Bring a Big Gun to Your Next Knife Fight: A Biometrics Primer

Michael L Scheiern

In just six years, the Department of Defense (DoD) transformed biometrics, or, more appropriately, automated electronic biometric systems, from an advanced concept technology demonstration to a battlefield capability the Commander of US Central Command (General Abizaid) identified as "decisive" in The Long War on Terrorist Extremism (The Long War).[1] This impressive feat follows in the rich tradition of American technical innovation to provide Commanders with asymmetric, "game changing" tools that reshape military operations -- offering another "big gun" for the knife fights of The Long War.

As DoD redirects its focus beyond Iraq, an opportune moment exists to examine biometrics in light of "What have we learned to date?" and perhaps more importantly, "What is required to improve biometrics support for the full spectrum of military operations conducted by US forces?"

This primer provides a point of departure in addressing these questions through the theoretical and practical elements underpinning DoD's biometrics enterprise. The focus is primarily on socio-organizational issues; for though technology may be the catalyst, reshaping military operations is primarily a socio-organizational activity within DoD and with DoD's partners. The resulting recommendations help US forces avoid the excesses of Amara's Law; an observation by futurist Roy Amara that "we tend to overestimate the effect of a technology in the short run and underestimate the effect in the long run."[2] If that seems overstated, consider the following:

"We shape our tools, and thereafter our tools shape us."
Marshall McLuhan

AUTOMATED INFORMATION SYSTEMS WITH BIOMETRIC TEMPLATES AND INDEXES (BIOMETRICS)

Biometrics are reshaping military operations by enabling deployed forces to rapidly identify individuals and manage information pertaining to an individual. Biometrics leverage an unknown individual's physical features by translating them into electronic bits and bytes known as a biometric template. These electronic templates of faces, eyes and finger surfaces are linked with other data and accessed, updated, sorted, and shared to support a myriad of individual-oriented tasks.

A few of these tasks, like forensic investigation, make for popular television; meanwhile, the vast majority of all biometrics transactions conducted by US forces overseas are mundane and laborious administrative and security tasks that range from base access and security screening for local employees to managing detainees. In the future, these tasks may expand to included administering local employee personnel administration, contracting, and humanitarian aid

[1] General Abizaid's unpublished description of biometrics in staff briefings while Commander, US Central Command (CENTCOM).
[2] Roy Amara was a researcher, scientist ,and futurist. See: http://en.wikipedia.org/wiki/Roy_Amara

distribution. Their common features are: (1) the tasks are mundane and laborious with little press in most circles, and (2) the tasks are incredibly important to the sustained military operations overseas. Properly implemented, biometrics help military forces perform their tasks that help ensure honest persons receive the opportunities and assistance they deserve while denying criminals and terrorist extremists the anonymity to plan and conduct their illicit activities.

The DoD challenge is implementing biometrics across a myriad of tasks that integrate DoD activities both internal to DoD and with DoD partners. These challenges can be grouped into three inter-related areas:

1. Internally, improve DoD's enterprise-wide use, production and sharing of biometrics with the minimal standards necessary to *achieve* "network effects"
2. Externally, integrate DoD biometrics efforts with allies, alliances, and international non-governmental organization (NGO) efforts to *enhance* "network effects"
3. Overarching, update DoD assumptions related to biometrics, specifically: biometrics' strategic role in The Long War.

A suitable starting point for this discussion is appreciating that individual-oriented tasks predate current biometric technology by centuries.

INDIVIDUAL-ORIENTED TASKS

Forward-deployed militaries spend countless hours managing and interacting with a wide assortment of individuals encountered during the conduct of an operation; they include civilians, local officials, criminals, and enemy combatants who surrender, are captured, or operate in disguise. This is not a recent phenomenon; Publius Flavius Vegetius Renatus wrote of the importance of these matters in his third century treatise *De Re Militari* on Roman Legion doctrine and operations.[3]

Whether managing local workers, detaining terrorists and criminals, or distributing aid to the needy, these and a thousand other individual-oriented tasks are the antithesis of popular images of war and warriors. The tasks do not involve firing weapons or feats of valor. Poets denigrate the tasks as war's "long periods of boredom" to be endured for glorious "brief moments of sheer terror."[4] Yet operations in Iraq and Afghanistan remind us that: (1) literally thousands of US forces are forward-deployed at present performing these mundane and tedious tasks, and (2) the tasks are fundamental to overall success in nation-building, Small Wars, and the small scale contingencies (SSCs) most-frequently performed by US forces. Fielding the means to make these tasks more efficient and effective can have a significant affect on a forward-deployed force's overall capability to perform assigned missions.

---

[3] See: The Military Institutions of the Romans translated by Lieutenant John Clarke in 1767 at: http://www.pvv.ntnu.no/~madsb/home/war/vegetius/

[4] The full cliché is: "war consists of long periods of boredom, punctuated by brief moments of sheer terror." Its true origin is unknown, for the cliché is credited to many different literary and noted figures and professions.

Biometrics provide a more ***efficient and effective*** approach to conducting the mundane and tedious tasks of identifying individuals and managing individual-oriented information. Biometrics achieve these transactional efficiencies through the use of an individual's unique biometric template(s) to automate identity management, indexing individual-oriented information, and documenting transactions between individuals. Collectively termed "biometrics information" for the purposes of this primer, these advances transform unwieldy pen-and-paper processes to a modern, automated approach with greatly reduced reliance on the bilingual skills and the typing acumen of users, or weak identifiers like a person's name, an official-looking document of unknown origin or the word of a local official whose trustworthiness cannot be determined. This reduces the long-standing cultural, language, and literacy obstacles that US forces encounter when operating in foreign lands, and brings a standard, automated approach to processes inherently prone to user variance and errors that undermine effective sharing and reuse of the information.

Biometrics also help to eliminate data gaps and seams between organizations and activities separated by space (geography) and time. Many organizations require similar types of information on individuals, and benefit from the sharing and reuse of information instead of newly creating it each time a person is encountered. The enduring nature of a person's physical features make the biometric templates valid for years, if not decades, and the portability of the electronic—virtual—information makes it easy and inexpensive to store and share. This broad sharing and reuse of information generates significant savings in time, money and effort. Known as ***"network effects,"*** the resulting savings can be applied to other tasks to improve operational effectiveness at both the local and enterprise level.[5]

BETTER SPEARS

Specific to The Long War, US forces in Iraq and Afghanistan are demonstrating that biometrics provide militaries with an asymmetric advantage over those who combat them from the shadows without recognizable uniforms or the doctrinal military formations of a conventional army. Whether labeled terrorist extremist, insurgent or criminal, these enemies are modern versions of Mao Tse-Tung's guerrillas; exploiting anonymity and deception with the support of like-minded citizens to "move amongst the people as a fish swims in the sea."[6]

Biometrics provide a better spear to catch Mao's fish (i.e., the terrorist, insurgent and criminal). Biometrics use difficult to change physical features to permanently establish an individual's unique identity in an electronic format. The individual's biometrics information is readily linked with other information and easily shared with other officials to greatly improve the identification, tracking, and targeting of Mao's fish. For example, while officials at several different organizations may possess small pieces of information on a terrorist, biometrics help all the officials link their information together into a single, permanent file (dossier) to help identify relationships, track the individual's activities, and determine likely whereabouts. The portable nature of an electronic file also ensures current and future forces across a region or the globe are

[5] See: Carl Shapiro and Hal Varian, *Information Rules: A Strategic Guide to the Network Economy*, Harvard Press, 1998.
[6] See Mao Tse-tung's, *Aspects of China's Anti-Japanese Struggle* (1948)

armed with the knowledge of the individual's true identity, to include recommended actions for future encounters.

These advances make biometrics a very sharp spear for catching Mao's historically slippery fish; piercing the anonymity and deception they require to operate and complicating their freedom of movement. It is also a concept that resonates well with DoD's traditional approach of confronting opposing forces through direct action; thus, relatively well-understood and appreciated by US forces as reflected by the widespread use of biometrics in Iraq and Afghanistan for checkpoints, raids, and sensitive site exploitation. However, while these security-related tasks make for great anecdotes and success stories, these security tasks are ***NOT*** biometrics' most significant contribution to winning The Long War.

SEA CHANGE

Biometrics' far more important role is in ***helping change the sea (i.e., local populace) to be inhospitable of Mao's fish.*** Sea change is the long-term effect that Amara and McLuhan spoke of, and is perhaps best explained through the writings of the noted American strategic theorist Carl Builder. A decade ago he reminded us that ***real*** strategy focuses on end states using means that an enemy cannot effectively counter.[7]

> "The strategic flame is a metaphor for the grand idea that military power can sometimes be brought to bear most effectively and efficiently when it is applied directly toward a nation's highest purposes without first defeating enemy forces. It is an enduring idea latent in the age-old precept of seizing the enemy capital, but one which was often frustrated by the interposition of defending forces.
>
> "Arguably the most important military concept of the [Twenty-first Century], the idea of the strategic is a much bigger idea than the one that dominates our military institutions today—warriors being able to defeat other warriors of like kind. It is serving the Nation—more directly, effectively, and efficiently—not just testing new arms one against the other."

While noting it is sometimes necessary to apply military power directly against opposing military power to advance strategic aims, Builder also notes those times are rare and makes three observations useful today:

1. The Nation is invariably better served by a military that is as equally adept at helping as it is destroying,
2. The mid-20th century strategic idea that a military can be used for something more pertinent than defeating its counterpart has been pushed into the background, not by funding but by interest, and,
3. History tells us that strategic thinking requires perseverance because it takes time for institutional mainstreams to move and join the "discovered" innovative courses of thought.

[7] Bulder, Carl, "Keeping the Strategic Flame" in *Joint Forces Quarterly*, Winter 1996–97.

The Joint Staff shares Builder's views on strategy, defining The Long War as a strategic campaign to:

> "Preserve and promote the way of life of free and open societies based on the rule of law, defeat terrorist extremism as a threat to our way of life, and create a global environment inhospitable to terrorist extremists."[8]

Far beyond some public relations gimmick, this three-prong strategy to win The Long War is one part applying military power directly against terrorist extremists and two parts "preserving and promoting freedom," and "creating a global environment" inhospitable to Mao's fish. The DoD biometrics community has made great advances in equipping US forces with "better spears" to support the first prong. The time appears ripe to advance on the Joint Staff's other two strategic prongs by applying biometrics to help ameliorate the socio-economic conditions that breed and sustain most of Mao's fish.

Sea change involves the deft art of introducing key enabling technologies in ways that lead to profound social change over time. The use of fax machines by Soviet dissidents is a great example where a piece of mundane office technology played a critical, strategic role in helped foster a revolution.

While some terrorists are implacable, many current and would-be terrorists—and those who support them—are motivated by repugnant socio-economic conditions, like poverty, and the real or perceived inequities and persecution of those they identify with.[9] Applying the right technologies can precipitate local, sustainable socio-economic improvements and alternatives that undermine local residents' motivation to engage in or support terrorism. In essence, shifting the personal cost-benefit analysis of most residents so they prefer to spend their time, efforts and resources engaging in more socially-accepted activities.

Biometrics' micro-efficiencies help achieve these macro strategic effects. While it takes far more than just biometrics to change the seas, biometrics provide a basic element that is integral to modernizing individual-oriented commercial and government functions in developing countries.

Often taken for granted in the developed world, ***developing countries lack electronic identity management and automated data processing capabilities to support modern commercial and government functions***. As a result, many transactions among individuals incur abhorrent inefficiencies inherent with paper-based processes and the need for people to physically meet to assuredly exchange information. These inefficiencies are compounded at institutional levels where the lack of electronic records and automation make it extremely difficult to cost-effectively audit individual transactions, or aggregate information in useful ways that improve

---

[8] Joint Staff Strategic Plans and Policy Directorate (J-5), *"Fighting the Long War--Military Strategy for the War on Terrorism"*, Briefing of January 12, 2006.

[9] See See: Neumann, Peter (ed), Addressing the Causes of Terrorism, The International Summit On Democracy, Terrorism And Security, Club de Madrid, Madrid, Spain, 2005, at: http://summit.clubmadrid.org/, and Library of Congress's "Bibliography on Future Trends in Terrorism," 1997, at: http://www.loc.gov/rr/frd/pdf-files/Future_trends.pdf, and Club de Madrid's, "Addressing the Causes of Terrorism"

commercial and public administration functions; such as: regional planning, equitable distribution of goods and services, and accounting for funds vulnerable to fraud and misuse.

Biometrics provide developing countries an electronic identity management and automation approach to modernize and make efficient individual transactions, and enable businesses and local governments to automate and aggregate information in useful ways. Biometrics also help reduce cultural, language, and literacy barriers that often stymie workers in developing countries when they attempt to use office-automation software designed for use in developed country processes. Automated electronic biometrics templates make transactions faster and more accurate, increasing the number of transactions that can occur with fewer errors to speed the provision of services. Both individuals and communities benefit by spending less time and effort on existing activities, enabling entirely new activities to be undertaken that were a priori unsupportable. This makes biometrics an integral element of any strategy to create better economic opportunities and better local governance as a means to sow intolerance of Mao's fish.

DoD leadership and routine participation in nation building, humanitarian assistance, and disaster relief makes it one of the US's most important resources for bringing about modern economies and better governance in developing nations. While not explicitly DoD's "lane in the road," many developing nations lack the resources or institutional incentives to update their business and government functions in ways that potentially empower individuals and bring about greater equality and transparency in commercial and government transactions. Manmade and natural disasters have a way of precipitating both the internal impetus for change and making available the international resources to actually effect change in developing countries. The use of biometrics to reconstitute and stabilize these affected local communities fulfills Builder's urging that, "the Nation is invariably better served by a military that is as equally adept at helping as it is destroying" by making three tangible "sea changing" contributions:

1. Favorably influences the local population by making the conduct of the operation more efficient and effective,
2. Teaches the locally-affected communities, businesses, and government officials to use biometrics-based approaches for identity management and automated tasks, and,
3. Provides initial biometrics capabilities given that US forces routinely transfer some equipment to local officials as part of DoD's transition plan for concluding the operation.[10]

The pursuit of sea changing biometrics capabilities has yet to materialize within DoD, representing one of the greatest unrealized strategic means to advance towards victory in the Long War. DoD's biometrics investments to date are almost exclusively for developing, fielding and sustaining biometrics' as a security tool to help identify and target terrorist extremists.[11] While security is integral to any operation, this spear building focus echoes Builder's observation

[10] Working in conjunction with the US Department of State and their Iraqi counterparts, DoD is presently fielding a biometrics-based prisoner administrative management system to the Iraqi Correctional Service (ICS).

[11] The DoD Biometrics Task Force Director recently noted, "Almost 7,000 Biometric Automated Toolset (BAT) and Handheld Interagency Identity Detection Equipment (HIIDE) systems have been deployed in Iraq and Afghanistan." Dr. Myra Grey, *Defense Dept. 'Institutionalizing' Use of Biometrics*, NDIA, January 2009. Also see the Supplemental Global War on Terrorism Budget request justifications at: http://www.defenselink.mil/comptroller/defbudget/fy2009/index.html

that “US military institutions are overly focused on force-on-force capabilities,” leaving US forces ill-equipped for tasks related to “preserve and promote free and open societies based on the rule of law.” As a result, US forces lack the biometrics doctrine, TTPs, and tools to manage local employee administration, document contracts and commerce, public administration, or transition local authorities to modern, automated public administrative and security systems. This void in “helping” capabilities also arguably undermines US efforts along three fundamental dimensions:

1. Complicates tasks related to stabilization, reconstruction, and humanitarian assistance,
2. Denies US forces the “network effects” and resulting cost savings of an integrated effort with local officials, and,
3. Raises questions as to the veracity of US policy statements that US forces are present in the host nation for stabilization, reconstruction, or humanitarian assistance purposes.

The current DoD approach also leaves unaddressed the other strategic aim of “creating a global environment.” Many allies, alliances and NGOs are focused on stabilization, reconstruction, and humanitarian assistance operations. Their biometrics investments and agreements inevitably align with their interests, making it difficult to envision how these allies participate in burden sharing, interoperability, and exchange of biometrics information with US forces when the latter are solely equipped with biometrics to identify and target Mao's fish.

SOMETHING IS MISSING

DoD's history of success suggests some resource constraint must exist as a plausible reason why DoD has yet to pursue biometrics as part of a sea changing strategy to win The Long War. The manpower and material resources appear resident. DoD's Biometrics Community is talented and many of the needed technologies already exist; for example, DoD already employs multi-level security (MLS) interfaces and data mirroring architectures in other enterprises to automate electronic exchange of information between US forces and allies.[12] The information exchange standards and policies also do not appear overwhelming for much of the individual-oriented information is already collected by officials, and biometrics simply transition existing database indices and primary identifiers from a name or serial number to more-unique, biometric identifiers that eliminate the need to know or correctly type in an individual's name or serial number.

There are also external policy resources. Homeland Security Presidential Directive #12 (HSPD-12) establishes a common identification standard for US government employees while Federal Information Processing Standard #201 (FIPS-201) provides the accompanying technical implementation details. These policies confine themselves to addressing identification and do not delve into critical matters like managing the plethora of information related to an individual, but they provide suitable points of departure for developing broader international policies on interoperability and sharing of biometrics-related information.

---

[12] See: Boardman, Jill and Donald Shuey. Combined Enterprise Regional Information Exchange System (CENTRIXS); Supporting Coalition Warfare World-Wide, US Central Command: Tampa, FL, April, 2004 at: http://www.au.af.mil/au/awc/awcgate/ccrp/centrixs.pdf

UPDATING ASSUMPTIONS

The "missing element" appears to be an update to DoD assumptions on biometrics' broader applicability, and the importance of broadening biometrics support across the spectrum of military operations. Such deficiencies are not new to DoD or unique to biometrics. Consider what Amron Katz, a World War II veteran who helped found the National Reconnaissance Office (NRO), observed 55 years ago about American aerial reconnaissance in World War II. [13]

> "Now what about reconnaissance and World War II? Well, we did have a bunch of pretty smart people involved. If we examine the course of that war we find that we entered the war with a set of aircraft, a kind of training method, some doctrine, some dogma, some principles, some practice, some organization and some understanding or preconception of how reconnaissance was to be employed. Not a single one of those elements survived the war: neither equipment, nor practice, nor theory, nor principles, nor aircraft. It was found necessary to make changes during the course of the war.
>
> A careful examination of the reasons for this indicates that we ran into situations and opportunities which were not anticipated. I defer to those who wish to argue whether or not the real situations could have been anticipated. I argue simply that this collection of smart guys did not so anticipate them, and that, by and large, they were at least as clever, at least as imaginative, as we are today with respect to the future.
>
> …If everything [reconnaissance] we entered World War II with was changed, how and by whom? We learned during the war. People were fired, others were promoted. It was a time for proof by fire and shot: the problems were at hand, and those ideas that were poor were demonstrated so, and quickly."[14]

Replace "reconnaissance" with "biometrics" and Katz's words still ring true today. Prior to September 11, 2001, DoD considered biometrics primarily an internal management tool for personnel administration. physical access control to facilities, and logical access control for computers. In 2003, DoD's assumptions shifted and biometrics were "externalized" to automate identification and information management on individuals encountered by US forces performing security tasks like detainee management and background screening of local employees on US bases in Iraq. Eventually expanding to include checkpoints and raids, DoD's reactionary use of biometrics for security tasks was never envisioned to be the last, or even most appropriate, set of assumptions to mature its biometrics enterprise—they were simply the necessary and sufficient assumptions to meet the pressing security challenges of a liberated Iraq and Afghanistan.[15]

As operations in Iraq and Afghanistan have evolved, the limitations of DoD's earlier assumptions are increasingly apparent. The security-centric approach to biometrics is only partially addressing DoD's strategy for The Long War. Biometrics assumptions need updating to include-

---

[13] See: NRO press release: http://www.nro.gov/PressReleases/prs_rel40.html

[14] See: Amron Katz, *Some Ramblings and Musing on Tactical Reconnaissance*, RAND Corporation, March 1963.

[15] In April 2003, the author wrote the first operational requirement for biometrics systems to support CG, I MEF in Iraq.

-***perhaps emphasize***--tasks that “preserve and promote” freedom, and contribute to "a global environment” that is inhospitable to Mao's fish. These updates begin with coalescing consensus as to biometrics' force multiplier effects.

FORCE MULTIPLIER

US forces traditionally understand military capabilities and effects through the lens of the “force multiplier.” The DoD dictionary defines force multiplier as: A capability that, when added to and employed by a combat force, significantly increases the combat potential of that force and thus enhances the probability of successful mission accomplishment. This slightly updated version of “combat multiplier” recognizes that military forces do far more than engage in firefights. Biometrics' force multiplier effects are evident in three inter-related areas:

- Individual. Biometrics vastly improve individual task efficiency and effectiveness when and where US forces must identify, differentiate and engage an ***unknown*** individual encountered in the conduct of an operation. They help speed the individual's decision-making process by providing trusted knowledge garnered from others who previously encountered the individual, and applying automation to more rapidly execute assigned tasks and document the present encounter. Faster access to trusted information and better task execution frees the individual's time and attention to perform more tasks within a given timeframe.

- Command. Biometrics provide commanders a means to better perform stated and implied tasks, improve staff planning, and influence the local populace and enemy actions. The individual effects “scale up” to provide commanders with more effective and effective manpower when conducting operations. Aggregating biometrics information provides commanders with ***actionable*** information on the ***actual*** encountered populace, to include enemy combatants who are captured or killed in an area of operation (AO). This helps refine operational planning and execution of actions such as: information operations, intelligence analysis, logistics and refugee management. Biometrics’ identity management functions also deny anonymity to persons within an AO. Adjusting where and when biometrics are employed enables a commander to: (1) better align the distribution of goods, services and information, and (2) influence the movement decisions and activities of those in or may consider passing through his AO. These effects combined to enable commanders to make more effective use of existing resources to speed mission success.

- Indigenous Populations and Institutions (IPI). Biometrics provide the local populace with ***transaction efficiency*** and ***accuracy*** in obtaining and providing security, public administration, employment, commerce, and humanitarian assistance. Collective physical security is enhanced, and once enrolled, individual identities can be quickly verified and automated accounts accessed to speed commercial and government transactions, freeing time and attention to pursue other activities. Biometrics also help address operational problems that diminish community resources, such as: user errors, identity fraud, and misuse of resources. The more efficient use of community resources, time, and attention helps the local populace more quickly achieve a stable, prosperous

environment to reduce or eliminate the need for international presence—freeing military forces for other duties.

The key concept is: ***biometrics improve transaction efficiency for individual-oriented tasks*** while generating information on the encountered populace that aids planners, operators and administrators. Select biometrics modalities and operations also enable commanders and administrators to influence the actions of those in, or considering entry into, their AO.

Biometrics' force multiplier effects are most pronounced across the lower spectrum of conflict that includes Small Wars and most SSC scenarios. These military operations are oriented towards individuals and communities rather than large-scale combat involving major weapons system engagements.

The force multiplier effects appear less pronounced for ***past*** Major Theater Wars (MTWs) or SSCs where actions center on major weapons systems—i.e., a warplane—instead of individual encounters. For example, successfully execution of Operation Desert Storm did not require biometrics, nor did Operations Southern and Northern Watch: the no-fly zone enforcement over Iraq from 1991 to 2003. These operations centered on readily identifiable major weapons systems and combatants whose distinct identifiers make them ***known*** from non-combatants.[16]

FUTURE MAJOR THEATER WAR

An interesting case is Afghanistan. If Afghanistan is the harbinger of ***future*** MTWs, it suggests biometrics may provide significant force multiplier effects in other future MTWs as well.

The war in Afghanistan is a stark departure from 1990's era MTW images and assumptions. The Afghan battlefield is a mix of combatants and noncombatant civilians absent a display of recognizable uniforms or intent. The battlefields are not fixed pieces of terrain but rather a shifting mosaic of places and peoples where even "military" style clothing is made non-descript by combatants and non-combatants wearing "military" jackets, boots, and trousers for their availability, warmth, and comfort. Likewise, many of the enemy combatants are ad hoc, part-time opportunists whose belligerence ebbs and flows with seasons, family life, local economics and the arbitrary political decisions of their tribal leaders.

DoD's own operations also differ from long-held images and assumptions about MTW in important ways. The foremost difference is the tremendous number of ongoing reconstruction and humanitarian tasks by US forces and allies. While news headlines focus on actual combat operations, literally thousands of non-combat projects and activities are ongoing to reconstruct Afghanistan. Those involved would likely find biometrics far more applicable than armored tanks, jet fighters, and aircraft carriers to aiding accomplishment of their tasks.

DoD's uniformed ground combat force is largely comprised of traditional infantry battalions augmented by Special Forces, but they are not operating in the conventional "two up, one back" regimental formations of Operation Desert Storm. These "maneuver units operate in a

[16] Biometrics are still present in combat support activities (e.g., Forward Operating Base (FOB) security, port security, and contracting), and critical post-combat actions ensure postwar stability).

disaggregated fashion, with companies, platoons and even squads dispersed at distances beyond the normal range of mutually supporting organic direct fires, but linked through a command and control network and supported by precision standoff weapons." It seems the future may already be present in Afghanistan for this operating concept forms the basic premise of the Marine Corps' next generation operational concept ("Distributed Operations") and its recent update, "*Marine Corps Operations in Complex and Distributed Environments*."[17]

Even DoD's forward-deployed force composition is different as a result of augmentation by thousands of US-funded civilian contractors. These armed and unarmed civilian personnel perform traditional uniformed military functions that range from security escorts for convoys and high-ranking officials to operating dining halls on base.[18] The breadth and depth of this civilian integration into military operations is perhaps best reflected by 2007 mortality figures that reflect civilian contractors are 1 out of every 9 American deaths in Afghanistan—a higher mortality ratio than either the US Navy or the US Air Force incurs in Afghanistan.[19]

In Afghanistan, biometrics are providing the reliable means to rapidly identify and differentiate combatants from non-combatants based on previous contact with the individual, and separate ***legitimate*** allied civilian contractors from imposters or the enemy. As one Marine stated, "It's a mess sorting out who's who in the zoo," when contracted civilians are global sourced, possess modest English language skills, and may appear similar to local citizens in mannerism and dress.[20] Consider the challenge of identifying and differentiating armed civilian contractors from enemy combatants. "Civilian" contractors carry private weapons, drive privately owned vehicles (POVs), and occasionally engage in firefights—actual combat—with similarly armed and dressed enemy combatants. Biometrics help US forces confidently distinguish between the two when encountered them in the course of routine—non-firefight—situations.

Are biometrics' force multiplier effects equivalent to an additional infantry brigade or squadron of jet fighters? Such procurement arguments are rather vacuous at present given the nascent state of current DoD biometrics capabilities and the transformational nature of The Long War. It is possible though to start ***qualifying*** biometrics' force multiplier effects though an approach known as maturity modeling.

MATURITY MODELING

Biometrics systems operate at the confluence of three emerging technologies: (1) portable computing devices to rapidly collect biometric data, enter (update), and display information on an individual, (2) fast "one to many" search algorithms to locate and recall individual records using biometric templates, and (3) enterprise-wide, secure data networks (e.g., SIPRNet) to speed remote access and updates to non-local users and data repositories. Each technology area operates at different levels of technical maturity with its own arcane technical language, making

---

[17] See: Headquarters, US Marine Corps, *A Concept for Distributed Operations*, April 25, 2005.
[18] See: Brad Knickerbocker, Silent Surge in Contractor 'Armies', July 18, 2007 at www.globalpolicy.org.
[19] Exact records on civilian deaths are sketchy; however, by mid-2007 at least 80 contractors are known to have died in Afghanistan along with 600 Uniformed Military Personnel. See: Joseph Giordono, "Contractor casualties in war zones top 1,000," *Stars and Stripes*, Mideast edition, August 9, 2007.
[20] Quote is from a Marine to the author in 2004 while in Iraq. For an excellent treatment on the diversity of contractors, see Knickerbocker article.

it difficult for policymakers, commanders, and biometrics system users (i.e., laymen) to cross-compare technical advances, understand their operational implications, discuss alternatives, and write effective policies that fully leverage their advances.

These challenges are not unique to biometrics. DoD and key partners (e.g., Department of Homeland Security (DHS)) are currently addressing similar challenges using maturity models like the capability maturity model (CMM) developed by the Software Engineering Institute (SEI).[21] CMM is an engineering-based, best-practices model that ***qualifies*** product and process maturity for software-intensive processes using a standard, repeatable approach (framework) expressed in maturity levels ranging from Level I (Initial) through Level V (Optimizing). It is one of literally dozens of models that: (1) help integrate traditionally separate organizational functions, (2) set process improvement goals and priorities, (3) provide guidance for quality processes, and (4) provide a point of reference for appraising the current process.[22] Their use helps DoD institutionalize and mature biometrics capabilities through a common approach and language that service providers, developers, and acquisition specialists can agree upon. However, engineering-based maturity models like CMM have limitations that significantly undermine their utility for equating technical maturity with force multiplier effects.

Engineering-based maturity models provide a useful proxy measure of force multiplier effects ***only to the extent the stated requirements documents embody the force multiplier effects***. These models appear to work well for this function when the capabilities that have existed long enough for their force multiplier effects to be well-understood and well-reflected in applicable capabilities requirements documents, such as: cannons and rifles. This is less true for rapidly-emerging technology, like biometrics, where many of the envisioned force multiplier effects and innovative use cases have yet to be achieved on the battlefield, thus are only partially understood and partially represented in existing requirements documents.[23] Constrained to evaluation based on immature requirements documents, ***engineering-based maturity models significantly underestimate the force multiplier effects of emerging technology.***

An alternative approach is sequential "generation" modeling. This approach is less precise than engineering-based maturity models, but offers an advantage in providing an intuitive approach that is inclusive of future capabilities and innovative use cases not envisioned, and perhaps unknowable, at present. Generation modeling also appears to offer a superior means to expressing biometrics capabilities in ways that resonate within DoD's "spiral development" approach to warfighting capabilities, thus enabling biometrics to better compete for procurement, operations and maintenance funding within DoD. In the absence of a more-formally defined sequential generation model for DoD biometrics, the following is provided as a point of departure:

- First Generation Biometrics (Technology-centric). This is the exploratory phase where technology has advanced to a functional level where US forces start adopting biometrics for the ***potential*** applicability to their operational and business functions. Institutional

[21] See: Software Engineer Institute (SEI) at: http://www.sei.cmu.edu/cmmi/
[22] Ahern, Thomas, Clouse, Aaron; Turner, Richard (ed), CMMI Distilled: A Practical Introduction to Integrated Process Improvement, Addison Wesley Press, 2003.
[23] The author participated in writing DoD biometrics capabilities requirements documents from 2005 through 2007.

efforts focus on understanding and resolving the significant operational limitations and disparities that result from technical limitations, competition among modalities, and technical approaches to addressing operational tasks. Rapid industry growth and advances occur in each technology arena, to include the appearance of new modalities (e.g,. gait, thermal) and useful combinations of modalities, algorithms, and integrated data communications. Technical standards coalesce and systems emerge that facilitate tasks; however, the challenge of getting new technology to function overshadows the work of optimizing the systems to perform specific tasks. Specialized organizations (staffs) emerge to coordinate technical and policy developments, as well as provide advocacy, expertise, and continuity across time and organizational boundaries.

- Second Generation Biometrics (Task-centric). This is the application phase where the various technologies and approaches mature to the point that optimum modalities and approaches for each task are widely recognized and adopted. Institutions have dissected and reconstructed individual tasks incorporating the appropriate biometric modalities and information design to be efficient and effective. Institutions ***achieve*** the anticipated force multiplier effects and best practices are institutionalized to preserve performance gains. Specialized staffs remain, but their knowledge is diffused across the enterprise so the services, unified and specified Commands operate in synch to facilitate trans-regional operations.

- Third Generation Biometrics (Implicit Use). This is the exploitation phase where advances in technology enable individuals to be innovative with their tools in ways that ***surpass*** institutional designs to yield wholly new force-multiplier effects never envisioned by the institutions. Optimization efforts shift toward advancing and sustaining the ***individual's ability*** to tailor personal biometrics tools to address tasks of individual interest. Biometrics are so well integrated that distinctions between the biometrics and the tool are no longer useful—a condition known as "implicit use." Special staffs are no longer required for the services; unified and specified commands manage further developments through those with staff cognizance over tasks instead of biometrics.

Applying this framework, US forces are currently equipped with first generation biometrics systems and are working to achieve a second generation biometrics capability that might aptly be termed "Wikipedia in the field." Once in place, these second generation capabilities will enable DoD to address the third generation biometrics capabilities that Commanders are demanding for today's "knowledge intense" battlefields.

DoD is not alone in this effort to frame biometrics advances and contributions to operations. Beyond other government institutions, the private (commercial) sector is addressing many of the same biometrics challenges with an aggregate investment that far exceeds DoD's biometrics budget.[24] Ensuring DoD biometrics is compatible with commercial efforts helps DoD leverage commercial advances to support military operations. This leveraging goes far beyond purchasing commercial-off-the-shelf (COTS) hardware and software to include the underlying theory DoD applies to build its biometrics enterprise.

[24] See: BCC Research, The Global Biometrics Market, January 2007.

INDUSTRIALIZING DOD BIOMETRICS

Organizing human capital is often far more daunting than technical architectures, so a suitable industrial organizational framework is central to providing biometrics' leadership, developers, support personnel, and system users an intuitive understanding they can embrace to organize and prioritize their activities. Absent this industrial framework, technical advances lack context and DoD risks repeating the common historical mistake of assuming the best technology determines battlefield outcomes, as the French learned to their dismay when technically superior French tanks were quickly annihilated by better German tactics in World War II.

The human capital challenges revolve around achieving efficient, widespread local production and consumption (i.e., usage) of biometrics information with the minimal standards to deliver sufficing results. While the technology may be new, the nature of such problems is not. American industrialists faced, and largely resolved, similar challenges over the last century.

Everyone remembers that Henry Ford organized the first assembly lines to build automobiles. Forgotten are how lousy were the pre-Ford automobiles and the automobile industry as a whole. The pre-Ford auto industry was a morass of laissez-faire factories with unreliable parts and equally unreliable workers. The resulting automobiles were haphazardly produced and unreliable—at prices few could afford—despite the widespread demand for automated transportation.

The pre-biometrics era was a similar morass. For generations, on-scene commanders developed and managed data on individuals without a standard approach, and suffered the limitations of weak identifiers and even weaker identity management and information exchange systems. Their methods were invariably ad hoc, informal creations born of necessity that ebbed and flowed as forces and key personnel arrived and departed. Even the early promises of 1990's micro computing proved disappointing. Operations in Somalia and the Balkans revealed that unchecked user variance in interpreting and entering information on individuals undermined useful sharing of this information when large numbers of users were distributed across an AO.

Like Ford's assembly line, electronic biometric systems fostered a new era of coherence by integrating data from an individual's electronic biometric template with portability and networked data communications to “industrialize” the tactical commander's individual-oriented tasks. In 2003, detainee administrative management in Iraq was the first process subjected to this Fordist approach. Subsequent efforts included local employment programs and the vetting of government officials. While nascent and plagued with the problems of early adaption, these Fordist industrialization efforts eventually helped DoD mass produce and mass consume standard biometrics products to the benefit of US forces, allies and local citizens--everyone but Mao's fish.

While layers of military jargon obscure fundamentals, DoD's biometrics enterprise is foremost a Fordist industrial enterprise. Think of Fordism as an explicit approach to achieve implicit use by helping organize literally thousands of geographically-displaced, disparate users to contribute,

update, analyze and apply biometrics information in ways that are readily exchangeable. It is the organizing principle to achieving network effects.

Like any enterprise, focusing on the fundamentals is invariably the shortest path to success. Consider DoD's biometrics enterprise through Fordism's three tightly-coupled thrusts of mass consumption, mass production, and standards, starting with the "glue" that binds them: the standards.

STANDARDS

Technical and social standards are the conventions that make network effects possible by ensuring users displaced by geography, time, and function operate with sufficient consistency to leverage each other's efforts. DoD actively participates in many biometrics technical forums to ensure US forces deploy with equipment that meets technical standards for data inputs, outputs and processing.[25]

While these technical efforts are important, force multiplier effects are generated though the social standards that determine actual use of biometrics across a large, heterogeneous user base. These social standards appear as guidance to managers and those who use or contribute to biometrics information in order to ensure usage and eliminate minor variances in how data fields are used, and the actual data entered, that can effectively thwart later searches, sharing and reuse of the information. Where technical limitations exist, they are typically addressed through social standards. First generation biometrics systems are no exception for their lack of a robust technical means to resolve anomalous and unstructured data, and inability to collect some biometric modalities to technical standards under field conditions, requires social standards to achieve effective use.

The negative consequences of biometrics' technical limitations and inadequate social standards were evident early on in Iraq, when every tactical commander in 2003 and 2004 adopted local techniques and procedures in the absence of centrally managed guidance. Differences in local usage and local data entry procedures across Iraq created local pockets of data that were incompatible with other pockets of local data. Effective sharing and reuse of biometrics information was thwarted as adjacent and follow-on forces found it exceedingly difficult to use another's data to know who was previously encountered or the circumstances of the encounter. The network effects were not materializing to justify the expense and effort of biometrics.

Unable to fix the problem through technology, higher commands applied detailed social standards on usage and user data entry. These social standards achieved network effects in 2005 by detailing the minimum acceptable "When" and "Where" the systems are employed, as well as the "Who" is an acceptable operator and "How" the tasks are performed. While tedious, this biometrics guidance was not unprecedented. Tactical commanders encounter similarly detailed guidance for analogous processes, including procedures for communications material security and ordering spare parts. The major differences were the relatively recent appearance of

[25] DoD representatives are present on many of the National Institute of Standards and Technology (NIST) and its international technical standards working groups. There is even national registry of recommended biometrics standards available from NIST at: www.nist.gov or www.biometrics.gov.

biometrics social standards, and the broader, direct applicability of this largely administrative guidance to micro field tasks.

Time will resolve most issues related to biometrics' relative recent appearance. More daunting is the challenge of maintaining biometrics guidance with the appropriate breadth and depth of detail to achieve network effects without compromising a local commander's innovative use of biometrics as opportunities avail themselves. Biometrics unify operational and administrative tasks at the point where an individual is encountered. This introduces a significant administrative component to field tasks previously spared such concerns. For example, riflemen accustomed to firing weapons and squad-level tactics are now operating portable biometrics devices and entering detailed administrative information on encountered individuals according to equally-detailed guidance that was generated by some distant higher command. While technical advances will eventually reduce some of the administrative minutiae, there is no viable near-term alternative to these somewhat onerous user standards. This makes biometrics a “lightening rod” for spirited debate on the appropriate balance between force-wide standardization and the authority of intervening levels of command to employ their forces as they see fit.

The nascent state of DoD biometrics standards, policies and procedures at levels above the individual user does little to quell the debate. Rather than globally-coordinated policies emerging from the Joint Staff, every DoD specified, and unified command (CINC) is presently developing “regional” biometrics policies and guidance with modest cross-CINC coordination or consensus.

These divergent regional policies and procedures translate to divergence in the manning, training, and equipping of US and allied forces by region. This "regionalization" of biometrics inevitably undermines achieving global network effects, thwarts economies of scale, and compromises the ability of a globally-sourced Combined-Joint Task Force (CJTF) to rapidly assemble, organize, and employ biometrics in an expeditionary operation. It also undermines DoD's ability to effectively engage allies, alliances, NGOs, and other US government partners since it is unclear to these allies which set of DoD regional policies and procedures they should align with.

This appears to be a matter of interest. Decades ago the US and Western European militaries solved similar challenges on issues like weaponry, communications, and battlespace coordination. It took the threat of the Soviet Union to do so, but perhaps the global nature of terrorism and the Joint Staff's Long War strategic guidance is sufficient motivation for DoD to forge a "global biometrics environment" across the CINCs, Services, and as many allies, alliances and NGOs as possible. Focus on the following three areas would help:

- Tasks, not biometrics. Tactical tasks give biometrics relevance and are rather universal across the enterprise, commands, and tactical situations. Operations in Iraq and Afghanistan led the US Central Command (CENTCOM) and US Special Operations Command (SOCOM) to develop task-centric guidance and improve task coordination. Their guidance serves as a set of best practices which others can leverage and align their policies and investments.

- Non-Combat Rules Of Engagement (ROE). DoD has extensive experience in developing integrated combat rules of engagement while their natural complement—non-combat rules of engagement—remain disaggregated and disjointed. As a result, the differences in information management process from one non-combat activity to another ***greatly complicate achieving network effects across non-combat activities***. For example, DoD has developed and published detailed guidance for a number of non-combat tasks where biometrics are applicable, such as: civilian contracting, humanitarian aid distribution, and disaster relief. The information management policies within each area may represent a de facto set of best-practices within their respective domains, but absent an overarching effort to integrate and standardize common aspects of these information enterprises, it inevitably ensures variance will result that undermines sharing and reuse of information among these activities. Establishing a standard approach through non-combat ROE both helps US force interoperability and provides powerful assurances to allies, the media, and the affected community that US forces are committed to the helping aspects of military operations.

- Audits. The Fordist concept of statistical process controls (SPC) is essential to improving and maintaining data quality—a key enabler of network effects. Users must be able to trust that biometrics information is accurate and authoritative. This requires astute audits by quality control elements to help identify and fix sources of error and anomaly. The improvement(s) may be better policy, training, supervision, and/or technology; but without consistent auditing, it is extremely difficult for busy commanders and staff to correctly identify and diagnose process problems or develop appropriate preventive actions.

MASS PRODUCTION

Standards improve mass production efforts, and so it is no surprise that DoD's ***internal*** biometric mass production challenges are consistency in implementation of standards across a broad, disparate body of personnel who produce or otherwise contribute biometrics information. While detractors may argue otherwise, DoD has shown forward thinking coupled with action to improve biometrics production support through entrepreneurial efforts like the Joint Processing and Exploitation Center (JPEC) in Western Iraq.[26] Nonetheless, DoD's focus on security tasks has resulted in a lag in biometrics production support to reconstitution, stabilization and humanitarian assistance (helping) tasks. These tasks usually occur within the local communities and involve transfers of money or goods of value (i.e., incentives). As a result, those who perform these helping tasks in the local community invariable encounter Mao's fish and those who support them. Biometrically-enabling these tasks improves the efficiency of US forces helping local communities, and ensures such efforts do not unwittingly provide support to Mao's fish. Thus, improving DoD's internal production support to reconstruction, stabilization and humhelping tasks can actually benefit security tasks as well.

[26] See: Manson, John, The Joint Processing and Exploitation Center (JPEC) Lessons Learned report, MCCLL, 2008.

DoD's ***external*** mass production challenge is to integrate DoD's biometrics efforts with those of allies, alliances, NGOs and other US government agencies. Allies and alliances are aggressively pursuing biometrics integration efforts. For example, the United Nations High Commissioner for Refugees (UNHCR) is presently recording biometrics information and issuing identity cards to the estimated 2.5 million Afghan refugees living in Pakistan to facilitate their repatriation back into Afghanistan.[27] Similarly, the North Atlantic Treaty Organization (NATO) employs a biometrics-capable system to manage local employees at bases in the Balkans and Afghanistan.

As a member nation with common interests and forward-deployed forces operating in the proximity of each other, one might assume DoD has closely aligned its biometrics efforts with UN and NATO efforts. Such cooperation would seem natural given the mutual benefits of eliminating the data "stovepipes" and "pocketing" that undermines network effects. Specifically, such cooperation would provide DoD, allies and alliances with:

1. Better Coverage—participants would leverage biometrics information from areas where they do not currently maintain a physical presence.
2. Better Quality—external data usage by allies helps motivate producers to maintain high quality standards to avoid the professional embarrassment that comes with a foreign military or civilian noting one's substandard performance.
3. Reduced Production Costs—participants would obtain the force-wide benefits while typically only paying for their organic manpower and equipment.
4. Experience Applicable to Future Operations—cooperation would mature the SOPs and the practical knowledge for improved conduct of future operations.

Despite the mutual benefits and technical feasibility, at present, there is no known automated electronic exchange of biometrics information between DoD Forces in Afghanistan and UNHCR's Iris Validation/Departure Centres (IVCs) in Pakistan. Likewise, there is no automated electronic exchange of biometrics information between DoD Forces and NATO's Local Employment Program (LEP) in the Balkans.[28]

Some Urgency

These unrealized opportunities are the harbingers of greater impending problems should DoD fail to develop suitable policies and laws with international governing bodies, alliances, and allied militaries. Allied nations and alliances are currently developing policy, legal frameworks, and public opinion regimes on the collection and use of biometrics and related personal information. While these path-breaking efforts are ***wholly consistent*** with DoD's strategic goal to "preserve and promote the way of life of free and open societies based on the rule of law," the resulting national policies and laws will also apply to a nation's military forces participating in coalition operations. Without active DoD involvement in these discussions, their policies, laws, public opinion, and resulting conventions are unlikely to adequately consider and reflect the need for ***legitimate*** military collection and use of biometrics and related personal information that provides for the common defense of free and open societies.

---

[27] Based on the UNHCR's 2006 estimate. See: UNHCR Report: Registration of Afghans in Pakistan, 2007, (http://www.unhcr.org.pk/)

[28] Telephonic interview with NATO LEP manager, 2005.

Where DoD's international engagement falls short, commanders suffer the burden of integrating these disparate policies and laws at the least favorable moment: when ordered to conduct a combined-joint operation. The operational consequences are complicated biometrics collection and exchange standards that vary by what country's military force occupies what terrain at any given moment. NATO operations in Kosovo provide a pertinent example.

In Kosovo, a unified NATO Kosovo FORce (KFOR) combined-joint headquarters oversees security operations across terrain divided among several national sectors (e.g., German, French, American, British). Each national sector operates with different tools and policies for the collection and use of biometrics. This complicates the exchange and use of biometrics within Kosovo, and with forces in neighboring Bosnia and distant Afghanistan where the nations also have deployed forces and/or personnel assigned to the unified combined-joint headquarters. The legitimate sharing of this data appears warranted given allegations of terrorist recruiting in Kosovo, and the routine presence of Kosovar workers on military bases outside Kosovo.[29]

These are solvable challenges. DoD's leading role in alliances and international governing bodies provide presence and voice to the legitimate military collection and use of biometrics and related personal information. Likewise, operations in Iraq, Afghanistan, and the Balkans provide DoD with rich sources of examples and experiences that, coupled with American leadership in technical and engineering standards, provide DoD with unique insight to marshal favorable international legal and political forces and public opinion. All the elements appear to be in place. What appears missing is DoD interest in leading these international developments as it did on similar issues throughout the Cold War.

MASS CONSUMPTION

Utility (benefit) is in consumption, not production (cost)

The benefits of biometrics accrue through the consumption and use of biometrics information and services. Consumption is the benefit; production is the cost. Their only relationship is value: a measure of benefit relative to cost. DoD's measure of success is not how much DoD spends building biometric “widgets” that stack up in some electronic warehouse, but rather, how many biometrics transactions are consumed by DoD consumers.

DoD's mass consumption challenges are: (1) clearly identifying its primary and secondary consumers, and (2) maintaining priority of effort on servicing primary consumer demands. These seeming simple challenges are proving difficult in execution because of the easily confused relationships between consumers and producers. This confusion bears out through the value metrics that typically tout biometrics' importance and success through examples of “how much DoD spends on biometrics,” or, “how many millions of biometrics records DoD has generated.” While impressive, these production cost statements say nothing about biometrics actual benefits--value--to military operations or other national security tasks. Or more succinctly, what really matters: consumption.

---

[29] See: Steven Woehrel, Islamic Terrorism and the Balkans, US Dept of State CRS Report for Congress, July 26, 2005; and interview of US Army Civilian Contract Managers in Kosovo and Afghanistan, 2005.

Primary Consumers

DoD's primary consumer base is readily apparent and arguably at the forefront of DoD biometrics efforts. DoD's primary function is the conduct of military operations. These military operations are primarily conducted overseas and span the entire spectrum of conflict. This includes important humanitarian and disaster response operations where the nation has tasked DoD to serve as the US's primary overseas HA/DR response force in lieu of a civilian response corps. With DoD primarily relying upon military personnel to perform these functions, deductive reasoning defines ***DoD's primary biometrics consumer base*** as: forward-deployed US military personnel executing an operation.

The confusion arises when attempting to define the actors. DoD's typical users of biometrics systems (e.g. tactical ground forces) are not just the Department's primary consumers, they are also DoD's primary producers of biometrics information. Additionally, by virtue of their sheer numbers and presence in chaotic and inhospitable regions, they are also the US government's primary producer of biometrics information on individuals encountered overseas who might be considered a threat to national security.

These three "hats" confuses matters by seemingly pitting the forward-deployed tactical commander's consumer requirements against secondary consumer requirements being generated by DoD-external partners like the FBI and DHS. These secondary consumer demands are typically absent a reciprocal benefit that is visible to tactical commanders, creating a "confused" situation where forward-deployed tactical commanders—often in a combat zone—bear all the risks and costs of producing biometrics information without a locally-identifiable benefit for doing so.

Such situations invite adverse consequences—if not outright failure—by violating the guiding principle of economics: self-interest. It is fundamentally counter to accepted economic principles to expect, or successfully demand, tactical commanders expend significant effort and resources on producing secondary consumer products at considerable expense to their local (i.e., primary consumer) needs. Policies that mandate such violations of "natural" law may briefly appear successful at better supporting secondary consumers, but inevitably undermine the original goals by creating powerful disincentives for tactical commanders to use biometrics systems or care about data quality. It requires looking at the secondary consumer issue from a different perspective to recognize that secondary consumers are far better served by DoD ensuring that tactical commanders have a vested self-interest in ensuring the biometrics information they consume and produce is of a quantity and quality that foremost serves their interests, and by extension will serve the interests of secondary consumers as well. Violating this principle of self-interest is a recipe for failure.

If that sounds overblown, consider what a recent GAO study recommended to improve DoD biometrics information sharing with secondary consumers.[30] Written in the arcane language of modalities and databases, the GAO report centers on reconciling the FBI and DHSs' current reliance on high-quality fingerprints relative to DoD's reliance on iris scans for supporting many

[30] GAO report 09-49.

tasks performed by tactical commanders in Iraq and Afghanistan.[31] Ignoring DoD's primary consumer demands, the GAO report recommended that DoD, as the primary producer of biometrics in operations overseas, adopt an "all modal" collection policy that mandates high-quality fingerprinting of those encountered in the conduct of an operation.[32] DoD partially non-concurred, noting that DoD already does high-quality fingerprinting of detainees, and, "In many cases, persons who are not suspected of causing, or intending to cause, harm to U.S. interests are simply screened against the DoD biometrics watchlist when encountered."[33] GAO "disagree[d] and continue[s] to believe that DoD should establish guidance on the collection of a minimum baseline standard set of biometrics information when collecting biometrics information during military activities in the field…" and indicates that high-quality fingerprints should be one of the baseline standards.[34]

The GAO confuses costs and benefits, and appears absent consideration that our Nation's interests are better be served by FBI and DHS updating their institutional processes to employ newer, more-appropriate biometrics modalities. More importantly, the GAO's recommendation excludes consideration of the international legal, political, and public opinion ramifications should DoD embark on high-resolution fingerprinting of local inhabitants in their native lands "who are not suspected of causing, or intending to cause, harm to U.S. interests." If adopted, such a policy:

- Could not be justified on technical grounds, because more efficient "touchless" and non-latent biometric modalities are already in use—notably iris and vein, respectively—by the UN, Gulf Cooperation Council (GCC) states, and commercial enterprises for public administrative and security tasks such as: border entry control, refugee management, facility access control, and individual account verification.

- Would appear at odds with the President's Homeland Security strategy pillars that include: (1) Preparing the Military to Meet 21st Century Threats, (2) Winning the Battle of Ideas, and (3) Restoring American Influence and Our Values.[35]

- Would ignore that most US forces deployed worldwide are the invited guests of sovereign host nations who do not look favorably upon US forces fingerprinting their law-abiding citizens for US domestic counterterrorism purposes.

- Would raise issues of reciprocity in granting foreign governments, like Iraq, the right to fingerprint US citizens in their country, as well as the right of foreign military guests of the US to fingerprint US citizens domiciled within US borders as a part of their official duties.

- Would greatly slow tactical task performance due to the orders of magnitude greater time investment required to perform high-quality fingerprinting relative to rapid

[31] Ibid, p. 13.
[32] Ibid, p.8.
[33] Ibid, p. 25.
[34] Ibid, p. 8.
[35] White House Homeland Security Strategy at: www.whitehouse.gov/agenda/homeland_security/

identification biometrics like iris or vein scans, thus greatly reducing the amount of biometrics information tactical commanders produce and make available to the FBI and DHS for screening.

- Would come at the expense of emerging biometric modalities like gait, voice, and extended distance iris and facial matching that appear to offer great tactical advantages over existing biometric modalities.

Ironically, DoD is not fingerprint adverse: ***all individuals detained on suspicion of terrorist or criminal activity currently undergo high-quality fingerprint collection.***[36] But an "all modal" policy like the one recommended by GAO ignores that DoD's primary consumers of biometrics information, the tactical commanders, perform a broad spectrum of tasks where some biometric modalities are simply more appropriate than others.

Similarly, the GAO report ignores the broader benefits of focusing on the primary consumer. DoD's forward-deployed tactical commanders' foremost interest is in consuming biometrics information to support the execution of local tasks, such as: identifying unknown individuals, managing information on local individuals, and documenting routine transactions and events. While biometrics information is often enhanced by "reach-back" analytical support, the routine use of biometrics tools for these tasks generates a tremendous amount of biometrics information through new and repeat encounters that ensure the biometrics information is up-to-date for all authorized users (i.e., network effects). Mandating the use of ill-suited modalities not only creates tangible disincentives for tactical commanders to use biometrics, it saddling US forces with inappropriate biometrics tools that undermine interoperability with participating allies and NGOs who ***will*** use the biometric modalities most appropriate for their analogous tactical tasks.

Biometrics are ultimately about maximizing the benefits of mass consumption. The success of DoD Biometrics hinges on expanding tactical commanders' consumption and use of biometrics information for all types of tasks as appropriate. It also hinges on institutionalizing these principles and legitimating the military use of biometrics throughout the legal, political and public opinion regimes that exist beyond DoD's cloistered biometrics community.

A NEED FOR ACTION

The images and assumptions in the press, the courts and everyday life on DoD biometrics activities have a significant impact on DoD biometrics operations. American press and military writings often discuss the terrorist' asymmetric advantages absent mention of US and allied asymmetric advantages. The underlying assumptions are apparently twofold: (1) it is nobler to battle an enemy while at a disadvantage than giving battle on favorable terms, and (2) the enemy fights "unfairly." Authors even note that, "Americans, in particular, have developed a keen sense of what constitutes fair and unfair behavior in conflict and war."[37]

Such assumptions ignore a simple truth: Only fools fight "fair." Wars are won by making fights as unfair as possible, within recognized legal bounds, so victory is assured. The art and science

[36] See: GAO report 09-49, p. 26.
[37] David Young, "They have no honor," Opinion in the Asian Times, Feb 15, 2009.

of warfare is to bring to bear every available asymmetric—unfair—advantage against one's enemy in a synchronized manner whether the asymmetry is in manpower, tactics, timing, terrain or technology. It was how George Washington's Franco-American Army "unfairly" defeated Cornwallis's force at Yorktown in 1781, and has been institutionalized as the founding principal of military operations research: the application of quantitative techniques to make military outcomes as "unfair" as possible.

DoD's vigorous advocacy of biometrics' asymmetric advantages—biometrics' inherent unfairness towards Mao's fish by making their life difficult and everyone else's better—is an essential aspect of developing and preserving the legal, political, and public opinion frameworks that ensure the ***legitimate*** military use of biometrics and related personal information to provide for the common defense of free and open societies. ***Biometrics can help save lives, avoid human suffering and advance the common goals of free and open societies only if the appropriate legal, political, and public opinion frameworks exist.***

At present, domestic and international advocates for civil rights, privacy, and other concerns are aggressively advancing legal and political agendas that, if left unaddressed by DoD, can seriously debilitate the legitimate current and future military use of biometrics. These are not idle threats or the actions of untalented interlopers. The Secretary of Defense and Congress are already receiving letters from well-meaning organizations expressing their opinion that, "the current [biometrics-based] Iraqi identification practices contravene international treaties…" and proceed to detail concerns to "ensure that Iraqis are afforded basic human rights in their personal information."[38]

Whether one agrees with such arguments or not, they raise pertinent questions that courts, politicians, and public opinion ***will*** address. These civilian privacy experts may better understand and articulate civil rights; but by definition, they are ill-positioned and ill-experienced relative to military officials at fully understanding and expressing the legitimate use of biometrics in military operations.

The onus is not upon civilians to seek out a better understanding of the legitimate use of biometrics in military operations. It is squarely upon DoD to seize the initiative and inform, advocate, and participate in establishing favorable legal, political, and public opinions that ensure the legitimate military use of biometrics. DoD is perhaps the only military in the world with the resources and biometrics experience to lead this dialog. It includes DoD developing the mastery of the subject matter to explain how biometrics contribute to reconstruction, stabilization and humanitarian assistance operations where the enemy is a natural or man-made disaster.

Time is of the essence. It takes years to develop the truly compelling insights and examples that resonate with public opinion and are suitable for codifying as public law and policy. The US is at peril of losing DoD's biometrics asymmetric advantages before they are even realized in military operations through a tangled web of ill-formed and ill-fitting legal, policy, and public opinions developed in the absence of DoD leadership.

---

[38] See: Letter to Secretary Robert M. Gates dated July 27, 2007 by the Directors of Electronic Privacy Information Center, Privacy International , and Human Rights Watch at: http://epic.org/privacy/biometrics/

BIOMETRICS “WORKING TRUTHS”

Primers like this one aspire to inform and advance a discourse on how DoD might improve current biometrics policies and efforts. Since many truths are knowable only in retrospect, at best, the concluding points are “working truths” that warrant further consideration:

Think Strategic. Biometrics are part of the US's asymmetric approach to winning The Long War through non-kinetic means. Biometrics are one of many strategic capabilities to change the underlying socio-economic conditions which breed and support terrorist extremists, helping make communities intolerant of Mao's fish. Biometrics accomplish this by reducing cultural, language and literacy barriers while providing strong identity management and automation to local commerce and governance in developing nations.

Think Integral to Military Operations and Tasks Oriented Towards Individuals. Biometrics are not just a security or Iraq and Afghanistan phenomenon; they are an asymmetric complement to weapons systems. They provide important force multiplier effects and affects across a broad spectrum of tasks conduct in military operations by virtue of their vastly superior transaction efficiencies relative to existing approaches to identifying or verifying an encountered individual, differentiating among individuals, or adding, recalling, updating, or exchanging information on individuals.

Think Enabling of Distributed Operations. Distributed operations require small teams capable of rapidly identifying, differentiating and engaging individuals. Operations in Afghanistan provide nascent examples of distributed operations in practice, and the role of biometrics in supporting US forces when the enemy operates amongst civilians without recognizable uniforms or intent.

Think Balance Across the Force. DoD has yet to field biometrics capabilities for non-combat stabilization, reconstruction, and humanitarian assistance tasks. These tasks make important tactical and strategic contributions towards mission success and often provide a foundation for building positive relationships, automated electronic interoperability and network effects with alliances, allies and international NGOs. These tasks also represent where most unknown individuals are encountered by DoD forces, with the potential to generate large volumes of biometrics information to support the ***legitimate*** military use of biometrics and related personal information to provide for the common defense of free and open societies.

Think Task (Consumption)-Centric. Military utility is created through accomplishing actual tasks, not collecting biometrics information. Biometrics add value to DoD's primary consumers—the tactical commanders—be ensuring the applied functional form, data structure and biometric modalities are appropriate to each and every task. This bends biometrics to support the Soldier or Marine instead of trying to bend the Soldier or Marine to support the biometric. These task enablers create local incentives—self-interest—to maximize use and data quality, thereby maximizing "network effects."

Think Social Over Technical. Most biometrics challenges today are socio-organizational issues related to how DoD integrates its own global operations and effectively integrates efforts with

alliances, allies and international NGOs. While technology is the catalyst, the products are internal guidance and external public laws, policies, and conventions that will ultimately determine biometrics' contribution to military operations.

Think System, not Component. Fordism is a system's approach to enterprise management that helps forge interrelationships between producers and consumers to achieve a biometrics enterprise capable of addressing the "knowledge intense" operating environment of current and future military operations. The system's approach reminds us that success is not achieved through technical prowess or more gadgets, but harmonizing human capital and technology investments with standard approaches that aid consumers and producers within an overarching institutional structure. Successful commercial businesses master an understanding of their consumers' preferences and tightly couple their hardware and human capital purchases to best serve their consumer base. DoD would benefit from doing the same.

Think Multi-Modal. There is no "uber"-biometric. Each biometric modality exploits a unique physical feature that provides tactical advantages and disadvantages to military operations. While advances in touchless and stand-off modalities offer great promise for further efficiencies in military tasks, it will still often require the statistical power of fusing two or more biometric modalities to support the forward-deployed tactical commanders' tasks.

Think Space and Time. Biometrics help eliminate exploitable gaps and seams between organizations and activities separated by space (geography) and time. The enduring nature of a person's physical features helps preserve the value of biometrics over time. For DoD's policymakers and tactical commanders, this infers great responsibility to ensure biometrics efforts are sustainable over time through proper usage and data entry so that adjacent and follow-on forces can benefit from their work.

Think Legitimate Application of Asymmetric Advantages. Victory in The Long War is hastened by applying every legal asymmetric advantage in the arsenal of free and open societies to deter, defeat, and undermine those who engage in or support terrorist extremists. Biometrics provide a rapidly evolving asymmetric capability that history will recall as far more important than armored tanks, aircraft carriers and fighter planes in winning The Long War.