

Special Report

Greatest Hits, Unfortunate Misses

November 2008

By National Defense Staff

Biometrics

Using attributes of the human body to identify crime suspects has been a law enforcement tactic for more than a century.



Until recently, fingerprints and mug shots were the means most employed to identify individuals, but today voice recognition, palm prints, vein and iris patterns and even DNA have been thrown into the mix. An added bonus is the digital revolution that makes collecting, storing and transmitting biometric data easier than ever.

Biometrics-based sensors and data-mining systems have been welcome by the U.S. military in Iraq, where insurgents hide among the population and separating friend from foe is tough business.

Some Iraqi villagers have submitted to fingerprint and iris scans to create secure identity cards so they can keep strangers out of their towns.

Special operators and other covert teams are coupling biometric with forensic science to take down bomb-making networks. Using a 22-pound kit designed by **Cross Match Technologies**, they can enter a suspect's house, take his fingerprints — or lift latent fingerprints if no one is there — and transmit them back via a small satellite dish to a massive database in West Virginia.

The goal is to find out if the fingerprints match within 15 minutes. More often than not, operators receive responses in as little as four minutes, said Konrad Trautman, an intelligence expert at U.S. Special Operations Command.

The kits have helped teams capture or kill an average of two bombmakers per day during the last two years, he said. "How many bombs would have been made by those individuals?" he asked.