TECH INSIGHTS

BIOMETRICS AND THE CONNECTED SOLDIER

—

WHAT'S WORKING, WHAT'S COMING AND WHY

The appearance of U.S. Department of Defense (DoD) visual information does not imply or constitute DoD endorsement.

A GROWING MARKET FOR BIOMETRIC-BASED INSIGHT

Biometric sensors are everywhere – on smartwatches and rings, in hospitals, at airports and warehouses, in automobiles and even in door locks. A biometric sensor is a device which converts a biometric attribute of a person (facial image, fingerprint, body temperature, heart rate, or many others) into a digital signal. Because biometrics can provide reliable information about individual identity and physical status, these sensors have implications for intelligence collection and other military operations.

Technical progress and pandemic-generated needs for remote biometric data have combined to create a growing market for wearable biometric devices. Demand for biometric sensors has surged as biometric sensors have become more capable and affordable. Global demand for biometric sensors of all types is growing, with some estimates[1] describing the global market size over $3B by 2030, with annual growth rates exceed 11%.

SOLDIER BIOMETRICS: MORE CONNECTIONS, MORE CAPABILITY, MORE RISK

American military use of soldier-level biometrics started in Kosovo in 2001 and expanded during the conflicts in Afghanistan and Iraq with systems intended to improve identification of detainees and other people encountered during force protection screenings. Since then, military biometric technology has become more capable, with devices now able to collect more data, and connected with artificial intelligence platforms. At the same time, the early risks associated with large scale biometric data collection have expanded, and now constrain wider applications of biometric data.

Biometrics for Identity: Who Are You?

Early military biometric technology was not wearable but was carried by operational units. Known as the "Biometrics Automated Toolset – Army" (or "BAT-A"), this system collected biometric identification data – fingerprints, iris images and a facial image – and maintained this data in a centralized, searchable database. **(IMAGE 1)** The BAT-A system included a hand-held device for collecting data, called the Handheld Interagency Identity Detection Equipment

(HIIDES). BAT-A and HIIDES were developed to allow military units to create national-level identification systems that could not be forged or evaded.

But this early use of biometrics to answer the question "Who are you?" had two critical flaws. First, the systems were cumbersome and often produced only partial or unusable data, especially when operated in field environments. Second, the huge national biometric databases could be exploited if they were stolen or hacked. This proved fatal in Afghanistan, when the Taliban used captured biometric collection hardware and biometric data to identify and then assassinate people who had worked for the Afghan government[2]. This event and others like it led to the European Union's General Data Protection Regulation[3] which prohibits processing biometric data for uniquely identifying an individual. Similar policies have been enacted in the United States, and the US Defense Department policy on biometrics now focuses on the rules for collecting, storing and sharing biometric data to ensure security and privacy of soldier-collected biometrics[4].

Biometric data collection continues to be part of the military and law enforcement capability set for intelligence operations. The US recently launched the "Next Generation Biometric Collection Capability" program[5] which will be capable of operating on multiple communications networks and achieve near real-time identity matching and data synchronization.

Biometrics for Health and Fitness: How Are You?

The COVID-19 pandemic led to significant investment by medical device companies in wearable devices to monitor patient vital signs, including respiration, heart rate and other variables. These developments led to military programs to adapt wearable biometrics for assessing soldier health and fitness.

In 2020, the Defense Threat Reduction Agency (DTRA) developed the "Rapid Assessment of Threat Exposure (RATE) Program[6]" – the first combination of soldier-wearable biometrics and artificial intelligence (AI) to assess soldier health and answer the question "How are you?" during the pandemic.

Unlike the BAT-A program, RATE uses commercial wearable biometric sensors (including smart watches and rings) to collect soldier data. The soldier data is processed through an AI algorithm that was trained using hospital data collected during the COVID pandemic and detects if the soldier is infected with the COVID-19 virus. After an early success, the program has been extended to more than 4,500 soldier users and has added capabilities to monitor overall health and vital signs.

The RATE program's use of commercial biometric wearables and civilian hospital data is similar to wearable biometric sensor programs used in the National Football league and other professional sports. Moving data from a soldier or athlete into an artificial intelligence system for analysis and reporting simply reflects the emerging ability of AI systems to create insights from small wearable devices.

But just as the BAT-A biometric data could be exploited, data privacy and security concerns have emerged around systems like RATE-A. Professional athletes raised legal concerns about the ownership and use of their biometric data, and it is now illegal to sell or use player biometric data in contract negotiations or for other purposes[7]. Military users may raise the same concerns about using their biometric data in promotion or retention boards or for other personnel actions.

Biometrics for Operational Effectiveness: Are You Mission-Ready?

Recent Army experiments have begun to test how soldier-worn biometric sensors can help commanders better understand the health status of units in operational environments. A Wearables Pilot program was included in Exercise TALISMAN SABRE 23, to merge wearable sensor data into a single architecture and network, allowing leaders to see the health readiness of many units operating across a widely dispersed battlefield[8]. Tank and infantry companies were equipped with single-lead electrocardiogram patches and smart watches, allowing multiple biometric variables to be collected and reported in real-time to a central platform. Because tanks also have GPS reporting systems, unit commanders could see soldier health conditions combined with location data, allowing triage and treatment for heat injuries and other conditions. Data from TALISMAN SABRE is under evaluation, and future applications of wearable biometrics will be decided based on this test data.

WHAT'S NEXT FOR SOLDIER-WORN BIOMETRICS?

TALISMAN SABRE 23, RATE and commercial applications of wearable biometric sensors in professional sports point the way for future development of soldier biometric systems.

These systems are moving beyond identity management and security applications, toward advanced management of individual and unit fitness, health and readiness.

Technology Drivers Create Possibilities…

As shown by TALISMAN SABRE and the RATE experiments, wearable biometric sensors are becoming smaller, less intrusive and easier for soldiers to wear. Because medical applications – not only military – are driving sensor development, the trend toward smaller, lighter and less expensive sensors is likely to continue.

At the same time, larger data sets are building around these sensors. Large-scale sports team physical databases, hospital-generated databases related to disease and injury experience, and military fitness and readiness data are now available for training artificial intelligence systems. These systems can help both individuals and commanders interpret and apply data from soldier-worn sensors.

Taken together, the knowledge and analytical power of soldier-worn biometric sensors and artificial intelligence can create new insights and enable decisions in ways that cannot be fully foreseen today. At the same time, significant limitations appear likely to constrain increased use of biometric data in military settings.

…While Practical Constraints Must Be Addressed

Biometric sensors are advancing rapidly because of the medical and commercial potential of these devices. Aside from limited funding for soldier biometrics, adoption of these systems appears likely to face four important constraints[9]:

DOES THE SENSOR COLLECT USEFUL DATA?

Before committing to a specific commercial biometric wearable, the accuracy and usefulness of the data must be evaluated. Sampling rates, data types and collection methods must match the operational environment. A sensor that works well in a hospital or clinical setting may not generate useful data in a military training or operational environment.

WILL SOLDIERS ACCEPT THE DEVICE?

Apart from privacy concerns, soldiers may experience wearable biometric sensors as uncomfortable, intrusive or inconvenient. Advanced technology is not always accepted by the military user community. The Army's Hololens-based Integrated Visual Augmentation System (IVAS) was rejected by soldier-users because they were so uncomfortable that they imposed "mission-affecting physical impairments[10]" including neck pain and nausea.

HOW WILL BIOMETRIC DATA BE SECURED AND MANAGED?

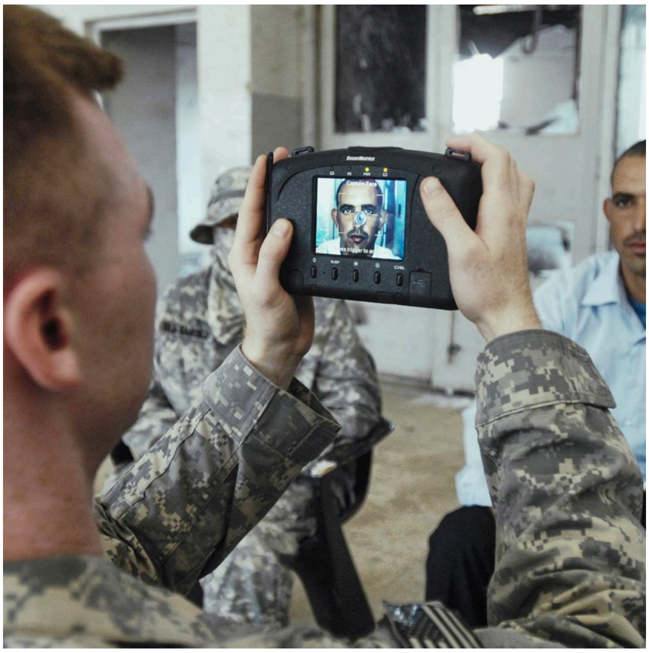
The legal and policy constraints on centralized biometric databases have already re-shaped the management and security practices applied to biometric databases. Future soldier-worn systems raise new issues of privacy and data security because they will contain personally-identifiable health information that is considered to be the property of the user.

But to be effective for unit-level analysis, a soldier-worn biometric system must share this data and include it in machine-learning databases. Developers will need to balance privacy and data security concerns against operational needs in future systems.

ARE BIOMETRIC INSIGHTS VALUED BY COMMANDERS?

The most difficult challenge may be to convince commanders that soldier-worn biometrics can generate useful operational information. TALISMAN SABRE demonstrated that user-worn biometrics are technically feasible, but commanders may prefer more traditional methods of assessing soldier welfare.

The Army's handbook for mission command emphasizes that the commander's responsibility includes personally assessing soldier readiness and overall condition through inspections and effective use of the chain of command[11]. Biometric data may, or may not, be viewed as an effective tool for undertaking this important command responsibility. If the technology is not embraced by commanders, it will not be used.



The appearance of U.S. Department of Defense (DoD) visual information does not imply or constitute DoD endorsement.

IMAGE 1: US Soldiers operating biometric screening system.

Part of Conextivity Group

YOUR PARTNER FOR SOLVING BIOMETRIC CONNECTIVITY CHALLENGES

Making the power and data connections that enable digital transformation is the core skill of the Conextivity Group, of which Fischer Connectors is part. From simple, reliable connectors and cables designed to meet strict military requirements and tactical hubs that connect sensors and minimize the soldier's physical burden, to advanced microelectronic solutions that optimize the performance of sensors and soldier-worn devices on military networks, the Group provides real solutions for the "Connectivity Challenge" facing today's commanders. Conextivity has the **innovation skills** to capture the military advantages of biometric technology, the **agility** to work on accelerated Army timelines, and the rigorous **attention to detail** in design and manufacturing to meet the most stringent Army requirements.

FISCHER CONNECTORS EXPERTS

Olivier THORMANN – Defense Product Leader

Xavier BIZE – Lead Software Engineer, Defense Products

Tomislav HAJAK – Lead Hardware Engineer, Defense Products

For any requests or further information, please send an email to o.thormann@fischerconnectors.ch

SOURCES

1. https://www.alliedmarketresearch.com/biometric-sensor-market
2. https://tolonews.com/afghanistan/taliban-used-biometric-system-during-kunduz-kidnapping
3. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679&qid=1632725403326
4. The policy is set forth in DoD Directive 8521.01E; described at: https://www.fedweek.com/armed-forces-news/army-establishes-new-biometrics-program
5. https://www.dacis.com/budget/budget_pdf/FY20/RDTE/A/0307665A_250.pdf
6. https://www.defense.gov/News/News-Stories/Article/Article/3377624/dod-investing-in-wearable-technology-that-could-rapidly-predict-disease
7. https://www.sportsbusinessjournal.com/Journal/Issues/2022/08/01/In-Depth/Biometrics.aspx
8. https://www.jpeocbrnd.osd.mil/Media/News/Article/3493550/1st-armored-division-participates-in-talisman-sabre-wearables-experiment
9. Some of these constraints are identified in: https://www.usni.org/magazines/proceedings/2023/october/challenges-wearable-technology
10. https://taskandpurpose.com/news/army-ivas-goggles-headaches-nausea-neck-pain
11. See for example: https://irp.fas.org/doddir/army/adrp6_0.pdf