Using Biometrics to Achieve Identity Dominance in the Global War on Terrorism

John D. Woodward, Jr.

A FINGERPRINT match identified the 20th hijacker. In December 2001, U.S. military forces detained Mohamed Al Kahtani as an enemy combatant on the field of battle in Southwest Asia.[1] During repeated interrogations Kahtani denied being a combatant and offered an innocent explanation for his presence in the region. While Kahtani was in military custody, an FBI team fingerprinted him in much the same way law-enforcement officials routinely fingerprint criminal suspects in the United States. They took Kahtani's 10 "rolled" fingerprints; that is, one fingerprint of each digit recorded from nail to nail. This collection of biometric data eventually led U.S. investigators to believe Kahtani was the missing 20th hijacker in the terrorist attacks of 11 September 2001. The 9/11 Commission concluded that Kahtani was "[t]he operative likely intended to round out the team" for Flight 93, which crashed in Somerset County, Pennsylvania.[2]

Kahtani was identified because U.S. authorities matched the fingerprints taken from him in December 2001 to his fingerprints of 4 August 2001, when he arrived at Orlando International Airport on a Virgin Atlantic flight from London. During the immigration inspection at the airport, Kahtani, despite holding a valid U.S. visa, raised the suspicions of an alert immigration official. According to the 9/11 Commission, "Kahtani was denied entry by immigration officials because he had a one-way ticket and little money, could not speak English, and could not adequately explain what he intended to do in the United States."[3] He received a "voluntary departure," which, in practical terms, meant officials placed him on a flight and returned him to Dubai. As part of the voluntary departure process, officials took prints from his two index fingers.

Once U.S. authorities biometrically linked Kahtani, the detainee in December 2001, to Kahtani, the foreigner who tried to enter the United States in August 2001, they had a valuable lead to pursue for counterterrorism and homeland security purposes. The Kahtani match raised an intriguing possibility: Investigators knew Mohamed Atta had been in Florida in August 2001. Could Atta be linked to Kahtani? Based on their review of surveillance camera footage taken at the airport on 4 August 2001, investigators matched a license plate to a car rented by Atta. Other corroboration established that Atta was at the airport terminal at the time Kahtani's flight arrived. Of course, Kahtani never volunteered this information during his many military interrogations. He stuck to his cover story. The fingerprint match provided the necessary actionable intelligence.[4] As a result, a person the military encountered on a foreign field of battle was linked to a terrorist activity—the 9/11 attacks. This case study illustrates the importance of "identity dominance," which the U.S. military must embrace.

What is Identity Dominance?

Just as the U.S. military has established its superiority in other arts of war, now, working with other U.S. Government organizations, it must strive for identity dominance over terrorist and national-security threats who pose harm to American lives and interests. In the context of the Global War on Terrorism (GWOT), identity dominance means U.S. authorities could link an enemy combatant or similar national-security threat to his previously used identities and past activities, particularly as they relate to terrorism and other crimes.

The U.S. military needs to know whether a person encountered by a warfighter is a friend or foe. To do so, we need to answer the following questions: Has the person previously—

- Been arrested in the United States or other countries?
- Used aliases or fraudulent "official" documents?
- Been detained by U.S. or coalition forces?
- Been refused entry into the United States?
- Been linked to a terrorist activity?

• Had his fingerprints found on the remnants of an improvised explosive device (IED)?

• Been seen within a crowd committing terrorist acts?

To the extent the U.S. military is forced to rely solely on a purported name or on "official" documents provided by someone, answers to these questions remain elusive. We cannot reliably find the answers if we use only the name the person provides and his "official" documents. Foes, particularly terrorists, will provide aliases and will often have the necessary fraudulent documents to back them up. A terrorist will also have a cover story that explains his actions in seemingly harmless terms. Fortunately, biometric technologies, based on a person's physiological or behavioral traits, can indelibly link a person to an identity or event. Names can be changed and documents forged, but a biometric is much less susceptible to alteration and forgery. Moreover, although many people have the same or similar names and many documents look alike, a person's biometrics tend to be robust and distinctive.

Biometric Technology Support

To achieve identity dominance, the U.S. military must make maximum use of biometric information and the technologies that collect, process, store, and search data. The military must work in cooperation with other U.S. Government partners, most notably the FBI, the Department of Homeland Security, the Department of State, and the intelligence community. Cooperation must also extend to state and local law-enforcement officials, who serve on the front lines of homeland security, and to our international allies as well.

Identifying individuals. Biometric technologies take automated measurements of certain physiological or behavioral traits for purposes of human recognition. Human recognition consists of verification: Is this person who he claims to be? and identification: Who is this person? These technologies can search a biometric data-base to verify a person's identity by doing a one-on-one match: Does this needle match that needle? And they can identify a person by doing a one-to-many search: Is this needle in any haystacks? This identification capability is critical for identity dominance because finding terrorists is like finding a needle in the midst of many haystacks.

Thanks to advances in computer technologies, pattern recognition, and algorithm development, some biometrics can search through large databases reliably and quickly. For example, the FBI's Integrated Automated Fingerprint Identification System (IAFIS), established in 1999, contains in an electronic database the 10 rolled fingerprint records of approximately 48 million individuals who have been arrested in the United States on felony or serious misdemeanor charges. When police make an arrest, they routinely submit the arrestee's fingerprints to IAFIS to determine if the person has a prior criminal record. The FBI processes an average of 25,000 such criminal identification submissions daily. Over 95 percent of the time, the search result is returned to the police in less than 2 hours.

Just as fingerprints can be found at crime scenes, fingerprints can be found at terrorist sites. Forensic examiners can harvest these latent prints and search them against the IAFIS database and its counterparts. Because a latent fingerprint contains much less data than a set of 10 rolled fingerprints, the system returns a candidate list of possible matches as opposed to a firm, highly reliable, match/no match result. A latent fingerprint examiner must then review the list for a final determination.

The IAFIS experience is instructive for the Department of Defense (DOD). Just as domestic law enforcement takes 10 rolled fingerprints (and other biometrics) from arrestees, U.S. military units must take 10 rolled fingerprints (and other biometrics) from Red Force members (enemy combatants and national security threats). Just as IAFIS stores arrestees' fingerprints in an interoperable format, DOD must store Red Force biometric data. Just as law-enforcement officials routinely search arrestees' fingerprints against IAFIS, so too must DOD routinely search Red Force members' fingerprints (and other biometric information) against all relevant databases to find the terrorist "needle."

The military needs reliable answers to several questions to enable it to identify people who are or might be national security threats. To get such reliable answers regarding previously used names and past activities, the U.S. military, working with other U.S. Government organizations and allied governments, must fully leverage the power of biometrics to ensure identity dominance. In doing so, some important and related functions would be served:

• Force protection—keeping U.S. and coalition personnel safer.

• Actionable intelligence—gaining information to use to detect, detain, disrupt, and deter terrorists.

• Law enforcement—recording legally admissible evidence to use to prosecute terrorists through the judicial system, if that path is pursued.

• Homeland security—safeguarding Americans and the Nation.

Emerging foes. The U.S. military has always faced the challenge of identifying friend or foe. In the GWOT, this challenge is all the more difficult

because we face a highly mobile, elusive enemy who deliberately engages in tactics to conceal his true affiliation and allegiance. Terrorists use aliases to hide who they really are, and they have fraudulent official documents to support their claimed identities. Assistant Secretary of Defense for Homeland Security Paul McHale explains: "Our enemy today is no longer in uniform, our enemy today is no longer in combat formation. Our enemy is probably wearing civilian clothes and is virtually indistinguishable from innocent counterparts throughout civilian society."[5]

The mobility of terrorists poses a serious challenge for the United States and its allies. Terrorists have demonstrated they can enter Western countries, blend into society, and remain elusive. They take advantage of our free and open societies to plot and carry out operations intended to destroy our countries. The 9/11 plotters planned and supported their attacks from the United States, Germany, Spain, Malaysia, Saudi Arabia, and other free countries.

Ensuring Identity Dominance

How can we better identify and target this elusive enemy? The Defense Science Board Task Force on Identification Technologies recently advised Secretary of Defense Donald Rumsfeld that "the [GWOT] cannot be won without a 'Manhattan Project'-like tagging, tracking, and locating" program for national security threats.[6] A critical component for identifying national security threats is for the U.S. military to process biometric data taken from Red Force members using the Automated Biometric Identification System (ABIS), an interoperable enterprise approach modeled after and interoperable with the FBI's highly successful IAFIS.[7] This approach is multitheater, multiservice, multifunctional, and multibiometric.

Multitheater. The ABIS capability must reach across all theaters of operation for the U.S. military and international allies. Biometric data must be taken to standards that ensure interoperability so biometric data collected in any theater of operation can be searched against all relevant databases for possible matches.

Multiservice. DOD cannot afford to permit each military service to do its own thing with respect to biometric data. For example, U.S. Army troops in Najaf should take biometric data from Red Force members and forward it to the central ABIS database; Navy units performing maritime interception operations in the Persian Gulf or U.S. Marines patrolling in Fallujah could later access and search the same biometric data.

Multifunctional. The ABIS approach serves multiple functions, which means U.S. military forces can gather biometric data for use by a Department of Homeland Security inspector at a port of entry for foreigners visiting the United States, by a Department of State diplomat issuing visas, or by law-enforcement personnel carrying out arrests. Because it contains biometric data taken from Red Force members, the ABIS is a true national resource for homeland security purposes.

Multibiometric. The ABIS approach must include multiple biometric records or modalities, such as fingerprints; mug shots (face); DNA; and iris, voice, and palm prints. DOD's immediate focus must be on fingerprints as the essential modality for an identity-dominance capability. (See figure 1.) Several factors account for this focus on fingerprints:

- Established biometric. Since the late 19th century, fingerprints have been recognized as distinctive, ubiquitous, and robust. Nearly everyone has fingerprints, fingerprints do not change over time, and the legal system has long accepted fingerprints

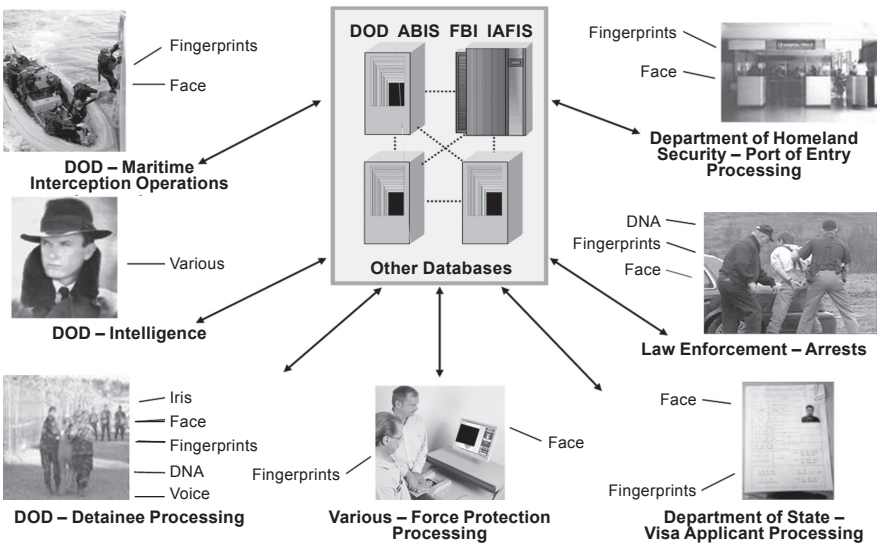

Figure 1. Identity dominance.

as evidence of identity.

• Established technology. Since 1999, searching and matching fingerprint data has become a highly accurate, automated process based on a standard that ensures interoperability. The keystone to this process is the FBI's IAFIS.

• Established databases. There are already many fingerprint databases. IAFIS, with its computerized records on approximately 48 million people, is the leading example. Many states have their own fingerprint databases. Moreover, many foreign countries have national fingerprint databases.

• Established benefits. Fingerprints might be left behind at criminal or terrorist sites. Forensic investigators routinely harvest latent fingerprints from such sites, which are subsequently searched against databases for possible matches.[8]

While face-recognition technology does not perform as well as fingerprint technology, it is improving and can be used as a valuable screening mechanism. With state of the art surveillance cameras, we can capture an image of a person's face clandestinely and from a distance. As with fingerprints, there are many legacy databases of mug shots, which are routinely taken during the police booking process and used for many other forms of vetting, such as visa applications.

Other biometric modalities, such as iris images, palm prints, and voiceprints, should also be incorporated into the ABIS approach. Doing so would improve and expand our identity-dominance capability by allowing our allies and us to search multiple biometric modalities on suspected national security threats.

A multimodal approach maximizes the use of biometric data, but identity dominance requires a single, virtual database in the form of a network of interoperable databases. For example, the IAFIS and ABIS databases must be interoperable. This seamless approach would make any standard query from another entity transparent. That is, it would be forwarded to the portal of the national security database and then searched among all relevant databases. The response would be returned to the user in a similarly transparent fashion. (See figure 2.)

Enhancing Identity Dominance

To enhance its identity dominance capability, DOD must take immediate steps in four critical areas: standards, policy, operations, and architecture.

Standards. First and foremost, military units processing Red Force members must collect fingerprints in the correct internationally accepted format—the 10 rolled fingerprints. Fingerprints taken in this way are interoperable with other fingerprint databases, such as ABIS and IAFIS. In February 2004, the DOD chief information officer mandated that DOD organizations conform to the Electronic Fingerprint Transmission Specification (EFTS) derived from American National Standards Institute/National Institute of Standards and Technology, ITL 1-2000.[9]

In response, Lieutenant General Steven Boutelle, the executive agent for biometrics, issued new standing operating procedures (SOPs) for biometric collection from detainees that requires collecting EFTS-compliant fingerprints, mug shots based on NIST best practices, and DNA samples from detainees. The SOP also encourages collecting iris patterns and voice recordings from Red Force members. My hope is that we can expand this biometric collection in the future. The military should also collect additional modalities such as palm prints and voice recordings from Red Force members.

Policy. Thanks to McHale's leadership, DOD has a policy in place to permit routine sharing of Red Force biometric data with the FBI. This policy needs to be broadly applied to permit other organizations to submit searches to ABIS. For example, federal, state, and local law-enforcement officials submit approximately 25,000 criminal search requests per day to IAFIS. These front-line responders should be able to search the fingerprints of criminal arrestees against ABIS.

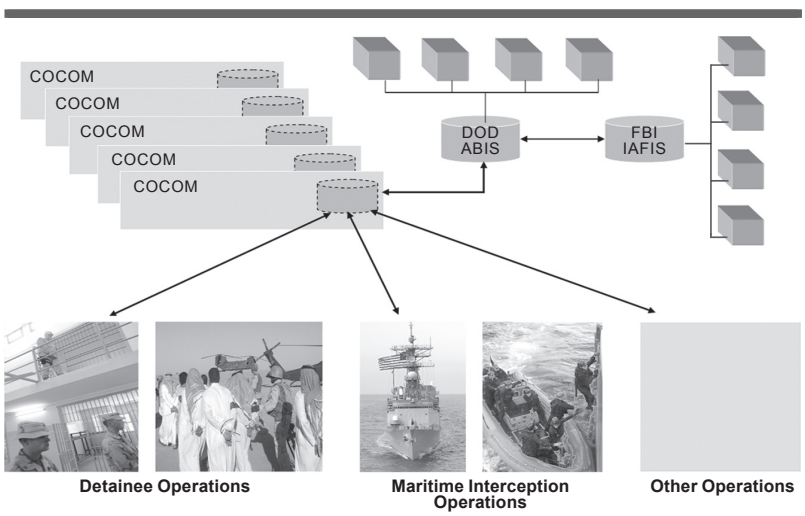

Figure 2. Conceptual DOD ABIS architecture.

DOD policy must also encourage military units to collect biometric data from foreigners who access U.S. installations in places like Iraq or who interact with U.S. forces. In this way these foreigners, known as Grey Force, can be better vetted as security risks. Similarly, DOD policy must enable military services, like the Navy, to collect biometric data from foreign seafarers stopped in international waters as part of maritime interception operations. This data could then be rapidly searched against ABIS, IAFIS, and related databases for matches. Ideally, the Navy's biometric capability also would be integrated into a U.S. Coast Guard biometric capability.

As an urgent priority, DOD also needs a policy to ensure effective use of biometric data it collects from Red Force members. Specifically, the military should not release a detainee from custody until the detainee's fingerprints have been searched with negative results against ABIS (to identify recidivists or match fingerprints left at a terrorist scene) and IAFIS (to identify someone who has a U.S. arrest record). In this way, the military could show that it recorded the detainee's fingerprints to FBI standards and received the results of a search (negative ABIS; negative IAFIS). Thus, DOD would ensure it has a good set of fingerprints before releasing a detainee from custody. This approach will also quickly identify detention centers in places like Iraq and Afghanistan that have not been upgraded with proper equipment and/or training. If a police department in the United States did not take fingerprints of arrestees, it would be committing a dereliction of duty. There is a lesson in this for DOD.

Operations. The military must exploit biometric data left behind on IEDs and in terrorist safe houses and other terrorist sites. The military should use both U.S. and foreign forensic investigators to harvest latent fingerprints found at terrorist scenes and routinely search latent prints against ABIS and IAFIS for possible matches, indicating, for example, that the same person was involved in multiple IED bombings. Such pattern analysis would provide useful intelligence.

Architecture. In 2004, the DOD Biometrics Fusion Center, with the support of the U.S. Northern Command, the Army Chief Information Officer/G6, DOD leaders, and other organizations, established the DOD ABIS, which is interoperable with IAFIS. DOD has a state-of-the-art system in place to process biometric data. DOD now needs to improve ABIS to push its capabilities closer to the warfighter, which would mean DOD must encourage development of rugged, lightweight, portable biometric-collection devices that can capture and transmit biometric data for rapid searching. The next generation of devices must also be fairly easy to use. As recent experience in Iraq demonstrates, it is extremely difficult for the military to provide extensive training during hostilities. Therefore, the devices must be intuitive and reliable.

The Future

In the GWOT, the relevance of biometric technology has grown exponentially. The military must achieve identity dominance, where military forces have the distinct ability to separate friend from foe by linking people to their previous identities and past terrorist or criminal activities. We can use biometric technology to achieve identity dominance and must deploy it to meet the requirements of force protection, actionable intelligence, and law enforcement. Establishing identity dominance through a comprehensive ABIS will enable the U.S. military to identify friend or foe to keep America safer. ***MR***

NOTES

1. Mohamed Al Kahtani is also spelled Muhammad Al Qahtani.
2. *The 9/11 Commission Report, The Final Report of the National Commission on Terrorist Attacks upon the United States* (Washington, DC: U.S. Government Printing Office, 2004), 11, on-line at <www.9-11commission.gov/report/911Report.pdf>, accessed 26 August 2005.
3. Ibid., 248.
4. For more information on the Al Kahtani case, see Tim Golden and Don Van Natta, Jr., "The Reach of War; U.S. Said to Overstate Value of Guantánamo Detainees," *New York Times*, 21 June 2004, A1.
5. Paul McHale, Assistant Secretary of Defense for Homeland Defense, "Homeland Security Defense: An Update," 4th Global Homeland Security Conference and Expo: Protecting the Nation's Critical Infrastructure and Key Assets, E.J. Krause and Associates and Deloitte Consulting Conference, Bethesda, Maryland, 23 November 2004.
6. Melana Zyla Vickers, "Going on a Manhunt: Do We Have the Technology to Win?" On-line at <www2.techcentralstation.com/1051/printer.jsp?CID=1051-102404B>, accessed 25 August 2005. For information on the Defense Science Board Task Force on Identification Technologies, see *Federal Register,* on-line via GPO Access, at <http://cryptome.quintessenz.org/mirror/dsb101504.txt>, 15 October 2004, accessed 26 August 2005.
7. For more information on ABIS, see John D. Woodward, Jr., "Another View: Who Goes There? Biometrics Can Make Positive ID," *Government Computer News*, 5 July 2004.
8. Peter T. Higgins, "Fingerprints and Hand Geometry," in *Biometrics: Identity Assurance in the Information Age* (2003): chap. 3; Colin Beavan, *Fingerprints: The Origins of Crime Detection and the Murder Case that Launched Forensic Science* (New York: Hyperion, 2001).
9. U.S. Department of Defense Chief Information Officer Memorandum, "Department of Defense Compliance with the Internationally Accepted Standard for Electronic Transmission and Storage of Fingerprint Data from 'Red Force' Personnel," Washington, D.C., 2 February 2004.

John D. Woodward, Jr., is Associate Director of the RAND Corporation's Intelligence Policy Center and is the former Director of the U.S. Department of Defense Biometrics Management Office. Before joining the RAND Corporation in 2000, he served as an Operations Officer for the CIA. He received a B.S. from the Wharton School, University of Pennsylvania, an M.S. from the London School of Economics, and a J.D. from the Georgetown University Law Center.