Catalysts of Military Innovation: A Case Study of Defense BIOMETRICS

COL Glenn Voelz, USA

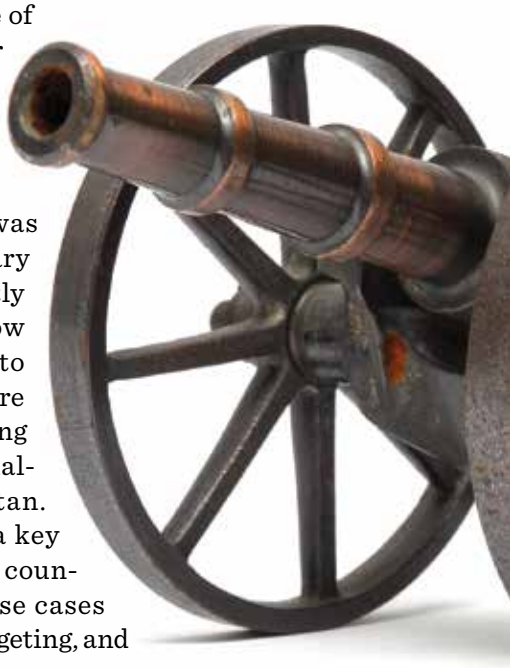
Military innovation is a central component of U.S. strategic advantage; however, the precise conditions that enable such innovation remain a matter of debate. The recent introduction of biometrics onto the battlefield offers a useful case study for examining catalysts of military innovation and specific factors that enabled the Department of Defense to rapidly field new technologies in response to urgent operational requirements. This article considers how doctrinal design and warfighting strategies became important catalysts, and how challenges associated with rapid fielding, interoperability, and training limited U.S. forces from realizing the full potential of these new technologies. This case study proposes that military innovation can occur only by using an integrated approach that encompasses the interdependent elements of technology, acquisition, doctrinal design, and warfighting strategies. It offers general conclusions on conditions that create fertile environments for military innovation and identifies lessons learned for future efforts at introducing new technologies into the field.

Keywords: *Doctrine, acquisition strategy, Department of Defense Automated Biometric Identification System*

Lead image by Diane Fleischer

Military innovation has reemerged as a topic of interest among national security professionals. This has been spurred by a growing concern that the United States has ceded the military-technological advantage it enjoyed for most of the post-World War II era. The push to regain this edge has led to a number of new initiatives such as Better Buying Power 3.0, aimed at accelerating acquisition reform and incentivizing innovation within government. Similarly, the Department of Defense (DoD) recently announced the Defense Innovation Initiative, a set of long-range research and development programs intended to identify advanced capabilities as the basis of a "Third Offset Strategy." These efforts focus on achieving high-payoff breakthroughs in areas such as artificial intelligence, robotics, additive manufacturing, and nanotechnology, among others. Last year, Secretary of Defense Ashton Carter opened the Defense Innovation Unit Experimental in Silicon Valley to "scout, connect, and support the innovation of disruptive technology" with potential military value. The common theme among these initiatives is to create U.S. strategic advantage by improving the process of military innovation; however, the precise conditions that enable this to occur remain a matter of some debate.

One source of insight comes from analyzing recent examples of military innovation that emerged during the conflicts in Iraq and Afghanistan. Among these, biometrics offers a useful case study of a technology that was virtually unknown on the battlefield prior to 9/11, yet by the end of the decade had become a ubiquitous feature of U.S. military operations. This particular example is instructive because it involved the rapid and relatively successful integration of a new technology that substantively changed the way U.S. forces conducted operations on the ground. This outcome was due to several factors. As an untested military technology, biometrics evolved concurrently with new doctrinal concepts describing how the tools would be used on the battlefield to create desired effects. These capabilities were then applied as part of a coherent warfighting strategy focused on specific operational challenges encountered in Iraq and Afghanistan. Within this context, biometrics became a key enabling technology of population-centric counterinsurgency, applied across a range of use cases such as detainee management, high-value targeting, and



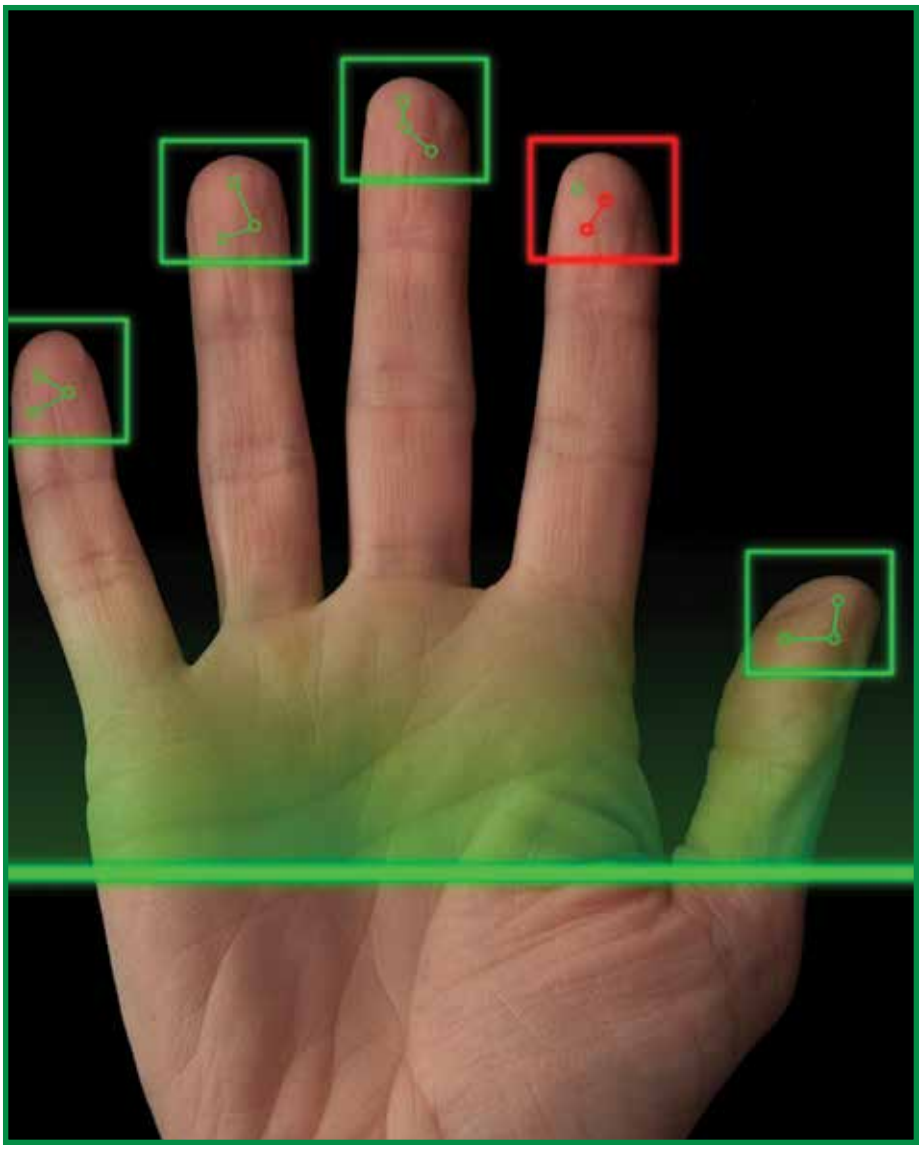
support to Rule of Law operations. However, despite the success in rapidly moving these new technologies into the field, in some cases the operational impact was limited due to challenges with interoperability, informational sharing, and training. The case study of biometrics demonstrates that effective military innovation can only occur through an integrated approach that takes into account the interdependent elements of technology development, acquisition planning, doctrinal design, and warfighting strategy.

Defining Military Innovation

Innovation describes the process by which a new idea, technology, or method provides an improved capability for addressing an existing need. Generally, it follows a process of discovery, application, and exploitation where basic research is transformed from a concept into a tool or process that delivers some kind of operational advantage. Scholars of military innovation look to several characteristics for evidence of meaningful change. The first is whether the process of innovation substantively alters the manner in which military formations function in the field. A second factor is whether these changes are significant in terms of scope and organizational impact. A third component takes into account whether these changes ultimately produce greater military effectiveness (Grissom, 2006).

There exists a relatively deep body of academic literature on military innovation, examining the technological, cultural, and bureaucratic aspects of change. Much of this research focuses on "innovation inhibitors" that undermine the successful adoption of new technologies and methods (Jungdahl & Macdonald, 2014). Many of these studies apply the lens of organizational theory with emphasis on institutional factors such as bureaucratic culture and leadership dynamics as key variables in the process of innovation (Avant, 1994; Posen, 1984). Williamson Murray's influential study, *Military Adaptation in War*, notes how modern bureaucratic and military cultures have become antithetical to adaptation, often for reasons relating to parochial interests or avoidance of negative consequences resulting from incorrect decisions (Murray, 2009).

Some experts consider wartime innovation a phenomenon that must be examined separately from that of peacetime change (Rosen, 1991). Indeed, with many examples of wartime innovation, the causal pathways of change tend to be somewhat less complex and highly responsive to the exigent demands of the battlefield. In such instances, the act of warfighting becomes a laboratory for conducting "natural experiments" in which technology requirements are explicitly articulated in response to challenges posed by an actual adversary rather than a hypothetical one. This situation provides



immediate tactical feedback and creates a powerful dynamic for iterative design and process improvement. These factors inevitably sharpen how operational needs are defined, while at the same time accelerating the bureaucratic process of research, development, prototyping, and fielding.

Yet, even in cases where explicit tactical demands drive the adoption of a new military technology, these tools do not exist in isolation. Successful diffusion of new technologies or methods still requires a conceptual driver to guide the course of innovation. This provides the context for how a given technology will be employed on the battlefield, thereby creating meaningful military effects. Importantly, Williamson Murray observes that technological sophistication is not necessarily the most critical factor of successful innovation. Rather, it is how well a new technology is incorporated into an effective concept for fighting that matters. This emerges from evolutionary problem solving focused on specific operational challenges. However, effective implementation also requires a coherent framework of employment grounded in doctrine, operational concepts, and an overarching strategic vision for how the technology will be used.

In the case of biometrics, the key conceptual driver was the realization that counterinsurgency and counterterrorism operations against irregular adversaries required different doctrinal approaches and technical tools than those optimized for conventional military conflict. In particular, the intelligence, surveillance, and reconnaissance technologies needed for identifying and targeting individual combatants and their networks were not the same as those designed for detecting and destroying motorized rifle battalions. This new mode of warfare turned combatant identity into a critical technical signature of the battlefield. In this complex human terrain, biometric technologies helped put a uniform on the nation's enemies and reduced their ability to leverage anonymity for military advantage. This paradigm shift in thinking about identity and military targeting established a clear operational role for biometrics. It firmly placed the new technology within an explicit doctrinal framework and described how it would be used to support the overarching warfighting strategy. In the case of biometrics, several specific factors were instrumental as catalysts for innovation:

1. **Clear Operational Use Case.** Military innovation is most effective when it addresses a well-defined operational challenge. As a largely untested battlefield technology, biometrics evolved rapidly for the simple reason that it provided a practical solution to help identify, track, and target irregular combatants fighting without uniforms or conventional formations. Within the context of waging

counterinsurgency, biometrics technologies offered a powerful tool with a wide variety of use cases such as detainee management, high-value targeting, and support to Rule of Law operations.

2. **Value Proposition Linked to Doctrinal and Strategic Concepts.** New military technologies require a coherent concept of employment that clearly demonstrates their value within a larger doctrinal and strategic framework. Biometrics succeeded in part because it was introduced within the context of new doctrinal and strategic approaches focused on population-centric counterinsurgency and identity-based targeting. These priorities emerged within the broader context of Iraq and Afghanistan, where biometrics became an increasingly important technical tool for navigating complex human terrain and assisting U.S. forces in waging war against the enemy.

3. **Effective Bureaucratic Constituencies.** Military innovation ultimately occurs within an organizational context; therefore, it requires strong bureaucratic advocates with the institutional capacity to manage the development and integration of new technologies. Biometrics had a distinct advantage of being a multiuse technology with a broad range of operational applications. Just as biometrics appeared on the battlefield, the value of the technology was also recognized by law enforcement, Homeland Security, and the Intelligence Community, thereby creating a critical mass of interest groups—all pushing for new investments. However, numerous constituencies pursuing parallel development programs also created challenges for interoperability and data sharing as the new technologies evolved.

4. **Development Partners in a Competitive Marketplace.** Military innovation works best when government works collaboratively with a diverse range of development partners in a dynamic and competitive marketplace. As biometrics technologies appeared on the battlefield, a growing demand also emerged for new commercial applications that drove a period of rapid innovations in the nondefense sector. This enabled DoD to benefit from significant private investment in research, development, and prototyping. While DoD was not the only market driver of this innovation, it was in a unique position to exploit the latest developments for the commercial sector and adapt these tools directly to military needs.

Biometrics Fundamentals

As a general term, biometrics describes the measure of biological and/or behavioral characteristics that can be used for automated recognition or identity verification. A biometric modality refers to a type or class of biometric samples such as those derived from a facial image, fingerprint, iris, or voice pattern. Biometric matching describes the capability and/or process of comparing biometric data in order to link previously obtained biometrics and related contextual data to a particular identity or for the verification of identity (Defense Forensics and Biometrics Agency, 2013). Biometric data can be combined with biographical and other contextual information to build a "pattern of life" profile for individual subjects. When analyzed together with other biometric records and all-source intelligence, this information can reveal connections among individuals, correlate their activities, and expose the structure of their networks.

Biometrics as Military Innovation

One of the early lessons learned from the conflicts in Iraq and Afghanistan was that many of the legacy intelligence technologies developed for conventional warfare against state-based adversaries did not provide the kind of information needed to effectively support counterinsurgency operations and, in particular, identity-based, high-value targeting (Defense Science Board, 2011). As the United States shifted towards a counterinsurgency strategy, it required population-centric information and refined targeting intelligence for identifying, isolating, and eliminating insurgents from the battlefield. These operational challenges demanded new technologies to enable U.S. forces to detect and identify individual actors, characterize and geo-locate their activities, and understand the structure and function of their networks. This presented an enormous tactical dilemma for soldiers fighting on an irregular battlefield against adversaries who did not wear uniforms and could not easily be distinguished from the local population. As such, identity verification emerged as one of the major technical challenges of the campaigns in Iraq and Afghanistan. Although relatively untested as a military technology, biometrics rapidly emerged as an important tool for differentiating actors within a complex and often ambiguous operational environment.

Prior to 2001, the U.S. military had no significant operational experience in the use of biometrics. DoD's original vision for biometrics was relatively limited in scope and focused principally on tasks such as information assurance

for automation systems and physical access control (Defense Science Board, 2007; National Science and Technology Council, 2008, p. 21). However, new Homeland Security concerns following 9/11 and the subsequent conflicts in Iraq and Afghanistan became the initial catalysts that transformed biometrics into an operationally focused technology. Although the Army's biometric development program had been operating since 1999, it was not until 2001 that the Battle Command Battle Laboratory produced the first Biometric Automated Toolset (BAT) prototype, a multimodal (fingerprint, iris, and face) system for collecting, matching, and storing personally identifying information. This technology was initially field-tested in the Balkans where it was primarily used for identifying local national workers accessing U.S. installations. As these technologies matured from prototype design into a functional capability, a number of new uses evolved that greatly expanded the value of these tools across the range of military operations.

Biometrics Use Case: Detainee Management

Almost immediately at the start of operations in Iraq and Afghanistan, U.S. forces faced an unprecedented challenge of managing the large numbers of detainees on the battlefield. One report from early in the conflicts noted how the "handling of detainees, appropriately documenting their capture, and identifying and accounting for them, were all dysfunctional processes, using little or no automation tools" (Jones, 2004, p. 21). New biometrics technologies offered one solution for this dilemma. In early 2002, a BAT prototype was fielded to Joint Special Operations Command in Afghanistan and first used for enrolling persons of interest detained on the battlefield. By 2003, similar systems were deployed at detention facilities in Iraq for detainee management and later as a tool for generating biometrically enhanced interrogation reporting (Iasso, 2013). By 2004, DoD directed that all U.S. military units worldwide would collect biometric data from detainees (DoD, 2004). One vivid demonstration of the value of this data came in 2011 when 500 Taliban prisoners escaped from Kandahar's Sarposa prison. All detainees had previously undergone biometric enrollment, and within 1 month 30 individuals were recaptured in the local area as a result of random biometric checks (The Eyes Have It: Biometrics in Afghanistan, 2012). Since then, biometric data gathered by DoD and other government agencies have been used to identify and prevent tens of thousands of potentially threatening individuals from entering the United States (Partnership for Public Service, 2013, pp. 12–13).

The first major operational employment of the BAT system was by Marine Corps units during the resettlement of Fallujah following major combat operations in 2004. Handheld biometric devices and databases were used to monitor the flow of residents into and out of the city as a means of identifying insurgents moving among the population (McWilliams & Schlosser, 2014, p. 62; Shanker, 2011). The use of this technology on the battlefield expanded rapidly as the United States shifted towards a population-centric counterinsurgency strategy in Iraq and became a critical tool during the "surge" period for identifying and segregating insurgents from the larger population. By that time, thousands of BAT toolsets and the newer Handheld Interagency Identity Detection Equipment (HIIDE) systems had been fielded to tactical units. Multimodal or 13-point biometric collection (10 fingers, two irises, and one face) became a standard feature of combat patrols and documenting encounters with persons of interest. By the end of combat operations in Iraq, U.S. forces had compiled a biometric database containing some three million individual files (Ackerman, 2011).

Biometric technologies proved equally important in Afghanistan where few inhabitants possessed verifiable identity documentation and combatants could not easily be distinguished from the surrounding population. Over 7,000 biometric collection devices were fielded and used for functions such as detainee management, execution of high-risk warrants, and targeted raids against named insurgents. During the conflict, U.S. forces collected over 2.5 million biometrics records and placed some 33,000 individual identities on biometrically enabled watch lists (The Eyes Have It, 2012; U.S. Government Accountability Office [GAO], 2012).

Biometrics as Doctrinal Innovation

The basic act of fielding a new technology by itself does not represent true military innovation. Tools are not inherently valuable without a viable concept of employment that describes how a given technology will contribute towards achieving an organization's core functions. This requires a concurrent process of doctrinal innovation that exploits the potential of a new technology by providing a theoretical framework and methods for how it will be used to achieve military objectives. To be successful, doctrinal innovation must occur on a sufficiently large scale to overturn old ways of doing business, thereby institutionalizing the new tools and methods (Cote, 1996). This is no small task and sometimes requires a wholesale reconceptualization of how an organization perceives its central warfighting tasks.

The catalysts for such change may come from a variety of sources. Some theories focus on endogenous factors such as organizational culture, civil-military relations, or Service rivalries as central dynamics in this process (Posen, 1984; Rosen, 1991). Other theories weigh more heavily on the influence of exogenous factors such as the rise of unanticipated threats or emergence of novel technologies that disrupt the fundamental balance of military advantage on the battlefield. In the case of biometrics, several external factors played a role in driving how these technologies evolved on the battlefield.

The U.S. military's adoption of biometrics emerged within the context of a larger paradigm shift that moved identity to the center of a new warfighting paradigm. Counterinsurgency and counterterrorism operations required the U.S. military to undertake a major doctrinal reorientation focused on targeting *networks* and *individual combatants* rather than formations and weapons platforms. In his counterinsurgency guidance to multinational forces in Iraq, Army Gen. David Petraeus directed commanders to "defeat the network, not just the attack" by focusing intelligence assets on the nodes and links of

the insurgency—identifying its leaders, financiers, suppliers, and operators (Petraeus, 2008, p. 2). This required technologies to support a new targeting paradigm by enabling U.S. forces to "identify and separate the reconcilables from the irreconcilables" on an irregular battlefield. Biometrics became a central technical component of this new strategic approach.

Biometrics Use Case: High-Value Targeting

An important aspect of U.S. counterinsurgency and counterterrorism strategies involved identity-based targeting of individual combatants. Biometric technologies and Biometrically Enabled Intelligence (BEI) became important elements of the shift to this new targeting paradigm. This process for targeting high-value individuals was doctrinally formalized within the find, fix, finish, exploit, analyze, and disseminate (F3EAD) methodology. Biometric databases and watchlist information played an important role in identifying, tracking, and targeting these individuals. For example Biometric Identification Analysis Reports (BIAR) provided U.S. forces with biographical information, encounter history, and disposition instructions for persons of interest. During the "surge" period in Iraq, these data were used to remove an average of two high-value individuals from the battlefield each day. When combined with forensic data, this biometric information was a powerful tool for penetrating cells employing Improvised Explosive Devices against coalition forces and matching specific individuals to these activities. For example, from 2007 to 2008, more than 1,700 adversary combatants were biometrically linked to forensic evidence directly associating them with the manufacture and use of these devices on the battlefield (Kieffer & Trissell, 2010).

As biometric technologies evolved within this new warfighting paradigm, DoD directed combatant commanders to integrate these capabilities into mission planning across the six-phase joint planning model (DoD, 2008). The Army formalized the doctrinal role for biometrics technologies as part of its concept for Biometrically Enabled Intelligence (BEI), or the intelligence resulting from the combination of biometric data with other intelligence information to identify potential threat actors. The Navy and Marine Corps adopted a similar concept known as Identity Operations (IdOps) into their respective Service doctrine. This approach encompasses the synchronized application of biometric technologies, forensics, and identity management capabilities in support of maritime and expeditionary operations (Department of the Navy, 2012).

More recently, the DoD Intelligence Community introduced into joint doctrine an overarching concept for Identity Intelligence (I2), or the collection, analysis exploitation and management of identity attributes and associated technologies and processes (Joint Chiefs of Staff, 2013). I2 integrates several distinct technical-functional areas combining BEI with other all-source data to connect individual actors to other persons, places, activities, or materials. This doctrine defines a specific role for biometric technologies across a range of mission functions including raids, checkpoint operations, border control and maritime interdiction, force protection, support to host-nation Rule of Law, and detailed human terrain mapping. These examples all illustrate the degree to which biometric technologies have been integrated within a doctrinal framework supported by specific use cases and tactical applications.

Biometrics Use Case: Support to Rule of Law and Stability Operations

U.S. counterinsurgency strategy presented enormous procedural challenges regarding legal adjudication of "unprivileged enemy belligerents" detained on the battlefield as well as monitoring released individuals for recidivism. Biometric technologies played a critical role in supporting such "evidence-based" operations, particularly during the stability and support phase when formal criminal proceedings became the only means of effectively removing insurgents from the battlefield (Voetelink, 2013). Biometric and forensic data provided much of the evidentiary basis for prosecution support packages used by detainee review boards and host-nation criminal proceedings against suspected insurgents. These packages provided detailed biological and biographical information linking suspect individuals to insurgent activities.

Counterinsurgency strategy also called for U.S. forces to help reestablish rule of law and support local governance. This included the transfer of biometric information and technologies to local partners and training on how to use these tools as part of legal proceedings. As one example, the Afghan government now maintains its own biometric database and uses this information in support of warrant-based targeting and prosecutions. Of recent cases tried in the Afghan National Security Court, there have been convictions in a majority of instances where biometric data have been linked to forensic evidence presented in the case (Pendall & Sieg, 2014).

Acquisition and Technology Integration as Factors in Military Innovation

The nature of bureaucratic culture and the dynamics of the acquisition process also play an important role in the process of military innovation. As a general rule, bureaucracies tend towards a status quo bias; therefore, they are not necessarily designed to accommodate adaptation (Samuelson & Zeckhauser, 1988). This means that organizations cannot always exploit the full potential of an emerging technology even when there are clear advantages over previous methods (Murray, 2009). In the case of biometrics, challenges relating to the acquisition process and integration of the new technologies produced mixed results in terms of creating the conditions for successful innovation.

In the initial aftermath of 9/11, government officials immediately recognized the need for improved border control and automated systems for identifying individuals trying to enter the country. New biometrics technologies offered one means of verifying identities and comparing these records against watchlists of potential threats gathered by DoD and other government agencies. Effective use of these data required an unprecedented effort to overcome deep institutional barriers between the Department of Defense, the Intelligence Community, Homeland Security, and domestic law enforcement so that threat identity information could be shared across the entire enterprise. However, the U.S. government had only two major operational biometric systems on 9/11—one at the Federal Bureau of Investigation (FBI) and another with U.S. Immigration and Naturalization—as well as a handful of smaller research projects and pilot studies (National Science and Technology Council, 2008).

As U.S. forces began collecting large amounts of biometric data on the battlefield, a critical need emerged for an authoritative database to process, store, and match these biometric records. This required an information management system designed for sharing identity information among widely dispersed military forces in the field, as well as with domestic law enforcement and the Intelligence Community. Within DoD, this led to the initial prototype design for what became the Department of Defense Automated Biometric Identification System (DoD ABIS), the military's centralized multimodal biometric data repository. This system later included a Biometrically Enabled Watchlist feature enabling analysts to highlight person-of-interest records, and provide disposition instructions and other relevant information. As DoD was deploying its prototype system, the FBI had already fielded its own automated fingerprint database system known as

the Integrated Automated Fingerprint Identification System. Concurrently, the Department of Homeland Security was conducting an upgrade of its own biometric identity system used for managing immigration, visa, border control, and law enforcement requirements. Additionally, in 2004 the National Counterterrorism Center was tasked with managing the Terrorist Identities Datamart Environment, intended to be the government's central repository of information relating to international terrorist identities.

Even as biometric collection devices proliferated across the battlefields of Iraq and Afghanistan, DoD struggled to articulate an overall strategic vision for how the new technologies would evolve as a warfighting capability and integrate into the larger national security apparatus. According to one assessment, the DoD biometrics enterprise lacked "specific and measurable strategic goals and objectives for using biometrics" and a lack of common understanding about the purpose and boundaries of the enterprise (Shontz, Libicki, Rudavsky, & Bradley, 2012). This ambiguity contributed to discontinuities in the acquisition program and criticisms that the overall DoD biometrics program lacked a long-range planning horizon. One specialist working on biometrics programs at the Army's Communications-Electronics Research, Development and Engineering Center observed how many of the Quick-Reaction Capabilities fielded during the conflicts were only used for a year or two, then not sustained due to shrinking budgets or changing operational priorities (Jontz, 2015). In the case of biometrics, the focus on rapidly moving collection devices out to units also meant that some new capabilities were fielded without adhering to DoD standards, performance measures, and operational testing and evaluation requirements (Shontz et al., 2012).

The rapid fielding process also had implications regarding preparing the force for integration of the new technologies. Because these technologies were a relatively untested capability, the military had not yet developed the human capital needed to fully exploit their potential. Initially, a relatively small number of trained users and leaders were familiar with the systems. For example, the GAO found that DoD did not sufficiently instruct unit commanders on effective use of biometrics, and noted that many military leaders were unaware of how the technology contributed to identifying

enemy combatants (GAO, 2012). This led to confusion over how and when to incorporate biometrics capabilities into mission planning and how to best employ the systems in the field. A separate study attributed some of these shortfalls to delays in establishing biometrics as a formal Program of Record that would have formalized the process of establishing common training standards (Shontz et al., 2012).

While some units such as Special Operations forces clearly leveraged the new technology to great effect, its operational integration across the force was uneven. Inconsistent training meant that individual units applied significant discretion in terms of what biometric data were gathered and the methods of collection. These training shortfalls affected the quality of biometric data collection, and in some cases resulted in the loss of information gathered from the field and delays in transmission into the centralized, authoritative database (GAO, 2012). In hindsight, rapid fielding was the correct decision from the perspective of supporting soldiers in the field with available technology; however, it was not without consequences. The process was likely a factor contributing to challenges with interoperability and training that ultimately limited the operational impact of a promising new technology.

Other problems encountered during the early deployment of biometrics were not specifically related to the technology itself, but rather reflected bureaucratic challenges involved in the acquisition process. Discussions with DoD's Biometrics program manager suggested that the Executive Agent was not sufficiently empowered to provide effective oversight and strategic guidance across the enterprise as the technology evolved (Vann-Olejasz, personal communication, 2014-2015). This contributed to challenges promulgating and enforcing standards of interoperability as various components pursued independent development programs (GAO, 2012; Shontz et al., 2012). For example, by 2011 the Army had still not fully adopted common biometric standards for its primary handheld collection device, the HIIDE, being used in Iraq and Afghanistan. This left the system unable to automatically transmit biometric data to other federal agencies.

According to the GAO, since the device was developed in response to an urgent mission requirement, it was not required to adhere to DoD's information technology standards.

Other difficulties emerged related to coordination among a diverse range of users, often with differing technology requirements and protocols for handling biometric information. According to the GAO, system capacities developed for different mission needs affected agencies' ability to process one another's queries for biometric information. This complicated the process of developing and approving interagency biometric sharing agreements between DoD and the FBI. Similar problems were encountered establishing direct connectivity between DoD and Department of Homeland Security (DHS) biometric databases (GAO, 2011). Even within DoD, various components were not always able to seamlessly share biometric information using a commonly understood process and methodology. This issue included challenges of passing and comparing information stored on domains of different classification. These examples support Williamson Murray's (2009) contention that technology implementation is an equally important aspect of military innovation as the sophistication of the technology itself.

Innovation Lessons Learned from Defense Biometrics

As a recent example of military innovation, biometrics offers a useful case study for understanding how a new and relatively untested technology was integrated into operational use during wartime. At the start of combat operations in Iraq and Afghanistan, the U.S. military had virtually no experience or operational concepts for employing biometrics. However, by the end of the decade the devices had become a commonplace tool on the battlefield and an important enabling technology of counterinsurgency and counterterrorism operations.

Several factors contributed to this outcome. First, within the context of the unique tactical challenges encountered by U.S. forces in Iraq and Afghanistan, biometric technologies had a number of specific and highly relevant use cases. Second, the technology was firmly grounded in a doctrinal framework and overarching warfighting strategy that clearly articulated how the technology could be used to improve the effectiveness of U.S. forces on the battlefield. Third, during the initial developmental stage, multiple constituencies actively pushed for the integration of biometrics technologies for a wide variety of applications. Finally, DoD and other users benefitted from a rapidly expanding commercial marketplace that was able to deliver

cutting-edge technologies, readily adaptable to military use. The combination of these factors played a significant role as catalysts for innovation and facilitated the relatively successful integration of a new military technology.

However, despite these significant achievements, biometrics was not a flawless example of military innovation. Some notable shortfalls related to challenges associated with the rapid fielding process. For example, the urgent demand to move collection devices out to units meant that some new technologies were deployed without adhering to formal performance measures and standards for interoperability. This contributed to difficulties in moving and sharing biometric information among interagency partners. Additionally, as the new tools were placed into units, initially a relatively limited number of users and leaders possessed sufficient knowledge and experience to fully exploit the potential of the new technology. These challenges were certainly not limited to DoD. Indeed, one group of experts recently noted that even as biometrics technologies rapidly evolved over the last decade, the legal, political, and resource framework for how to implement these tools has lagged behind the technological advances (Aughenbaugh, 2015).

> ***In terms of rapidly developing and fielding a new technology, the record of defense biometrics should be considered a tactical success.***

In terms of rapidly developing and fielding a new technology, the record of defense biometrics should be considered a tactical success. During the course of the conflicts in Iraq and Afghanistan, U.S. forces generally made effective use of an emerging capability that directly enabled new forms of identity-based operations in response to unique demands of waging irregular warfare. However, the rapid fielding process did reveal shortcomings in how DoD manages military innovation at the bureaucratic level. These challenges are undoubtedly not unique to biometrics and are certainly worthy of future study to better understand how DoD can improve process models for wartime innovation. As one recent study of military innovation noted, militaries exist for war, but they more often innovate during peacetime

(Hill, 2015). Therefore, strategies for innovation must be adaptable to both environments and able to survive the transition from one condition to the next. In the end, this may be one of the key lessons learned from the example of biometrics.

Challenges for the Future

The lessons drawn from the initial experience of fielding biometrics will be particularly important as the technology enters its second generation—an evolution that will most likely progress along a very different developmental path than the initial phase. In this respect, biometrics may offer an example of the changing model for development and acquisition of cutting-edge defense technologies. During the Cold War era, DoD developed many of its most important capabilities within a closed system of innovation dominated by the defense-industrial complex. Most of these technologies were created under the purview of government-sponsored research and development programs, built in collaboration with a relatively small circle of defense contractors. An emerging model of military innovation may increasingly involve a wider range of commercial providers developing new technologies not explicitly designed for defense applications, but later adapted to military purposes. The field of biometrics reflects the dynamics of this transition.

The attacks of 9/11 and subsequent conflicts in Iraq and Afghanistan were important initial catalysts driving the first biometrics revolution. Between 2007 and 2015, DoD drove a sizable portion of new investments in the field with an estimated $3.5 billion in program spending (GAO, 2011). These requirements substantially defined many of the initial prototype technologies that fueled industry growth rates in excess of 28 percent between 2005 and 2010 (Gelb & Clark, 2013). However, even during this period of rapid expansion, already underway was a gradual transition of the customer base—away from government and military requirements. As the sector matured, it shifted towards new applications in health care, retail services, banking, and consumer digital devices (Biometrics Gets Down to Business, 2006). This trend is only expected to accelerate as DoD represents an increasingly smaller fraction of this rapidly expanding marketplace.

One recent industry report placed the value of the current global biometrics market at $7 billion annually, projected to reach $44 billion per year by 2021. However, the key growth areas for the industry will likely come from sectors other than military and defense. Furthermore, the United States will not be the primary driver of this growth with countries such as India, Mexico,

Russia, and China expected to create much of the future demand for biometrics technologies (National Security and Market Watch, 2015; King, 2014). What this means in practical terms is that DoD will increasingly need to look beyond the traditional jurisdiction of government-sponsored research and development programs to access cutting-edge technologies in the field. This will be particularly true across the range of research areas likely to be critical for the next generation biometrics capabilities—areas such as remote sensing, data science and artificial intelligence, information management, and communications. All of these factors suggest that future military innovation will depend largely on DoD's ability to identify and effectively assimilate commercial technologies from the nondefense sector. The lessons from biometrics suggest a few of the potential challenges.

> ***One recent industry report placed the value of the current global biometrics market at $7 billion annually, projected to reach $44 billion per year by 2021.***

Biometrics, in particular, is a technology where the benefits derive from network effects, meaning that its utility is directly related to the number of users able to input data, conduct searches, and discover associations within a commonly accessible database. This makes interoperability central to the value proposition of the technology. As the last decade of counterinsurgency and counterterrorism operations demonstrated, U.S. national security strategy increasingly requires a "whole of government" approach based on seamless information sharing between the military, Intelligence Community, State Department, DHS, and law enforcement. Furthermore, transnational concerns about terrorism, organized crime, and mass migrations will require expanded collaboration and greater information sharing across borders and between governments in the future. The issues of interoperability and technology integration will be increasingly critical aspects of innovation as governments adopt strategies based on data-intensive decision making.

Given the rate of change in the commercial sector, DoD will be challenged to keep pace with new developments, continuous upgrades to existing systems, and the rapid evolution of new applications for existing technologies. Furthermore, some of the initiatives intended to spur innovation such as greater service autonomy in acquisition, increased prototyping, and

accelerated fielding may even exacerbate existing challenges regarding interoperability, data sharing, and integration. This also raises concerns about whether doctrinal development, concepts of employment, and force training can keep up with the pace of technological advances. These issues highlight the fact that identifying and acquiring cutting-edge technology is only one aspect of successful military innovation.

References

Ackerman, S. (2011, December 21). U.S. holds on to biometrics database of 3 million Iraqis. *Wired*. Retrieved from http://www.wired.com/2011/12/iraq-biometrics-database

Aughenbaugh, S. (2015). *Shaping the strategic landscape on technology for the national security enterprise.* Retrieved from http://csis.org/files/publication/150828_Aughenbaugh_ShapingStratLandscape_Web.pdf

Avant, D. (1994). *Political institutions and military change: Lessons from peripheral wars.* Ithaca, NY: Cornell University Press.

Biometrics Gets Down to Business. (2006, November 30). *The Economist.* Retrieved from http://www.economist.com/node/8312246?zid=318&ah=ac379c09c1c3fb67e0e8fd1964d5247f

Cote, O. R. (1996). *The politics of innovative military doctrine: The U.S. Navy and fleet ballistic missiles* (Doctoral thesis). Retrieved from http://edocs.nps.edu/AR/topic/theses/1996/Feb/96Feb_Cote_PhD.pdf

Defense Forensics and Biometrics Agency. (2013). *DoD biometrics enterprise architecture (integrated) v2.0 common biometric vocabulary* (CBV). Retrieved from http://www.dfba.mil/Files/Documents/References/common%20biometric%20vocabulary.pdf

Defense Science Board. (2007). *Report of the Defense Science Board Task Force on defense biometrics.* Washington, DC: Office of the Under Secretary of Defense (Acquisition, Technology, and Logistics).

Defense Science Board. (2011). *Report of the Defense Science Board Task Force on defense intelligence: Counterinsurgency (COIN) Intelligence, Surveillance, and Reconnaissance (ISR) operations.* Washington, DC: Office of the Under Secretary of Defense (Acquisition, Technology, and Logistics).

Department of Defense. (2004). *DoD detainee biometric collection processing policy.* Washington DC: Office of the Secretary of Defense.

Department of Defense. (2008). *Department of Defense biometrics* (DoDD 8521.01E). Retrieved from http://fas.org/irp/doddir/dod/d8521_01.pdf

Department of the Navy. (2012). *Marine Corps identity operations (IdOps)* (Marine Corps Order 5530.17). Retrieved from http://www.marines.mil/Portals/59/MCO%205530_17.pdf

Gelb, A., & Clark, J. (2013). *Identification for development: The biometrics revolution* [Social Science Research Network e-Library]. Retrieved from http://www.cgdev.org/publication/identification-development-biometrics-revolution-working-paper-315

Grissom, A. (2006). The future of military innovation studies. *Journal of Strategic Studies, 29*(5), 905–934.

Hill, A. (2015). Military innovation and military culture. *Parameters, 45*(1), 85–98.

Iasso, A. (2013, July 1. A critical time for biometrics and identity intelligence. *Military Intelligence Professional Bulletin*, 39–40.

Joint Chiefs of Staff. (2013). *Joint intelligence* (Joint Publication 2.0). Washington, DC: Chairman of the Joint Chiefs of Staff.

Jones, A. (2004). *AR 15-6 investigation of the Abu Ghraib prison and 205th Military Intelligence Brigade.* Washington, DC: Department of the Army.

Jontz, S. (2015). Are biometrics the new intelligence discipline? *Signal Magazine.* Retrieved from http://www.afcea.org/content/?q=Article-are-biometrics-new-intelligence-discipline

Jungdahl, A., & Macdonald, J. (2014) Innovation inhibitors in war: Overcoming obstacles in the pursuit of military effectiveness. *Journal of Strategic Studies, 38*(4), 467–499. Retrieved from http://dx.doi.org/10.1080/01402390.2014.917628

King, R. (2014). *Biometrics and national security white paper.* Biometrics Research Group, Inc. Retrieved from http://www.academia.edu/7434174/Biometrics

Kieffer, J., & Trissell, K. (2010, April-June 2010). DOD biometrics: Lifting the veil of insurgent identity. *Army AL&T Magazine,* 14–17.

McWilliams, T. S., & Schlosser, N. J. (2014). *U.S. Marines in battle: Fallujah, November-December 2004.* Retrieved from http://www.mcu.usmc.mil/historydivision/Pages/Publications/Publication%20PDFs/FALLUJAH.pdf

Murray, W. (2009). *Military adaptation in war* (IDA Paper P-4452). Alexandria, VA: Institute for Defense Analyses.

National Science and Technology Council. (2008). *Biometrics in government post-9/11, advancing science, enhancing operations*. Retrieved from www.biometrics.gov/Documents/Biometrics%20in%20Government%20Post%209-11.pdf

National Security and Market Watch. (2015). *Global biometrics market is expected to reach $44.2 billion by 2021.* Retrieved from http://www.marketwatch.com/story/global-biometrics-market-is-expected-to-reach-442-billion-by-2021-radiant-insights-2015-10-06

Partnership for Public Service. (2013). *From data to decisions III: Lessons from early analytic programs.* IBM Center for the Business of Government. Retrieved from http://www.businessofgovernment.org/sites/default/files/From%20Data%20to%20Decisions%20III_0.pdf

Pendall, D., & Sieg, C. (2014, January). Biometric-enabled intelligence in Regional Command–East. *Joint Forces Quarterly, 72*(1), 70. Retrieved from http://ndupress.ndu.edu/Media/News/NewsArticleView/tabid/7849/Article/577484/jfq-72-biometric-enabled-intelligence-in-regional-command-east.aspx

Petraeus, D. (2008). *Multi-National Force-Iraq commander's counterinsurgency guidance.* Retrieved from http://www.rs.nato.int/images/stories/File/COMISAF/15%20July%202008%20MNFI%20COIN%20Guidance.pdf

Posen, B. (1984). *The sources of military doctrine: France, Britain, and Germany between the World Wars.* Ithaca, NY: Cornell University Press.

Rosen, S. (1991). *Winning the next war: Innovation and the modern military.* Ithaca, NY: Cornell University Press.

Samuelson, W., & Zeckhauser, R. (1988). Status quo bias in decision making. *Journal of Risk and Uncertainty, 1*(1), 7–59.

Shanker, T. (2011, July 13). To track militants, U.S. has system that never forgets a face. *The New York Times.* Retrieved from http://www.nytimes.com/2011/07/14/world/asia/14identity.html?_r=0

Shontz, D., Libicki, M., Rudavsky, R., & Bradley, M. (2012). *An assessment of the assignments and arrangements of the executive agent for DoD biometrics and status report on the DoD biometrics enterprise.* Retrieved from http://www.jstor.org/stable/10.7249/j.ctt3fh0n8.11

The Eyes Have It: Biometric Data and the Afghan War. (2012, July 7). *The Economist.* Retrieved from http://www.economist.com/node/21558263

U.S. Government Accountability Office. (2011). *DoD can better conform to standards and share biometric information with federal agencies* (Report No. GAO-11-276). Retrieved from http://www.gao.gov/new.items/d11276.pdf

U.S. Government Accountability Office. (2012). *Additional training for leaders and more timely transmission of data could enhance the use of biometrics in Afghanistan* (Report No. GAO-12-442). Retrieved from http://www.gao.gov/assets/600/590311.pdf

Vann-Olejasz, S. (Personal communication, 2014-2015).

Voetelink, J. (2014) EvBO: Evidence-based operations: How to remove the bad guys from the battlefield. *Journal of International Law of Peace and Armed Conflict,* 194–201.

Biography

COL Glenn Voelz, USA, is the senior intelligence analyst on the International Military Staff at NATO Headquarters. He was previously the U.S. Army War College Fellow in the Massachusetts Institute of Technology (MIT) Security Studies Program and at MIT's Lincoln Laboratory. He is a graduate of West Point and holds advanced degrees from the University of Virginia and the National Intelligence University.

(E-mail address: voelz.glenn@hq.nato.int)