Vehicle is destroyed as part of post-blast crime scene demonstration

U.S. Air Force

Law Enforcement Technology, Intelligence, and the War on Terror

By **M. E. BOWMAN**

The warfare that most of us trained for now seems likely to become more an artifact of historical interest than the reality we feared. Today, the objective of conflict is less to obtain a political outcome than to create the conditions necessary for stability and responsible participation in international affairs. Perhaps the most striking difference from the war that Carl von Clausewitz spoke of is that today's conflicts have no time horizon. Still, there are constants; one is the requirement for intelligence concerning the enemy.

History illustrates that intelligence is a critical element of success in conflict. Even so, when military conflict encompasses transnational threats that include terrorism, insurgency, organized crime, weapons proliferation, and weapons of mass destruction—all of which inevitably invite the complications of public corruption—intelligence takes on a new meaning and generates requirements unknown a few years ago. The reasons are many, with technology at the top of the list.

Even though intelligence remains a critical element of warfare, it is startlingly apparent that the Department of Defense (DOD), even with a vast array of intelligence capabilities, is not able to produce and analyze all the vital information necessary. In an era when the enemy is supported globally and transnational capabilities for communications, financial transactions, and transportation confound the utility for direct application of force, civilian agencies are key to obtaining vital elements of information for the success of the mission.

Indeed, modern technology has greatly improved the combat capabilities of the American fighting forces. Network-centric warfare is a significant technological advancement and a proven way of fighting both more efficiently and more safely. However, the object is no longer merely to win the fight. Today, the object is to win the peace, which means creating conditions that will lead to stable societies. For that, partnering the technologies and capabilities of law enforcement, particularly those found within the Federal Bureau of Investigation (FBI), with the military mission is necessary. Coupling the innovations and skills discussed in this article with true cooperation between civilian law enforcement and the U.S. military will undoubtedly lead to a more effective prosecution of the war on terror.

Communications

Advances in communications technology have made our lives more convenient, but they have also provided the means for terrorists and criminals to communicate more easily. Twenty years ago, cellular telephones were relatively rare, clunky, and inefficient. Today, they are marketed to grade-school children. Cell phones and satellite phones are used by terrorists just as commonly as they are by organized crime members. What does

M.E. "Spike" Bowman is a Senior Research Fellow in the Center for Technology and National Security Policy at the National Defense University. Previously, he served in the Senior Executive Service at the Federal Bureau of Investigation.

this mean? Take a clue from organized crime: The FBI has stated many times that the defeat of organized crime on the U.S. east coast could never have been accomplished without electronic surveillance. The same is true of terrorism, but the task is now infinitely more difficult because of not only cell phones but also the Internet.

Members of al Qaeda may live in caves, but many of them are sophisticated and learned. Using skills unimagined only a few years ago, al Qaeda has set a standard for terrorists by embracing the Internet as a tool for organizing, training, and propagandizing. Although the Internet is not new, improvements in computer, communications, and storage technology have made it a medium of choice for networking, information-gathering, and anonymous activities. Moreover, it is so cheap—often free—that anyone can use it.

Using the skills of modern technocrats, al Qaeda has adopted online tactics that mirror its offline techniques for evading discovery. These tactics include instant messaging, chat, bulletin boards, and a constantly shifting collection of Web sites where propaganda can be posted. For example, in 2005, a Web server operated by the Arkansas highway office was hijacked and used to distribute 70 files, including videos featuring Osama bin Laden. Recently, a group believed to be al Qaeda's Web-based propaganda arm debuted a weekly state-of-affairs Web cast and is reportedly searching online for recruits to aid with the coverage. This means that the group and their recruits will be searching for more and more computers to hijack in order to distribute additional content.

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, nearly anyone can 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 questions of who can do it and who has authority to do it.

The largest Internet providers are located in the United States. 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. Chat rooms, instant messaging, anonymizers, and other attributes of modern communications make the life of a terrorist much more flexible. However, monitoring email requires a judicially approved warrant. This means that the military must depend on law enforcement, perhaps even that of many nations, to bring in that part of the intelligence puzzle.

using the skills of modern technocrats, al Qaeda has adopted online tactics that mirror its offline techniques for evading discovery

Iraqi man in custody fingerprinted at Camp Fallujah, Iraq

U.S. Marine Corps (Louis Corwise)

DNA Testing

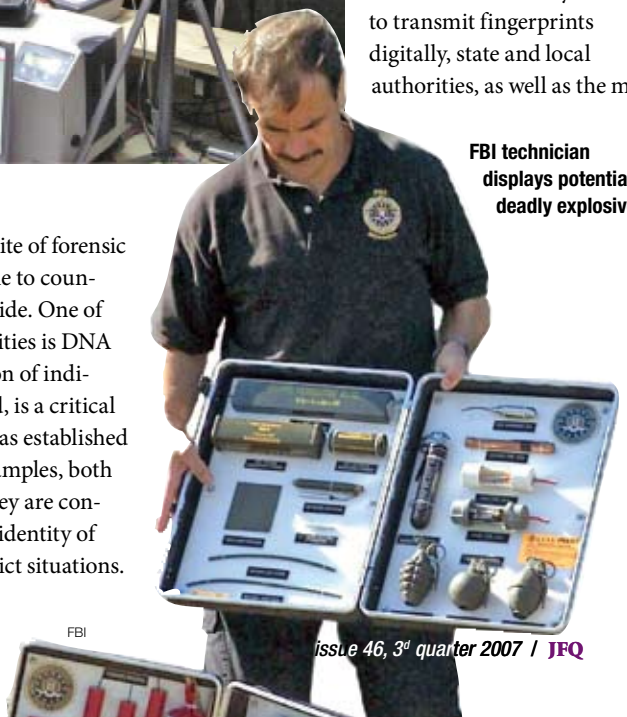
The FBI has a large suite of forensic capabilities that are germane to counterterrorism efforts worldwide. One of the most important capabilities is DNA testing. Precise identification of individuals, both alive and dead, is a critical need. To this end, the FBI has established a large inventory of DNA samples, both to identify persons when they are confronted and to confirm the identity of bodies resulting from conflict situations. For example, 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 airstrike by Pakistani forces near the border with Afghanistan.[1] On the other side of the world, FBI DNA testing confirmed the death of the Philippines' "most wanted" terrorist.

However, as valuable as this identification capability is, there are more subtle uses for DNA. For example, even though the body of Abu Musab al-Zarqawi was identified by fingerprints, tattoos, and scars after he was killed in an airstrike, DNA samples were sent to the FBI crime laboratory in Quantico, Virginia. The DNA collected was then compared to other samples in an effort to help establish locales where al-Zarqawi had been and who had been with him.

Fingerprints

One of the most common forensic capabilities is fingerprinting.[2] The FBI maintains an Integrated Automated Fingerprint Identification System (IAFIS), which comprises the largest biometric database in the world. It contains the fingerprints and corresponding criminal history information for more than 47 million subjects in the criminal master file. This information is submitted voluntarily by state, local, and Federal law enforcement agencies.

With the ability to transmit fingerprints digitally, state and local authorities, as well as the mil-



FBI technician displays potentially deadly explosives

FBI

itary abroad, can send prints for comparison and receive electronic responses to criminal 10-print fingerprint submissions within 2 hours and civilian fingerprint submissions within 24 hours. The ability to identify suspected terrorists and insurgents in Iraq and Afghanistan is a highly desirable capability. As early as April 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.[3]

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. Consequently, if those fingerprinted subsequently attempt to enter the United States, they will be flagged. When a large group was rounded up in 2004 in Iraq, 44 were determined to have criminal records in the United States and 2 were sought on Federal warrants.[4] In 2005, the Department of Defense created its own biometric database, the Automated Biometric Identification System (ABIS), modeled on IAFIS. To ensure quality and interoperability of all fingerprint data collected, DOD has directed that all acquisitions related to fingerprinting must conform to the same standards and be interoperable with the IAFIS system.[5]

today, suspected terrorists are "booked" using the same tools that police in the United States use to check criminal backgrounds

Now, prints sent to ABIS are sifted through IAFIS, where they are screened and compared to the FBI's most-wanted terrorists lists.[6] 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 United States in August 2001.

Improvised Explosive Devices

More deaths in Iraq are caused by improvised explosive devices (IEDs) than anything else. Additionally, IEDs have become the weapon of choice for terrorists worldwide. To address this threat, in December 2003, the FBI created the Terrorist Explosive Device Analytical Center (TEDAC). This center established a single Federal program responsible for the worldwide collection, complete forensic and technical analysis, and timely dissemination of intelligence regarding terrorist bombs. All information gleaned from TEDAC's analysis is shared throughout the law enforcement, intelligence, and military communities.

Additionally, using breakthrough technology, FBI technicians are beginning to identify the locales where the devices are made and even who is making them.[7] According to a 5-year accounting of FBI progress in transformation, 56 bomb-makers were identified through TEDAC analysis.[8] These analyses suggest that there is a relatively small number of master bomb-makers, and those identifications have resulted in the capture of some, while others who were identified are being sought.

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. Students do not watch the explosion; they pick up the actual pieces 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 started as 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 2

U.S. Navy (Jim Watson)

Agents examine Pentagon after terrorist attack

overseas—since the school was launched in 1998. The size of the explosions limits where the course 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 vehicles to blow up. Bomb technicians deploying to Iraq and Afghanistan get first crack at the maximum 50 slots in each class.

Financing

The technology that allows us to pay our bills online or send money to a child at college also permits the transfer of funds to or between terrorists. If those funds can be stopped short of their ultimate goal, the means to finance the terrorist fight against military forces can be curtailed. To do so, however, requires investigations at a great distance from the battlefield and often involves the authorities of several nations. It also requires information developed in the conflict zone—information that may be best recognized and evaluated by law enforcement personnel. However, the situation is complicated for two reasons. First, money laundering is not illegal in most nations. Second, and of immense importance, transactional data are not required to "follow the money." That means anonymous transfers of money are both possible and likely.

Where do authorities have to look to find the sources of terrorism financing? Donors, nongovernmental organizations, and criminal enterprises all fund terrorist causes. The Detroit U.S. Attorney's Office recently indicted a Hezbollah smuggling ring operating in Michigan that helped fund that terrorist organization with profits from bootlegged cigarettes, counterfeit tax stamps, phony Viagra tablets, and stolen toilet paper, according to a Federal indictment unsealed in Detroit in July 2006. A similar Hezbollah ring was prosecuted in North Carolina in 2003.

Other terrorist supporters in the United States have been indicted for credit card fraud, smuggling blue jeans, and currency violations. Moreover, just as with terrorism itself, terrorism financing is global. According to the Canadian agency responsible for tracking money laundering, Canada's suspected financing for terrorism almost tripled to C$180 million (US$153 million) in 2005.[9] In the United States, a Federal judge found two U.S.-based Islamic charitable organizations and an individual fundraiser liable for the 1996 killing of an American in Israel by Hamas terrorists. The Islamic Association for Palestine and the Texas-based Holy Land Foundation were both found liable for funneling money to Hamas.[10]

Battling such sources of terrorist support is a universal task—and one that yields information at every turn. The need is to exploit that information. In November 2005, more than 180 experts from 55 countries met in Vienna to consider the problem. Attendees included specialists from the North Atlantic Treaty Organization, United Nations Office on Drugs and Crime, U.S. State Department, and the Organization for Security and Cooperation in Europe.[11]

Closer to home, U.S. intelligence agencies, including those of the Department of Treasury and FBI, have been adopting innovative forms of investigation to deal with the issue. For example, the Terrorist Financing Operations Section (TFOS) of the FBI Counterterrorism Division was formed in response to this critical need. TFOS combines traditional FBI expertise in conducting complex criminal financial investigations with advanced technologies and has built on these established mechanisms by obtaining cooperation and coordination among law enforcement, regulatory, and intelligence agencies, both domestic and foreign, to become an internationally effective terrorist financing investigative operation. The mission of TFOS has evolved into a broad strategy to identify, investigate, disrupt, and dismantle all terrorist-related financing and fundraising activities. Following the money can lead to an individual relevant to the military mission abroad.

following the money can lead to an individual relevant to the military mission abroad

Weapons of Mass Destruction

If it is true that we are in for a long, drawn-out struggle against terrorism, the chance of avoiding another event involving weapons of mass destruction (WMD) grows slimmer. The difficulty of obtaining or developing chemical, biological, or nuclear weapons has made their use rare, 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 in Oregon. Ricin, a toxin, was mailed to the White House in 2003 and Congress in 2004.[12]

Domestically, there is a significant opportunity to control access to materials that contribute to WMD. Federal law enforcement agencies now have greater power to gather intelligence on terror groups and their members. Increased information about groups, combined with apprehension of any who have chemical or biological weapons, may create further barriers to terrorist acquisition and use of these weapons. A registration system for researchers and facilities possessing select agents has been developed by the Department of Health and Human Services, and additional restrictions regarding access to these agents have been made law.

Internationally, the picture is far murkier. Where terrorists find haven, they can seek the means of destruction they desire. It is known that terrorists have experimented with chemical and biological materials, most likely without significant success. Furthermore, most chemical and biological agents are difficult to apply with the precision that would be desirable to induce terror. However, chemical, biological, radiological, and nuclear weapons are themselves harbingers of fear, so it is almost beyond cavil that terrorists will seek and use them if possible.

Although there is repeated evidence of terrorist interest in chemical weapons or chemically enhanced explosive devices, available information suggests that this is more a reflection of jihadist aspiration than an indication of genuine capability. Nevertheless, jihadist Web forums contain manuals describing the construction of gas dispersal devices. Also, in late 2001, videos discovered in Afghanistan purported to show the testing of hydrogen cyanide gas on dogs.

This category also has to take into account the possibility of a "dirty bomb." There are no truly accurate historical events that give us an idea of what the effect of a dirty bomb might be. However, there is a relevant event in which a tragic radiological accident occurred in Brazil between September 1987 and March 1988. An abandoned radiotherapy clinic was burglarized, and a capsule

containing Cesium-137 chloride was opened and handled by several individuals. From this incident of common burglary, over 112,000 people were potentially exposed. After careful monitoring, it was determined that a total of 249 people had been contaminated. Of these, 151 exhibited both internal and external contamination and 49 were admitted to hospitals, with the most seriously irradiated having doses from 100 to 800 rads (radiation absorbed dose). The contaminated patients were themselves radioactive, seriously complicating their treatment. In the end, 28 suffered radiation burns, and 3 men, 1 woman, and 1 child died.[13]

Far more problematic is the potential use of conventional explosives or other easily obtained materials to create a WMD event. Not unlike the idea of turning fuel-laden aircraft into WMDs, a conventional explosive at a chemical plant or a dam could wreak massive destruction. When household items, fertilizer, or castor beans can be turned into WMD devices, it is not governments, with all their capabilities, that are likely to detect the threat. Rather, it is local policemen, storekeepers, tourists, and ticket agents who are the eyes and ears of prevention. If terrorism is to be prevented, then any theory of transformation has to take into account all those who have a role in prevention.

U.S. Air Force (Roy Santana)

Decontamination facility set up after simulated chemical attack during Exercise Seahawk

Terrorist Screening Center

The Terrorist Screening Center (TSC) is a unified watch list of known or appropriately suspected terrorists that can be used by every official sworn to protect the United States—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 a briefing at FBI headquarters. "Our list is not a stagnant list. We add, modify, and delete every day."[14] The 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 Central Intelligence Agency and the Department of Homeland Security, under the umbrella of the Director of National Intelligence.

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

Preserving Information

Precisely because contemporary threats have no time horizon, carefully preserving information becomes an important intelligence capability. 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. Additionally, law enforcement agents have provided training to U.S. military personnel on how to exploit "pocket litter."[15] Moreover, it is a normal function of the FBI to build up dossiers, often with fingerprints and increasingly with DNA, on every potential criminal or terrorist.[16]

In the battlespace, law enforcement officers have aided military enterprises by applying 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.

Of significant importance, the FBI has developed and maintains the Investigative Data Warehouse (IDW), a centralized, Web-enabled closed system repository for intelligence and investigative data. This system allows appropriately trained and authorized personnel throughout the country to submit queries relevant to investigative and intelligence matters. Information contained in IDW comes from all agencies of government and, more importantly, from information picked up on the battlefields of Iraq and Afghanistan. This is a constantly growing database.

IDW now provides special agents, intelligence analysts, and members of Joint Terrorism Task Forces 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, stovepiped

law enforcement officers have aided military enterprises by applying law enforcement skills to data, tangible objects, and interrogations

systems. New analytical tools are used across multiple data sources providing a more complete view of the information possessed by the Bureau. Users can presently search up to 560 million pages of international terrorism-related documents and billions of structured records, such as addresses and phone numbers, in seconds. They can also rapidly search for pictures of known terrorists and match or compare the pictures with other individuals in minutes rather than days. Coupled with sophisticated state-of-the-art search tools, the IDW enhances governmental ability to identify relationships across cases quickly and easily.

It is a simple fact of contemporary life that the current security environment presents unique and difficult issues that few of us have trained for. Even leaving aside the complexities of stabilization and reconstruction, addressing the direct threat requires the expertise and technological capabilities of law enforcement agencies, both in the conflict arena and at great distances, in order to terminate or restrict support to terrorism. Moreover, the effective utilization of law enforcement capabilities requires the cooperation of networks of not only law enforcement organizations but also military organizations across the globe. **JFQ**

NOTES

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

[2] A more complete explanation of the utility of fingerprinting in the war on terror can be found in Paul J. Shannon, "Fingerprints and the War on Terror: An FBI Perspective," *Joint Force Quarterly* 43 (4th Quarter, October 2006), 76–82.

[3] Federal Bureau of Investigation (FBI) Web site, International Operations, available at <www.fbi.gov/aboutus/transformation/international.htm>.

[4] FBI Web site, Headline Archives, "Protecting America from Terrorist Attack: War Zones link to FBI's Fingerprint Database," available at <www.fbi.gov/page2/june05/iafis062705.htm>.

[5] Robert S. Mueller III, FBI Director, before the House of Representatives Committee on Appropriations, Subcommittee on Science, State, Justice, and Commerce, September 14, 2005.

[6] Ibid.

[7] CBS News, "Forensics ID Bomb Makers in Iraq: FBI Uses Breakthrough Forensics to Track Homemade Bombs," January 17, 2006, available at <www.cbsnews.com/stories/2006/01/17/evening-news/printable1216945.shtml>.

[8] FBI Web site, Headline Archive, "What's New in the FBI? A Five-Year Accounting," September 15, 2006, available at <www.fbi.gov/page2/september06/testimony091406.htm>.

[9] Alexandre Deslongchamps, "Canadian Financing for Terrorism Triples to C$180 Million," Bloomberg, November 4, 2005.

[10] The ruling is the first to hold American organizations responsible for damages for terrorist acts committed overseas and opens a new window for the use of civil suits to stop the flow of funds to terrorist organizations. Whether the ruling is a watershed or an aberration that opens the door to frivolous law suits is yet to be seen. See Hilary Leila Krieger, "U.S. charity found liable for Hamas attack," *Chicago Tribune*, November 14, 2004. Additionally, the Holy Land Foundation has since been dismantled and officers of the organization are under indictment for material support to terrorism.

[11] Henry Crumpton, the U.S. State Department's counterterrorism coordinator, stated that at least US$150 million in terrorism funding has been intercepted worldwide, and millions more—in cash or other resources—has been stopped in transit or at borders. See Susanna Loof, "Battling terrorist financing helps map terrorist networks, experts say," Associated Press, November 9, 2005.

[12] Dana A. Shea, "Terrorism: Background on Chemical, Biological, and Toxin Weapons and Options for Lessening Their Impact," Congressional Research Service, Order Code RL31669, December 1, 2004, available at <www.fas.org/irp/crs/RL31669.pdf>.

[13] Peter D. Zimmerman and Cheryl Loeb, *Dirty Bombs: The Threat Revisited*, Defense Horizons 52 (Washington, DC: National Defense University Press, January 2004), available at <www.ndu.edu/ctnsp/defense_horizons/DH38.pdf>.

[14] Statement by Donna Bucella, Director of the Terrorist Screening Center, March 15, 2006, available at <www.fbi.gov/page2/march06/tsc031506.htm>.

[15] Law enforcement officers are well aware that the items a person carries on him have significance to the person. It may be a phone number, a matchbook from his favorite bar, or the address of a girlfriend. All of this "pocket litter" tells a story about the person and his habits and will often lead to useful intelligence.

[16] When the United States invaded Afghanistan, it was agents of the FBI's New York field office who were the most knowledgeable about al Qaeda and who were able to provide information to military forces who were picking up people on the battlefield.