laude*) and The George Washington University (LL.M., International and Comparative Law, *With Highest Honors*).

The FBI and Al Qaeda

It was in Afghanistan where the utility of law enforcement expertise and techniques in a conflict zone first became evident. Shortly after the land campaign had begun, the FBI deployed two agents to Bagram. At first they were met with skepticism and concern ─ what, after all, would the FBI be looking at? After they had been there only a short time the FBI decided to recall them out of concern for maintaining good relations. Before that could occur, however, on a cold Saturday morning in February of 2002, an FBI employee in Washington, D.C. received a phone call from Bagram on his secure cellular phone. An Army general's opening words were specific and to the point: "You've got to help me; they're trying to take my FBI agents away!"

How respect for law enforcement and law enforcement skills developed among the military is instructive.

Prior to the terrorist attacks of 9/11, the FBI, and more specifically the New York Field Office, was the single most complete repository of information about Al Qaeda. The two agents deployed to Bagram were from the New York Field Office, and their knowledge of Al Qaeda organization, personnel, and modus operandi quickly became invaluable in helping military forces to understand what and who they were confronting, both on the battlefield and in detention facilities.

Since those early days of confronting the threat of terrorism, the utility of law enforcement in a conflict area has increased, at least in part due to dramatic increases in FBI capabilities to monitor terrorism activity world-wide and to share those capabilities and information with others. Some of the developments, explained more completely below, include:

- Growing from 31 to 104 Joint Terrorism Task Forces (JTTFs) and adding 3,000 personnel to them;
- Forming a National Joint Terrorism Task Force of senior officials from all executive agencies;
- Forming a Foreign Terrorist Tracking Task Force (FTTTF);
- Creating 56 Field Intelligence Groups (FIGs);
- Sponsoring a Terrorist Screening Center that operates 24/7;
- Creating a Terrorist Explosive Devices Analytical Center;
- Forming a Weapons of Mass Destruction Directorate;
- Sponsoring an Investigative Data Warehouse shared by agents and analysts across government;
- Establishing a significantly enhanced overseas presence to partner with other government agencies; and
- Integrating an already robust fingerprint database with fingerprints derived from conflict zones and sharing that database with other agencies.

These capabilities, partnered with other agencies, including the Department of Defense, have steadily been picking apart the Al Qaeda apparatus.

The FBI has enhanced its knowledge of terrorism, as well as its capability for preventing terrorism, and has increasingly made its expertise and capabilities available to other agencies, to the military in the field, and to the security services of other nations with whom it partners. That expertise, ranging from plain old gum shoe police work to highly sophisticated and unique forensic capabilities, has been made available worldwide, including in conflict zones. The simple fact is that threats today commonly have an international nexus, and the network of global law enforcement organizations is a useful tool in combating terrorism.

There is another reason that this expertise is useful, and this reason is both simple and complex. It is simple because today the ends for which we fight have transitioned from imposing a political outcome to establishing conditions to shape the outcome —clearly a multi-disciplinary effort. It is complex because those conditions are rarely going to be cross-culturally clear. Nevertheless, information and the exploitation of that information is a key element of the national objective, and the FBI presents both unique capabilities to gather information and the experience to interpret it.

Forensic Capabilities

More than at any other time in history, forensic skills have become relevant to the conflict. For one thing, when the enemy consists of terrorists and insurgents, they blend in with the populace, and a means to identify individuals becomes critical. Similarly, when individuals are killed, it is still important to identify them to know what part of the threat has been eliminated and what part remains. Furthermore, when the weapon of choice becomes increasingly sophisticated improvised explosive devices (IEDs), ways must be found to defeat them. As an additional benefit, forensics may help to identify the maker. Forensics are a limited but effective part of the effort to prevent harm, and the skill sets employed in forensic endeavors are constantly evolving.

DNA

Precise identification of individuals, both alive and dead, is a critical need.[1] To this end, the FBI has established a large inventory of DNA samples that is useful in identifying persons when they are confronted and confirming the identity of bodies.[2] For example, in October 2006, DNA testing confirmed a claim by the Pakistani government that Muhsin Musa Matwalli Atwah, an Al Qaeda operative wanted by the United States in connection with the 1998 U.S. Embassy bombings, had been killed in an air strike by Pakistani forces near the border with Afghanistan.[3] In January of 2007, on the other side of the

[1] Because most of the known or suspect terrorists are non-U.S. citizens, DNA samples from the terrorist's maternal family must be collected abroad. For this, foreign governments have been enlisted to help collect samples that can be compared with DNA from individuals captured or killed.

[2] When an Australian patrol in Afghanistan came across 23 graves said to contain the bodies of Arab fighters, they gathered forensic (DNA) evidence for future reference. "Blowing Up Caves in Afghanistan," *Army: The Soldier's Newspaper*, June 6, 2002.

[3] Henry Schuster, "One of FBI's 'Most Wanted Terrorists' confirmed dead," October 24, 2006. Available online at <http://www.cnn.com/2006/WORLD/asiapcf/10/24/alqaeda.operative/index.html>.

world, FBI DNA testing confirmed the death of the Philippines most wanted terrorist.[4] In both cases authorities were relieved of the burden of having to continue looking for these two individuals.

Less obvious uses of DNA. For example, even though the body of Abu Musab al-Zarqawi had been identified by fingerprints, tattoos, and scars after he had been killed in an air-strike, DNA samples were sent to the FBI crime laboratory in Quantico, Virginia. There, his DNA was compared to other samples to help establish where he had been and perhaps determine who had been there with him.[5]

Fingerprints

One of the most common forensic capabilities is fingerprinting.[6] The FBI maintains an Integrated Automated Fingerprint Identification System (IAFIS). The IAFIS maintains the largest biometric database in the world, containing the fingerprints and corresponding criminal history information of more than 47 million subjects in the Criminal Master File. The fingerprints and corresponding criminal history information are submitted voluntarily by state, local, and federal law enforcement agencies.

With the ability to digitally transmit fingerprints, state, local, and military abroad can send prints for comparison and receive electronic responses to criminal ten-print fingerprint submissions within 2 hours, and within 24 hours for civil fingerprint submissions using the Integrated Automated Fingerprint Identification System (IAFIS). [7] Needless to say, the ability to identify suspected terrorists and insurgents in Iraq and Afghanistan is a highly desirable capability. As early as April of 2002, the Attorney General directed that terrorist fingerprints and biographical data be gathered internationally from military detainees, from cooperative international exchange programs, through legal attaches in embassies abroad, and from domestic law enforcement sources. As of September 1, 2006, more than 19,000 such prints had been added.[8]

Today, when the U.S. military rounds up suspected terrorists they are "booked" and fingerprinted using the same tools that police in the United States use to check criminal backgrounds. If any of those fingerprinted subsequently attempt to enter the United States, they will be flagged. Moreover, when a large group was rounded up in Iraq in 2004, 44 were determined to have criminal records in the United States and two were sought on federal warrants.[9] Fingerprint identification has been so successful that in 2005

---

[4] Jaime Laude**, "**Janjalani dead, FBI DNA tests confirm," *The Philippine Star*, January 21, 2007. Available online at <http://www.philstar.com/philstar/News200701210401.htm>.

[5] Xinhua Online, "FBI to Conduct Test on Zarqawi's Biological Samples," June 9, 2006. Available online at <http://news.xinhuanet.com/english/2006-06/09/content_4672135.htm>.

[6] A more complete description of fingerprint use in a conflict may be found in Paul J. Shannon, "Fingerprints and the War on Terror," *Joint Force Quarterly*, Issue #43, 2006.

[7] For more information on IAFIS see <http://www.fbi.gov/hq/cjisd/iafis.htm>.

[8] FBI, "International Operations," September 1, 2006. Available online at <http://www.fbi.gov/aboutus/transformation/international.htm>.

[9] FBI, "Protecting America From Terrorist Attack: War Zones Link To FBI's Fingerprint Database," June 27, 2005. Available online at <http://www.fbi.gov/page2/june05/iafis062705.htm>.

the Department of Defense (DOD) created its own biometric database, the Automated Biometric Identification System (ABIS) modeled on IAFIS. To ensure quality and interoperability of all fingerprint data collected in support of the Global War on Terror, DOD has directed that all DOD acquisitions of fingerprint data collected must conform to the same standards and be interoperable with the FBI's IAFIS system.[10]

Prints sent to ABIS are sifted through IAFIS, where they are screened and compared to the FBI's most-wanted terrorist lists.[11] The value of that screening has been demonstrated several times when suspects were detained after their fingerprints showed they had been arrested before. In one case, suspected Al Qaeda terrorist Mohamad al Kahtani was positively identified based on prints taken when he was denied entry to the U.S. in August 2001.[12]

Improvised Explosive Devices (IEDs)

More American deaths in Iraq result from IED explosions than from any other cause. Additionally, IEDs have become the weapon of choice for terrorists worldwide. Because of this, in December of 2003, the Federal Bureau of Investigation (FBI) created the Terrorist Explosives Device Analytical Center (TEDAC), a collaborative effort of law enforcement and military experts under the aegis of the FBI.[13] TEDAC established a single federal program responsible for the worldwide collection, complete forensic, and technical analysis and timely dissemination of intelligence regarding terrorist bombs. Every bit of information gleaned from TEDAC's analysis is shared throughout the law enforcement, intelligence, and military communities.

Drawing linkages between terrorist devices and their makers—sometimes even continents away—can produce or add information that could keep the next bomb from going off. The intelligence is also used to develop new countermeasures and to train first responders on improvised explosive devices actually being used by the terrorists. Using breakthrough technology, TEDAC technicians are identifying locales where devices are made and even who is making them.[14] According to a "Five-Year Accounting" of FBI progress in transformation, 56 bomb makers were identified through TEDAC analysis.[15]

In testimony before Congress in September 2005, FBI Director Robert Mueller made the following comment:

> The TEDAC receives and exploits raw intelligence and information, component hardware and other physical items from various members of the Explosive Ordnance

[10] Robert S. Mueller, III, Director, Federal Bureau of Investigation before the United States House of Representatives Committee on Appropriations, Subcommittee on Science, State, Justice and Commerce, September 14, 2005. Available online at <http://www.fbi.gov/congress/congress05/mueller091405.htm>.
[11] Ibid.
[12] Although there is no evidence to prove it, several have suggested that al Kahtani was attempting to enter the U.S. to become the 20th hijacker.
[13] For more information on TEDAC, please see <http://www.fbi.gov>.
[14] CBS News, "Forensics ID Bomb Makers in Iraq," January 17, 2006. Available online at <http://www.cbsnews.com/stories/2006/01/17/eveningnews/printable1216945.shtml>.
[15] FBI, "What's New on the FBI: A Five Year Accounting," September 15, 2006. Available online at <http://www.fbi.gov/page2/september06/testimony091406.htm>.

> Disposal (EOD) and IED community worldwide. Functioning as the repository for all information and items received, the TEDAC conducts a full range of forensic analysis deemed appropriate on each item. TEDAC reports the results of these forensic analyses to the IED community and maintains a database for all information developed. TEDAC provides link analysis of all intelligence developed and provides devices to members of the IED community for any further exploitation deemed necessary to facilitate research, development and engineering imperatives. TEDAC is committed to providing international, federal, state and local law enforcement and bomb squads with current information relating to terrorist IEDs being used overseas. To date, the TEDAC has received over 3,000 devices for analysis with the majority of those devices coming from the Iraq Theater of Operations. In addition, it has made over 350 forensic and technical associations between devices.[16]

The FBI also runs a Large Vehicle Bomb Post-Blast Crime Scene School that replicates a 2002 bomb blast overseas that killed more than 200 people.[17] Students do not watch the explosion, they pick up the pieces—literally—from the scattered wreckage that set the forensic groundwork for a criminal or terrorist investigation. They then learn how to identify the vehicle that blew up.

The post-blast school used to be a basic lesson on working a car-bomb scene—from forensics and equipment to crime scene mapping and processing—but it evolved to a "graduate level" curriculum in 1998 so law enforcement and military investigators with plenty of bomb scene experience can get practical training in the devastation created by large-vehicle explosions.

The FBI has sponsored more than 70 classes around the nation—and two overseas—since the school was launched in 1998. The size of the explosions limits where they can convene; a 6,000-pound bomb, for example, might spread a field of evidence across 225 acres. Fortunately, the U.S. military has provided bases with huge, barren acreage for the classes and even donated vehicles to blow up. Bomb technicians deploying to Iraq and Afghanistan get first priority for the maximum 50 slots of each class.

Traditional Law Enforcement Skills and Capabilities

Because today's threats are more often than not transnational in nature, information of value to prevent harm may be found virtually anywhere in the world. In this environment, law enforcement capabilities, and particularly law enforcement networks, have the potential to gather information of use in many different venues. Additionally, if it is true that we will be combating terrorism for a long time, information discovered today may be useful in years to come. To preserve the integrity of that information, law enforcement skills used in processing "evidence" will be invaluable. Finally, information collected and

[16] Robert S. Mueller, III, Director, Federal Bureau of Investigation before the United States House of Representatives Committee on Appropriations, Subcommittee on Science, State, Justice and Commerce, September 14, 2005. Available online at <http://www.fbi.gov/congress/congress05/mueller091405.htm>.
[17] FBI, "Picking Up The Pieces...And Building A Case From It: FBI School for Large Vehicle Bombs," October 11, 2005. Available online at <http://www.fbi.gov/page2/oct05/postblastschool101105.htm>.

evidence developed in the United States have proved to be of value in reducing the terrorist threat abroad.

Joint Terrorism Task Forces (JTTFs)
JTTFs are small cells of highly trained, locally based investigators, analysts, linguists, SWAT experts, and other specialists from dozens of U.S. law enforcement and intelligence agencies. It is their responsibility to chase down leads, gather evidence, make arrests, provide security for special events, conduct training, collect and share intelligence, and respond to threats and incidents at a moment's notice.

There are more than 100 JTTFs in cities nationwide, including at least one in each of the 56 field offices.[18] Collectively, these offices contain more than 3,700 personnel—more than four times the pre-9/11 total—including approximately 2,200 Special Agents, 850 state/local law enforcement officers, and nearly 700 professionals from other government agencies (the Department of Homeland Security, the CIA, and the Transportation Security Administration, to name a few).

JTTFs have been instrumental in breaking up cells like the "Portland Seven," the "Lackawanna Six," and the "Northern Virginia jihad." They have traced sources of terrorist funding, responded to anthrax threats, halted the use of fake IDs, and arrested suspicious characters with all kinds of deadly weapons and explosives. JTTFs are coordinated through the interagency National Joint Terrorism Task Force, working out of FBI Headquarters, which makes sure that information and intelligence flows freely among the local JTTFs.

Information collected and analyzed by the JTTFs has been instrumental in developing information that has led to the disruption, and sometimes to the prosecution of support elements for terrorists that indirectly confront the military abroad. Sometimes the information collected is more direct, leading straight to information relevant within the battlespace.

Field Intelligence Group (FIG)
The FBI has established a FIG in each of its 56 field offices to manage and coordinate intelligence functions in the field. The FIGs are the mechanism through which the FBI contributes to regional and local perspectives on a variety of issues, including the receipt of and action on integrated investigative and intelligence requirements.

FIGs take raw information from local cases and attempt to make big-picture sense of it. Although relatively new, FIGs already have filled gaps in national cases utilizing locally developed information. FIGs also share their findings, assessments, and reports with other FIGs across the country, and with partners in law enforcement and intelligence. In doing so they seek to frustrate terrorist supporters by, for example, shutting down money laundering schemes or developing the information that will keep a bomb from going off. Intelligence analysts (IAs), not agents, are the lynch pins of the effort. Some are

[18] Sixty-five of these JTTFs were created after September 11, 2001.

dedicated to the big picture, others are actually "embedded" in squads to work with street agents on specific counterterrorism, counterintelligence, and criminal cases.[19]

In addition, FIGs provide an intelligence link to the JTTF, Fusion Centers, FBIHQ, and other intelligence community agencies. FIGs are staffed by IAs, special agents (SAs), language analysts (LAs), and surveillance specialists. As called for in the Intelligence Reform and Terrorism Prevention Act (IRTPA), each FIG reports directly to a field office senior manager responsible for intelligence matters.

Because virtually all terrorism-related arrests in the United States, and many abroad, have involved common criminal enterprises, the FIGs also have the responsibility to correlate information obtained from both intelligence and criminal sources. Additionally, the criminal enterprises uncovered in investigating terrorism issues nearly always lead to overseas connections. That information can then be passed to partner agencies in other nations or even to the United States military, when it is relevant to the conflict environment.

Tracking Terrorists

The Foreign Terrorist Tracking Task Force (FTTTF) was created pursuant to Homeland Security Presidential Directive No. 2 and was consolidated into the FBI pursuant to the Attorney General's directive in August 2002. The FTTTF uses innovative analytical techniques and technologies that help keep foreign terrorists and their supporters out of the United States or lead to their location, detention, prosecution, or removal. Information obtained by the FTTTF will often be relevant to other nations' counterterrorism efforts and even to the United State military deployed abroad.

The participants in the FTTTF include the Department of Defense, the Department of Homeland Security's Bureaus of Immigration and Customs Enforcement and Customs and Border Protection, the State Department, the Social Security Administration, the Office of Personnel Management, the Department of Energy, and the CIA.

To accomplish its mission, the FTTTF has facilitated and coordinated information-sharing agreements among these participating agencies and other public and proprietary companies to assist in locating terrorists and their supporters who are, or have been, in the United States. The FTTTF has access to over 40 sources of data containing lists of known and suspected foreign terrorists and their supporters, including the FBI's Violent Gang and Terrorist Offenders File.

Terrorism Financing

In concert with the Internal Revenue Service, the Central Intelligence Agency, and the Saudi Mabahith, the FBI has created the Terrorism Financing Operations Section (TFOS). As originally conceived, this task force specialized in facilitating counterterrorism financing investigations with leads connected to the Kingdom of Saudi

[19] FBI, "FOCUS On FIGs: Networking Intelligence Across the U.S. to Prevent Crimes and Terror," April 27, 2005. Available online at <http://www.fbi.gov/page2/april05/fig042705.htm>.

Arabia. TFOS has also aggressively pursued a rigorous, multi-phase training program for the Saudi Mabahith officers assigned to the task force.

Most importantly, TFOS combines the FBI's traditional expertise in conducting complex criminal financial investigations with advanced technologies and has built upon these established mechanisms. TFOS has also facilitated cooperation and coordination among law enforcement, regulatory, and intelligence agencies, both domestic and foreign, to create an internationally effective terrorist financing investigative operation. The mission of TFOS has evolved into a broad effort to identify, investigate, disrupt, and dismantle all terrorist-related financing and fund-raising activities.

Terrorist Screening Center

The TSC is a unified watch list of known or appropriately suspected terrorists that can be tapped into by every official sworn to protect the U.S.—everyone from border patrol and transportation officials to federal agents and local police officers working their beats. "There is one watch list," TSC Director Donna Bucella told reporters during an informational briefing at FBI headquarters. "Our list is not a stagnant list. We add, modify, and delete every day."[20]

The terrorist identities information that flows into the TSC comes from the FBI (domestic terrorist information) and the National Counter Terrorism Center (international terrorist information), which gets information from more than a dozen intelligence agencies, such as the CIA and DHS, under the umbrella of the Director of National Intelligence.

By serving as the day-to-day, 24-hour conduit that links front-line law enforcement to critical field intelligence on terrorists, TSC staff is able to do more than maintain the database and link calls. Their access to a constant flow of intelligence helps them assemble the big picture of potential threats and connect the dots for the agencies they support.

Weapons of Mass Destruction

Transnational and domestic terrorists and state sponsors of terrorism continue to demonstrate an interest in acquiring and using chemical, biological, radiological, and nuclear weapons, or CBRN. CBRN weapons would be advantageous for terrorists to use to cause mass casualties, mass panic, and economic disruption, and summon U.S. government responses. If it is true that we are in for a protracted struggle against terrorism, the chance of avoiding a WMD event grows increasingly slimmer.

Few if any terrorist groups are likely to have the capability to produce complex biological or chemical agents needed for a mass casualty attack, but their capability will improve as they pursue enhancing their scientific knowledge base by recruiting scientists as some

---

[20] Donna Bucella, "The Terrorist Screening Center," March 15, 2006**.** Available online at <http://www.fbi.gov/page 2/march06/tsc031506.htm>.

groups are doing. Currently, terrorist groups have access to simple chemical and biological agent recipes passed on at training camps or through the Internet and anarchist cookbook publications.

Obtaining or developing chemical, biological, or toxin weapons is difficult, but these weapons have been used for terror purposes. Sarin, a chemical nerve agent, was used in the Tokyo subway system in 1995 by the Aum Shinrikyo cult. Anthrax bacteria were used in 2001, infecting individuals in Connecticut, New York, Florida, and the District of Columbia. Also, salmonella bacteria were used by the Rajneeshee cult in 1984 in an attempt to influence local election turnout. Ricin, a toxin, was mailed to the White House in 2003 and Congress in 2004.[21]

The intent of terrorists to obtain weapons-usable material is a continuing concern. A terrorist nuclear attack is the least likely WMD event because of the high level of technical expertise required and the difficulty of acquiring fissile material. Building and using a radiological dispersal device, however, is well within the capability of extremists who already understand explosives. And acquiring radiological material, which is available in civilian facilities, is not as difficult as acquiring fissile material, which tends to be heavily guarded, usually by military forces.

Fortunately, no country has had experience with a "dirty bomb." However, we can make some assumptions drawing on the facts of a radiological accident that unfolded in Brazil between 13 September 1987 and March 1988. In that case, an abandoned radiotherapy clinic was burglarized and a capsule containing Cesium 137 Chloride was broken open. From this incident of common burglary, over 112,000 people were potentially exposed. After careful monitoring it was determined a total of 249 people had been contaminated by the Cesium-137. Of these, 151 exhibited both internal and external contamination and 49 were admitted to hospitals, with the 20 most seriously irradiated having received doses from 100 to 800 rads. The internally contaminated patients were themselves radioactive, seriously complicating their treatment. In the end, 28 people suffered radiation burns and five died, including three men, one woman, and one child. [22]

To counter this type of threat, the FBI established the WMD Directorate in July 2006 to consolidate the FBI's WMD components. The Directorate integrates and links all the necessary intelligence, scientific, and operational components to detect and disrupt the acquisition of WMD capabilities and technologies for use against the U.S. homeland by terrorists and other adversaries. Additionally it relies on networks with agencies of other governments to cull information from human sources that may be in a position to observe and report attempts to gather the materials for WMD devices.

---

[21] Dana Shea, Congressional Research Service, "Terrorism: Background on Chemical, Biological, and Toxin Weapons and Options for Lessening Their Impact," December 1, 2004. Available online at <http://www.ndu.edu/library/docs/crs/crs_rl31669_01dec04.pdf>.

[22] Peter D. Zimmerman and Cheryl Loeb, "Dirty Bombs: The Threat Revisited," *Defense Horizons* 38 (Washington, DC: National Defense University Press, January 2004).

Gathering Information: The Ad-Dujayl Case
Collecting and organizing information is the stock-in-trade of law enforcement. This basic skill is increasingly proving to be important in conflict regions. The Ad-Dujayl case serves as one example.

On July 8, 1982, a small group of dissidents attacked a convoy in which Saddam Hussein was riding. Within hours the Iraqi Intelligence service arrived under the leadership of Saddam's half-brother, Barzan al-Tikriti, who ensured that:

- Every male over the age of 13 who could carry a weapon was arrested;
- 15 males were summarily executed and others were tortured;
- 147 men and boys were tried by the Revolutionary Court and executed;
- More than 1,000 were detained, and 399 women and children were held in a remote desert prison until 1986;
- All orchards and farm lands for a kilometer around the village were razed.

This incident has been well publicized because the war crimes trial that resulted in the executions by hanging of Saddam Hussein, his half-brother, and the judge who condemned the 147 men and boys. What is less widely known is that preparation for the trial began in 2004, when FBI agents were sent to Ad-Dujayl to interview witnesses and prepare them for trial. The FBI work delivered information sufficient to cause an indictment that was handed down in 2005.

Without a heritage of due process and evidentiary requirements, the nascent government of Iraq was in need of experts to help in gathering and structuring information related to other crimes of the prior regime. Accordingly, the FBI was asked to provide the expertise of American law enforcement to gather information, validate it for use as evidence, and assist in preparing trial witnesses for prosecution of Iraqi crimes committed in the course of:

- Summary executions through abuse of the judicial system;
- The destruction of the world's largest wetlands which destroyed the livelihoods of hundreds of thousands of Marsh Arabs during the period 1985-2003;
- War crimes committed during the 1990-91 invasion of Kuwait;
- The 1991 Shi'a Uprising and Saddam's offensive against Shi'a Iraqis in the South following the 1991 Gulf War; and
- A 1998 offensive that killed some 100,000 Kurds.

In addition, the FBI is assisting the Iraqi High Tribunal in pursuing some additional cases of brutality, such as the cutting off the ears of Army deserters, forced sterilizations, and the killing of all males in one clan.

Preserving Information
Precisely because the contemporary threats have no time horizon, carefully preserving information becomes an important intelligence capability. Preservation of information

seized, even on the battlefield, may be important for future prosecutions, but even more so for making sense of other information acquired later. For example, what does it mean to find a telephone number in a country without telephone books? Phone numbers in other countries can be traced through law enforcement channels, but rarely through military capabilities. It is a normal function of the FBI to build up dossiers on every potential criminal or terrorist. These dossiers often have fingerprints and, increasingly, include DNA. Law enforcement agents also have provided training to U.S. military personnel on how to exploit "pocket litter."[23]

In the battlespace, law enforcement officers have applied law enforcement skills to data, tangible objects, and interrogations of individuals. They have photographed, catalogued and organized items as they would for evidentiary purposes, thereby preserving the integrity of the items for future reference. Moreover, they have applied their skills operationally, providing interpretation of information that often has been instrumental in helping the military know how and where to next apply force.

The FBI has also developed the Investigative Data Warehouse (IDW), a centralized, web-enabled, closed system repository for intelligence and investigative data. This system, maintained by the FBI, allows appropriately trained and authorized personnel throughout the country to query for information of relevance to investigative and intelligence matters. Information contained in IDW comes from all agencies of government, and, importantly, from information picked up on the battlefields of Iraq and Afghanistan.[24]

IDW now provides special agents, intelligence analysts, and members of JTTFs with a single access point to more than 47 sources of counterterrorism data, including information from FBI files, other government agency data, and open source news feeds, that were previously available only through separate, stove-piped systems. New analytical tools are used across multiple data sources, providing a more complete view of the information possessed by the Bureau. IDW now contains over 560 million FBI and other agency documents from previously stove-piped systems.[25] Nearly 12,000 users can access it via the FBI's classified network from any FBI terminal throughout the globe.

IDW is not merely an FBI tool; nearly 30 percent of the user accounts are provided to task force members from other local, state, and federal agencies. Users can also access billions of structured records to find, for example, addresses and phone numbers in seconds. They can also search rapidly for pictures of known terrorists and match or compare the pictures with other individuals in minutes rather than days. Coupled with state-of-the-art search tools, the IDW enhances the Government's ability to identify relationships across cases quickly and easily.

---

[23] Law enforcement officers are well aware that the items a person carries have significance to the person, be they a phone number, a matchbook from a favorite bar, or the address of a girlfriend. All of this pocket litter tells a story about the person's habits and will often lead to the next piece of the puzzle.

[24] FBI, "Draft Audit Report: The Federal Bureau of Investigation's Management of the Trilogy Information Technology Modernization Project," January 26, 2005. Available online at <http://www.fbi.gov/pressrel/pressrel05/response.htm>.

[25] FBI, Statement of Deputy Director John Pistole before the Senate Select Committee on Intelligence, January 25, 2007. Available online at <http://www.fbi.gov/congress/congress07/pistole012507.htm>.

Fly Teams

Bombs are not the only things that can yield clues for prevention of terrorism incidents, but intelligence is often subtle and difficult to extract. To account for the complexities of modern life, the FBI has also developed "fly teams."[26] These are small, highly trained cadres of terrorism first responders—including agents and analysts—who have their bags perpetually packed and can reach anywhere on the globe in hours. They bring a capability to conduct sensitive, high-profile counterterrorism investigations even in difficult and dangerous and hostile environments. The agents and analysts collectively speak about a dozen languages, including Arabic, Spanish, French, Swahili, and Dutch. These agents and analysts are selected after rigorous tests, drills, and team-building exercises. They learn everything from advanced post-blast investigative techniques to how to use specialized weapons and handle hazardous materials. They are taught combat medical skills, fingerprinting, hostage survival and resistance, and cultural awareness. They study all aspects of terrorism and get briefings from a range of terrorism experts. Between deployments, they fine-tune their skills.

Once called, they quickly gather intelligence reports and information about the situation, talk to their counterparts in the field, assemble equipment and pull together situation-specific specialists as needed — evidence experts, bomb technicians and HAZMAT personnel are examples. They learn as much as they can about the locale. Once on the ground, the Fly Team quickly sets up a command post. They share and compare information and intelligence with FBI offices around the globe through a secure computer network. They proactively identify potential terrorist targets and work to prevent future attacks. Once the investigation is solidly in motion, the team hands it over to long-term investigators and heads home. Fly teams have been called on numerous times in the last few years, including assignments in Afghanistan and Iraq.

Communications

Advances in communications technology have made our lives easier, but have also given terrorists and criminals the means to communicate more easily. Twenty years ago cell phones were relatively rare, clunky, expensive, and inefficient devices. Today, they are being marketed to children. Cell phones and satellite phones are used by terrorists just as commonly as they are by organized crime.[27] What this means is that surveillance of terrorist communications is needed. The FBI has stated many times that the defeat of organized crime on the East Coast could never have been accomplished without electronic surveillance—which is just as important to countering terrorism. However, electronic surveillance is much more difficult today than it was forty years ago, and not just because of the ubiquity of cell phones─the Internet poses even greater problems.

Al Qaeda has set a standard for terrorists by embracing the Internet as a new tool for organizing, training, and propagandizing. Although the Internet was used twenty years ago, improvements in computer, communications, and storage technology have made it a

[26] FBI, "Protecting America From Terrorist Attack: The FBI's Fly Team: Have Expertise, Will Travel," March 30, 2005. Available online at <http://www.fbi.gov/page2/march05/flyteam033005.htm>.

[27] A satellite conversation of Osama bin Laden was declassified and used as evidence in the trial of the 1998 embassy bombers.

medium of choice for communications, information gathering, and anonymous activities. Moreover, it is so cheap ─ often free ─ that anyone, and virtually everyone, can use it. It is also so ubiquitous that scope alone makes monitoring a daunting and cumbersome task. A group believed to be Al Qaeda's Web-based propaganda arm recently debuted a weekly state-of-affairs Webcast and is reportedly searching online for recruits to aid with the coverage ─ meaning that the group, and their recruits, will be searching for more and more computers to hijack in order to distribute additional content.

Many Al Qaeda members are sophisticated and educated.[28] Using the skills of modern technocrats, Al Qaeda has adopted online tactics that mirror its offline techniques for evading discovery: instant messaging, chat, bulletin boards and reliance on a constantly shifting collection of Internet sites and hostile takeovers of Web servers where propaganda can be posted. For example, in 2005, a server operated by the Arkansas highway office was hijacked and used to distribute 70 files including videos featuring Osama bin Laden.

Officials of all nations are faced with the prospect of choosing between sabotaging terrorist uses of the web (commonly referred to as "whack-a-mole") or attempting to monitor them. Neither option yields a satisfactory response. On the one hand, there is an agile ability for even the marginally technologically savvy person to put up web sites. On the other, monitoring the web is like counting grains of sand on a beach, so vast are the opportunities and methods of communication over the Internet. Moreover, if the choice is to monitor it begs the question of who will do it, and, perhaps, who has the authority to do it.

Despite the difficulty, monitoring electronic communications is an avenue that will always hold promise. More than 70 percent of the world's communications pass through gateways in the United States. Also, because the Internet was invented here, the largest Internet providers are located in the United States. Moreover, Hotmail and Yahoo offer unlimited free accounts. Terrorists can, and do, use the Internet extensively, undoubtedly changing their free accounts as often as practicable. A terrorist in Pakistan can log into a Yahoo account in the United States and communicate with a networked terrorist in Jordan—perhaps even a person he had never met. Chat rooms, instant messaging, anonymizers and other attributes of modern communications make the life of a terrorist much more agile.

However, monitoring email is electronic surveillance. Just as with telephone monitoring, it requires, with rare exceptions,[29] a judicially approved warrant.[30] That is, in most cases,

[28] There is a non-apocryphal story about a person who tried to join Al Qaeda several years ago. When interviewed by a senior leader of the organization it was learned that he had no formal higher education. The individual was told to go back to school, get an engineering degree and then come see them again.
[29] The controversy over certain activities of the National Security Agency is not included in any of the succeeding discussion.
[30] Other nations often have even greater difficulty with gaining approval for electronic surveillance. For some, authority is strictly limited. Other nations are not permitted to use the results of such surveillance in a court of law.

a function of law enforcement acting through judicially tested mechanisms that are monitored by the Attorney General.

Sharing Information

In an era of transnational threats, the mandate to share information is a *sine qua non* of success by any measurement. For domestic law enforcement organizations, and particularly for the FBI, it is especially difficult due to restrictions on the dissemination of privacy-protected information. This is true because the FBI inevitably collects vast amounts of collateral information in the course of domestic investigations. This collateral information is carefully restricted from disclosure and, depending on several variables, often separated altogether from the "relevant" information sought.

Nevertheless, the ability to pull information together for broad-scope analysis is a requirement for counterterrorism efforts and the FBI is the only source of this broad-scope domestic information. To manage this requirement, and to protect privacy, the President and Congress have mandated an all-source center where all terrorism information in the possession of the United States can be collated and analyzed by a limited number of individuals. The result was the National Counterterrorism Center (NCTC).

United States Government agencies are required to share *all* foreign intelligence related to terrorism with NCTC. Additionally, pursuant to the Intelligence Reform Act, domestic terrorism information in possession of the FBI may/must be shared with NCTC as well. This is an important modification to laws that have become clumsy in an age of transnational and fast-paced threats.[31] As previously noted, clues produced in the United States, from financial matters to telephone calling records, may be relevant to projected terrorism activities in the Homeland, in other nations, or in the conflict zones where American military are threatened.

[31] Normally, privacy-protected information would be disclosed by the FBI only to another agency which could either aid the FBI understanding the information or further developing it for FBI needs. Alternatively, if the privacy information were relevant to the other agencies mission it could be disclosed. Shedding those rather strict conditions, this information, which combined with other information, might yield valuable clues for prevention of harm, can be brought out of the dark for analysis. If found not useful, the privacy information would again be relegated to the arena of privacy protections, having been disclosed to a minimal number of persons who are trained in the required procedures for protection of privacy.

Instructor's Guide to Counterterrorism Activities of the FBI: At Home and Abroad

The role of the FBI in combating terrorism is a useful subject in itself, and one that increasingly bears on the military role abroad. However, for purposes of this case study, it should be discussed with broader concepts in mind.

First should be the strategic importance of coalescing interagency skills in modern warfare.

Second is a consideration of the force multiplier capabilities of law enforcement skills in a combat environment.

Third should be the tactical significance of interagency skills in the modern battle space.

The following objectives are among possible discussion points:

Objective 1: Provide an assessment of the strategic importance that law enforcement skill sets bring to the concept of military transformation.

Objective 2: Demonstrate the tactical importance of law enforcement skills in the battle space.

Objective 3: Analyze the implications for mission planning of having and using multiple, non-combat United States Government agencies in the battle space.

Objective 4: Analyze the challenges for agencies like the FBI, Treasury, and Customs in applying their expertise in a war zone.

Objective 5: Assess the means to optimize interagency skills in and for the battle space.

Discussion Points for Objective 1: When the enemy is transnational in character and organization, the ability of the warfighter to engage is severely truncated. Moreover, in an era of instantaneous and long-range communications, the ability of networked law enforcement agencies worldwide to focus on individuals across borders is an absolute requirement as a force multiplier. Additionally, the forensic capabilities of law enforcement to identify individuals (and where they have been) through DNA, fingerprints and even through their handicraft (e.g., bomb-making skills) are a critical asset. Another law enforcement asset is rudimentary training for the warfighter. When the enemy and the populace look alike, it is important to know what identifiers to look for in encountering individuals and how to maintain records that will be useful for the future. Law enforcement does this routinely and can be a resource of training for the military.

Questions for Objective 2: What skill sets can law enforcement bring to the battlespace? There are probably several answers to this. For one thing, when the enemy is an irregular and widely dispersed force, or set of forces, information is the key to engagement. There

is often substantial information available, but it is of a type that law enforcement, and sometimes intelligence officers are accustomed to dealing with – the warrior is not. For example, pocket litter – the detritus we all carry with us may contain telephone numbers, names, addresses, etc. In regions that do not sport telephone books this information can be valuable. However, it is also the case that the information may not be useful when discovered but may be at a later point in time. What that means is that the integrity of the information – where it was found, in what circumstances, who possessed it, etc. – must be available for the future. For this, evidence-handling procedures are invaluable. Similarly, interrogations skills are far superior in the law enforcement community – especially if the person being interrogated is in detention and not on the battlefield.

Questions for Objective 3: Should the military commander, or even the squad leader, take into account the skill sets of civilian agencies in planning missions? To what extent must the military commander plan around the missions of the inter-agency in the battle space? There are two main lines of thought concerning this. One leads directly to the military mission and the extent to which other agencies can contribute to tactical advantage. The second concerns the broader picture of winning the peace. It is simply insufficient merely to win military victory. Experience clearly shows that more than 50 percent of all conflicts of the past three decades have subsequently re-erupted because the arena of conflict was left unstable. If the conflict arena is not stabilized legally, politically and economically, military prowess will go for naught. Therefore the skill sets of civilian agencies need to be brought in early to begin erecting a stable regime. That means that military planning needs to maximize the opportunity of civilian agencies to apply meaningful skills to the environment.

Questions for Objective 4: How do civilian agencies, historically unprepared to go into combat zones, prepare for the battle space? What is the role of the military in preparing civilian agencies? It is an article of faith that a stable regime is an international necessity. As shown in the Balkans conflicts, unstable regimes cause regional instability so every effort must be made to create stable regimes when conflict is ended. It may be necessary to rebuild financial systems (Treasury), create judicial systems for governance (Justice) and reconstitute police (Justice/law enforcement). What makes this all difficult is that none of the potentially needed agencies are prepared either for combat zones or for collaboration with the military or with each other. A governance mechanism is needed. Civilian agencies need to learn from the military what the battle space is like, how military operations are carried out and where they will be and for what purpose they are designed. In turn, civilian agencies need to be able influence military operations in order to maximize their own capabilities. The chicken-and-egg quality of this should be obvious to all, however it will likely fall to the military to convince the interagency that each agency needs to think, and act, beyond its own singular mission. For example, when the FBI went into Iraq it was initially to exploit intelligence archives. Once on the ground, however, both agent and warrior recognized symbiotic needs even if their superiors in Washington had not yet learned that lesson.

Questions for Objective 5: How can the various skill sets of the inter-agency be brought to bear in a combat zone? Is there a mechanism to coalesce those skill sets? What entity is, or should be, responsible for bringing an inter-agency perspective to the battle space? This is the most difficult part of the equation and there is no simple or easy answer. There may not be an answer at all. However, there is one instructive, if nascent prototype that may be worth evaluating. When CENTCOM was given the Afghanistan mission General Franks stood up a small inter-agency coordinating committee. It has representatives from several major agencies on it, including the FBI. By all accounts it was a highly successful experiment – for what it was. It was too small to do more than provide advice and guidance to the COCOM. It was not even robust enough to be a theater-wide asset. However, it was very effective within its limited sphere of influence. It may be worth considering whether there should be something on a national scale – perhaps similar to the National Security Council – that can provide a permanent focus on skill sets that are available in the inter-agency, where they may be physically located and that can recommend to the President what civilian skills are needed in a particular environment. Students will no doubt think of other potential mechanisms.

Bottom Line: If the conflict zones of the past two decades are a harbinger of the future, no conflict will be fought, or won, by military force alone. In many, perhaps most, instances, the military role may be the most poignant mission, but not the most important. The military will not create stability in a regime. It can stabilize it in place while civilian agencies apply their skills for a future regime that can take its place in the community of nations, but that is all. If the military merely establishes combat superiority without more, history indicates that the society it leaves behind will be open to organized crime, insurgency, corruption and future conflict.