Revealed: U.S. Military's Massive Biometric Data System

The U.S. Military is heavy-laden with Technocrats bent on collecting data for the sake of social engineering. Their rapidly growing global dragnet now contains images, fingerprints and DNA data on 7.4 million people. TN Editor

Over the last 15 years, the United States military has developed a new addition to its arsenal. The weapon is deployed around the world, largely invisible, and grows more powerful by the day.

That weapon is a vast database, packed with millions of images of faces, irises, fingerprints, and DNA data — a biometric dragnet of anyone who has come in contact with the U.S. military abroad. The 7.4 million identities in the database range from suspected terrorists in active military zones to allied soldiers training with U.S. forces.

"Denying our adversaries anonymity allows us to focus our lethality. It's like ripping the camouflage netting off the enemy ammunition dump,"

wrote Glenn Krizay, director of the Defense Forensics and Biometrics Agency, in notes obtained by *OneZero.* The Defense Forensics and Biometrics Agency (DFBA) is tasked with overseeing the database, known officially as the Automated Biometric Information System (ABIS).

DFBA and its ABIS database have received little scrutiny or press given the central role they play in U.S. military's intelligence operations. But a newly obtained presentation and notes written by the DFBA's director, Krizay, reveals how the organization functions and how biometric identification has been used to identify non-U.S. citizens on the battlefield thousands of times in the first half of 2019 alone. ABIS also allows military branches to flag individuals of interest, putting them on a so-called "Biometrically Enabled Watch List" (BEWL). Once flagged, these individuals can be identified through surveillance systems on battlefields, near borders around the world, and on military bases.

The presentation also sheds light on how military, state, and local law enforcement biometrics systems are linked. According to Krizay's presentation, ABIS is connected to the FBI's biometric database, which is in turn connected to databases used by state and local law enforcement. Ultimately, that means that the U.S. military can readily search against biometric data of U.S. citizens and cataloged non-citizens. The DFBA is also currently working to connect its data to the Department of Homeland Security's biometric database. The network will ultimately amount to a global surveillance system. In his notes, Krizay outlines a potential scenario in which data from a suspect in Detroit would be run against data collected from "some mountaintop in Asia."

The documents, which are embedded in full below, were obtained through a Freedom of Information Act request. These documents were presented earlier this year at a closed-door defense biometrics conference known as the Identity Management Symposium.

ABIS is the result of a massive investment into biometrics by the U.S. military. According to federal procurement records analyzed by *OneZero,* the U.S. military has invested more than $345 million in biometric database technology in the last 10 years. Leidos, a defense

contractor that primarily focuses on information technology, currently manages the database in question. Ideal Innovations Incorporated operates a subsection of the database designed to manage activity in Afghanistan, according to documents obtained by *OneZero* through a separate FOIA request.

These contracts, combined with revelations surrounding the military's massive biometric database initiatives, paint an alarming picture: A large and quickly growing network of surveillance systems operated by the U.S. military and present anywhere the U.S. has deployed troops, vacuuming up biometric data on millions of unsuspecting individuals.

The military's biometrics program, launched in 2004, initially focused on the collection and analysis of fingerprints. "In a war without borders, uniforms, or defined lines of battle, knowing who is an enemy is essential," John D. Woodward, Jr., head of the DoD's biometrics department, wrote in a 2004 brief.

That year, the Department of Defense contracted Lockheed Martin to start building a biometrics database for an initial fee of $5 million. Progress was slow: by 2009, the DoD Inspector General reported that the biometrics system was still deeply flawed. The department indicated that it was only able to successfully retrieve five positive matches from 150 biometric searches. A later contract with defense industry giant Northrop resulted in similarly disappointing results with reports of "system instability, inconsistent processing times, system congestion, transaction errors, and a 48-hour outage."

By 2016, the DoD had begun to make serious investments in biometric data collection. That year, the Defense Department deputy secretary Robert O. Work designated biometric identification as a critical capability for nearly everything the department does: fighting, intelligence gathering, law enforcement, security, business, and counter-terrorism. Military leaders began to speak of biometric technology as a "game changer," and directives from the DoD not only encouraged the use of the technology by analysts, but also by soldiers on the ground. Troops were instructed to collect biometric data whenever possible.

The same year, a defense company named Leidos, which had acquired a large portion of Lockheed's government IT business, secured a $150 million contract to build and deploy what is now known as the DoD ABIS system.

Read full story here…