CHAPTER ONE

Introduction

Background

Biometrics have assumed an increasing role in the Department of Defense's (DoD) operations over the last ten years after being initially deployed in Iraq to help manage detainees. Part of the reason for this increased role lies in the changed nature of today's wars. In historical combat and in accordance with the Laws of Armed Conflict, soldiers were easily identified because they wore uniforms or bore other easily distinguished markings.[1] Their exact identities were secondary: The uniform said everything about how they could be treated on the battlefield and thereafter. However, the United States faced foes in Vietnam, after the terrorist attacks of September 11, 2001, and during two subsequent wars in Afghanistan and Iraq who did not wear uniforms; indeed, their *modus operandi* was to blend in with the population as much as possible. This tactic poses difficulties for U.S. forces to determine who they are encountering, e.g., has a person been encountered previously and characterized as potentially hostile? Equally important was the need to know whether a person was associated (in time or location) with other hostile events or "bad actors." Biometrics provided a way to achieve a previously unavailable degree of certainty about a person's identity, record of previous encounters, and connections to other people and events.

In addition to the military's need to accurately identify a large number of people, biometric technology has also improved enough to enable greater use. Rapid advances in acquiring, processing, transmitting, and storing information now allow military forces to ascertain, *within minutes*, whether someone they encounter has been encountered before—and do so for tens of thousands of people a day.

[1] See, e.g., Article 4, Convention (III) Relative to the Treatment of Prisoners of War, Geneva, August 12, 1949.

Role of Biometrics

Use of biometrics is founded on the observation that certain characteristics of individuals differentiate one person from another in a way that is stable over time. Collecting these biometrics at two points in time can, ideally, establish whether a person encountered today is the same person encountered at some point in the past—and is no one else. The more popular biometrics include fingerprints, facial images, irises, and DNA, although there are many other biometrics in use or mooted for use.[2] The desirable qualities of a biometric include distinguishability, stability over time and circumstance, ease of collection, ease of processing (both by humans and computers), universal acquisition (everyone can generate one), deep archives, and forensic capabilities. Each biometric modality has limits in terms of one or more of these ideal qualities.

Fingerprints are one of the oldest biometric modalities in widespread use, with the most robust technical and analytical infrastructure for their use. No two individuals have the same fingerprints, and fingerprints remain the same over an individual's life, barring scarring or disease, which allows for matching fingerprints taken at different times. Fingerprints have the added feature of being frequently left behind at crime scenes (in the form of a latent fingerprint), allowing investigators to determine with a greater or lesser degree of reliability that a specific individual touched an item or visited a location at some point in the past.

Fingerprints have high distinguishability and stability, useful forensic properties, are easy to computer-process, and are deeply archived, but they must be collected through direct contact by trained personnel to ensure readable prints. A small percentage of the population lacks well-defined fingerprints as well. Irises have better distinguishability and believed stability, and are easy to process, but not that easy to collect; archives of iris images are still small, and no one leaves them behind at the scene of a crime. Facial images have the advantages of easy (even surreptitious) collection, the most widespread archives (more so than fingerprints), and universal possession. They can also be processed by humans to some extent, but the technology to distinguish one face from another (when the sample is very large) is still evolving and, again, they are never left behind, except for images captured by surveillance cameras with varying degrees of clarity. DNA is distinguishable, highly stable, universal, is often left behind at the scene of the crime (sometimes when fingerprints are not), and can be easily processed by computer but not at all by humans. However, collection requires proper training because DNA degrades at different rates depending on environmental conditions and can be easily contaminated.

Because no biometric is perfect, collecting multiple biometric modalities, sometimes in concert with biographic information, can increase the probability of a match and reduce the risk of an incorrect match. Multimodal collection when an individual is fully "enrolled" in a biometric database can also subsequently provide the means for different verification measures. For example, if a person is added to a biometric database using only an iris scan, there is no

[2] Special mention should be made of signatures and speaker recognition (previously referred to as "voiceprints"). Neither provides particular differentiation power nor stability over time and circumstance, but each has a unique role. The signature, as a biometric, can only be collected voluntarily and thus connotes assent to collection. Speaker recognition may be the only biometric that can be collected in some circumstances.

possibility of later matching that person's fingerprints discovered in another location. DoD's handheld biometrics collection device, for example, is made to collect fingerprints, irises, and facial images (but not DNA).

Uses of biometrics generally can be divided into two categories: verification and identification. Biometrics can be used to verify the identity of friendly forces, known as blue forces, and third-party foreign nationals, known as gray forces, for purposes of facility access and other actions.[3] To use an oft-repeated example, a person asserts that he has a right to enter federal property, and passes an identification card forward that has his picture (a biometric). The guard examines the credentials to link authentication with name (establishing that someone with that name and face is in the database), and the picture so that it may be compared with the face of the person holding the credential. In more secure locations, a person may present a fingerprint (or a palm print) so as to validate, with higher degrees of accuracy, that the presenter is who he or she claims to be. The DoD's Common Access Card (CAC) has an embedded biometric, a fingerprint, but facilities and computer access devices that read this biometric as a condition of access are the exception, not the rule.

Biometrics are also used to identify enemy forces, known as red forces, by matching information to previously collected data or through forensic work.

A canonical vignette illustrating the former would be when U.S. forces detain an individual in Afghanistan, collect his biometrics, and learn he is on the watch list, known as the Biometrically-Enabled Watchlist (BEWL). A common example from the wartime environment of forensic identification is retrieving a latent fingerprint from an improvised explosive device (IED) and matching it to an individual who is detained for other reasons. It is important to note that these categories of uses are general. For example, the identities of red forces may be verified for purposes of detainee management and movement. Further, gray forces may go through an identification process to ensure a person has not been previously characterized as hostile. As will be explained in greater detail below, blue-force biometrics remains a limited line of work for DoD, so this report focuses on red- and gray-force biometrics.

Biometrics are only potential enablers in the process of characterizing and validating an individual's identity, i.e., ascertaining that a person is who he says he is (blue biometrics) or accurately identifying someone as hostile (red biometrics). This broader context is sometimes referred to as identity operations, or identity management. Identity management, at some level, is carried out by all organizations as a necessary part of determining who merits what privileges. The process of authenticating and identifying people, depending on context, can take many forms—humans, after all, have been doing it since well before the first fingerprint was collected. For instance, computer network authentication may include a token (something you have, such as a CAC), a password (something you know), and biometrics (something you are). In other circumstances, people can be authenticated by networks of trust, e.g., personal

[3] For purposes of this report, blue forces are considered U.S. personnel and allied personnel authorized to enter U.S. or international coalition facilities. Gray forces are local nationals or other foreign nationals who have not been characterized as friendly or enemy, or who are allowed access to certain areas of U.S. or international facilities, but with fewer privileges.

knowledge of an individual's identity based on prior contact, biographical detail, and patterns of behavior. Although our study may contribute to an understanding of identity operations and related issues, we are not examining identity operations writ large.

Modern biometric technology, including that used by DoD, has allowed the process of collecting, storing, and analyzing data to be faster and increasingly automated. The collection device creates a digital image and/or representation of the physical characteristic. The biometric data are transmitted to a database where computer algorithms seek a match to existing records. Depending on the quality of the data collected and the size of the database, this automated attempt may result in several possible matches that are analyzed manually to make a final determination. The newly collected data are stored in the database and the match/no match result is sent to a person who can use the information. Ideally this happens quickly and includes the person who collected the data (who may still be with the person whose data were collected).

An example of this process begins with a person who has been arrested. His fingerprints are collected and transmitted to the Federal Bureau of Investigation's (FBI) national database, where they are successfully matched with fingerprints in a prior criminal record (perhaps from another state). The result is communicated back to the law enforcement agency, which can then decide whether to take additional action against the individual arrested.

The various components (relating both to people and technology) involved in this process ultimately determine the quality of the data collected, the speed of data transmission, whether the data can be analyzed automatically and compared to other data, and the accuracy of the analysis.

DoD Biometrics Program Documentation and the Executive Agent

Since a 2000 DoD memorandum designated the Secretary of the Army (SECARMY) as the Executive Agent (EA) for DoD Biometrics, DoD has sought coordinated deployment of biometric technology among its components.[4] The initiation of a formal DoD Biometrics program occurred as advancements in computing technology supported aspirations of highly integrated identification capability. However, beyond a goal of mass technology deployment, the aim of biometrics capability remained effectively undefined. A series of memos from 2003 to 2005 reveal early variability in goals regarding the biometrics program. In 2003, DoD designated the DoD Biometrics Program an Acquisition Category (ACAT) 1AM in an attempt to elevate the role of biometrics.[5] Shortly after that, in 2004, DoD repealed this designation noting a lack of progress, and conceding a need for a more coherent framework in which to

[4] Rudy de Leon, Deputy Secretary of Defense, "Executive Agent for the Department of Defense (DoD) Biometrics Project," memorandum, Washington, D.C., December 27, 2000.

[5] John Stenbit, Pentagon Chief Information Officer, "Designation of Biometrics as ACAT 1AM," memorandum, Washington, D.C., May 15, 2003.

deploy biometric technology; this memo suggests such capability should support an identity management vision, and describes the creation of a group that would develop it.[6] At the same time, troops deployed to Afghanistan and Iraq, as well as counterterrorism units, requested significantly different technological capabilities to complete their missions. Recognizing these urgent operational needs, DoD released a policy requiring biometric screening of individuals in Iraq for base access in 2005.[7] This static biometric collection and match requirement corresponded with another to collect biometric identifiers of the rapidly growing population of Iraqi detainees held by U.S. forces. These requirements and others like them clarified mission needs statements for biometric technology, albeit in very different forms than initially envisioned for mass identity management. In Iraq, biometric collection and matching efforts required electronic messages to traverse networks of different classification levels (Non-Classified Internet Protocol Router Network [NIPRNet] to Secret Internet Protocol Router Network [SIPRNet]). In Afghanistan—a very austere environment where troops regularly travel far from any Internet access—biometric collection devices must be "tactically" designed and oriented to take into account free movement of known terrorists or enemy combatants.

As DoD deployed biometric technology to support urgent warfighter requirements, the department worked to release documentation normally preceding development of such a largely utilized technology. In February 2008, DoD updated the Biometrics EA Directive to establish new roles and responsibilities. This document was followed shortly thereafter by the DoD release of the "Biometrics Enterprise Strategic Plan: 2008–2015," in August 2008, which recognizes the "dynamic" development of the newly named Biometric Enterprise.[8] It also focused the enterprise on the acquisition of technology geared toward "Red Biometrics" and efforts to thwart non-traditional adversaries.[9] The strategic plan's goals are provided in Appendix A.

The chronology of document development for the biometrics enterprise continued asynchronously. In April 2008, prior to releasing any identified, coordinated, and signed joint DoD technology requirements, DoD designated the DoD Biometrics Program as ACAT 1-Special Interest Program. Currently, no biometrics program of record (PoR) created by the EA exists for collection devices or for the authoritative database. U.S. Special Operations Command (SOCOM) has fielded a collection device under a PoR, and the Navy has a collection device PoR in development, known as the Identity Dominance System (IDS). All equipment currently deployed has been overwhelmingly supported by overseas contingency operations (OCO) funding.

[6] In 2004, Stenbit wrote, "To ensure that the mission needs and requirements for all IdM capabilities are adequately defined, an overarching vision must be developed. In memorandum of January 12, 2004, I established an Identity Management Senior Coordination Group (IdMSCG) as a DoD-wide focal point for policy, requirements, strategy, and oversight on physical and virtual IdM" (John Stenbit, "Development of an Identity Management (IdM) Vision for the Biometrics Program," memorandum, Washington, D.C., February 20, 2004b).

[7] Gordon England, Acting Deputy Secretary of Defense, "DoD Policy for Biometric Information for Access to U.S. Installations and Facilities in Iraq," memorandum, Washington, D.C., July 15, 2005.

[8] DoD, *Biometrics Enterprise Strategic Plan: 2008–2015*, August 27, 2008b.

[9] Use of biometrically based identification techniques is commonly divided into three categories: blue, gray, and red, each of which is described in more detail later in the document.

However, the era of large numbers of rapid acquisitions based on the Joint Urgent Operational Needs Statements (JUONS) and readily available OCO funding is coming to an end now that U.S. forces have left Iraq and are scheduled to leave Afghanistan after 2014. DoD must make difficult decisions about managing its biometrics "enterprise"—i.e., the collection of activities associated with biometrics collection and use—and the evolution of its biometrics capability.

Under the current official biometrics framework, DoD Directive (DoDD) 8521.01E, the EA is responsible for programming and budgeting for "sufficient resources to support common enterprise" aspects and coordinating "all component biometric requirements," among other things, while the DoD components are responsible for budgeting for their specific biometric needs.[10] In practice, through Acquisition Decision Memoranda (ADM), and based on other guidance, the Army has taken on roles in biometrics that go beyond DoDD 8521.01E. The Secretary of the Army was originally designated EA to "lead, consolidate, and coordinate all biometrics information assurance [IA] programs" of DoD by Public Law 106-246 before September 11, 2001, and the 2003 invasion of Iraq, when the context and reasoning for that designation was clearly different than today. Consequently, the changing budget and wartime environment prompted DoD to reexamine biometrics activities.

Study Purpose

In this context, the Principal Staff Assistant (PSA) for Biometrics within the Office of the Secretary of Defense (OSD) asked RAND to study the biometrics enterprise. Specifically, the PSA asked RAND to do the following:

- Assess the assignments and arrangements of the EA with respect to effectiveness and efficiency of meeting user needs as required by DoDD 8521.01E
- Provide a status report on the biometrics program for the Secretary of Defense, also as required by DoDD 8521.01E
- Provide the PSA with options and recommendations for the biometrics enterprise to help future planning and developing input for the Fiscal Year 2014 (FY14) Program Objective Memorandum (POM).

We understood "assignments and arrangements" to be all management decisions made by the EA himself and all management and programmatic activities carried out by the EA's components.

[10] DoD, "Department of Defense Biometrics," DoD Directive 8521.01E, February 21, 2008a, at paragraph 5.12.6 and 5.12.8.

How the Report Is Organized

Our report is organized into five chapters. The second chapter describes the study methodology and analytical framework we used. The third chapter assesses the assignments and arrangements of the EA, including the management structure and the functioning of the biometrics cycle. The fourth chapter provides the status report on the overall biometrics enterprise. The fifth chapter provides conclusions, options, and recommendations. The appendixes provide a summary of the Biometrics Enterprise Strategic Plan goal, the interview protocol, a discussion of metrics, and a list of references.