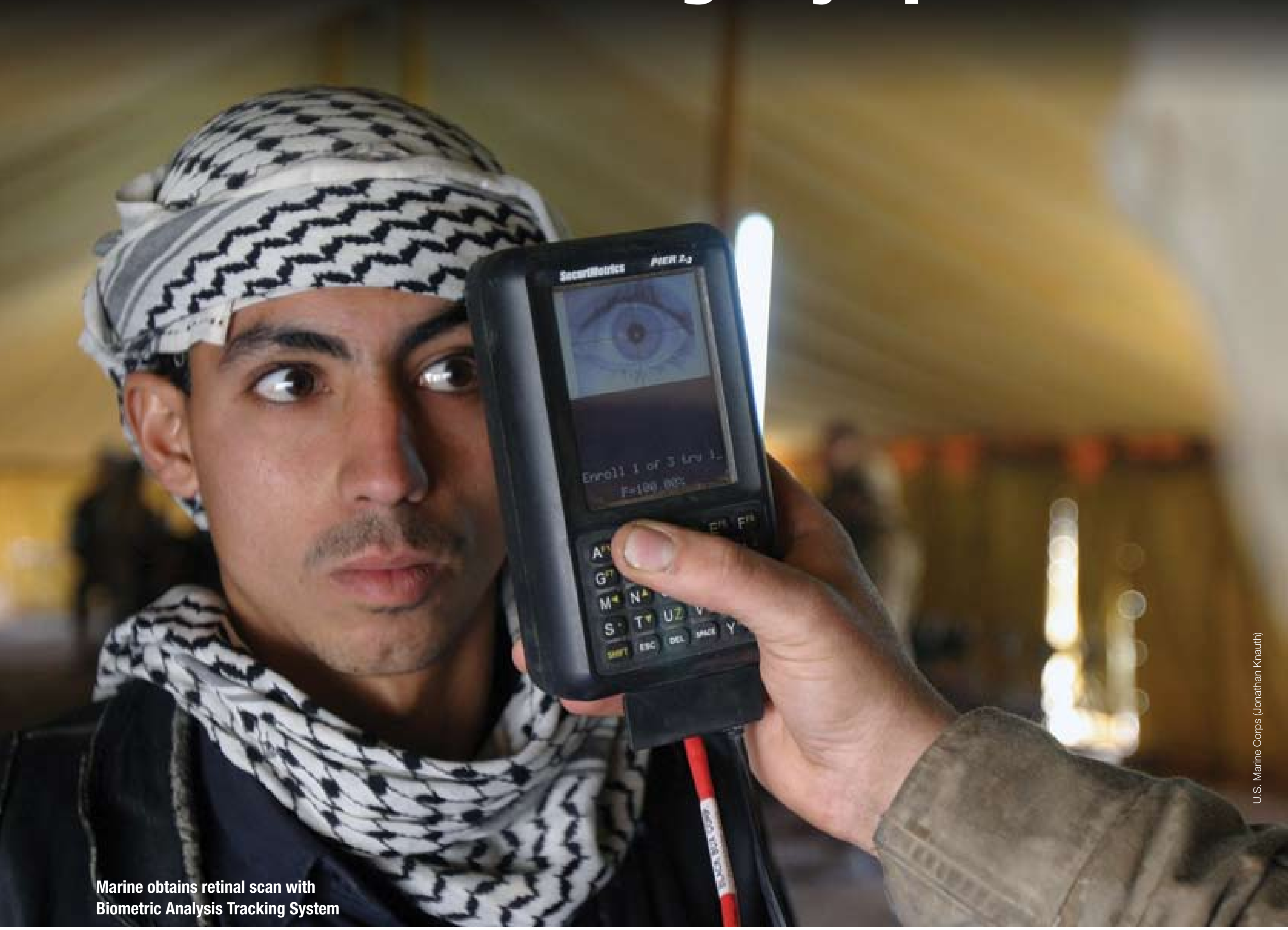
Applying Law Enforcement Technology to Counterinsurgency Operations



Marine obtains retinal scan with Biometric Analysis Tracking System

U.S. Marine Corps (Jonathan Knauth)

By GILES KYSER, MATT KEEGAN, *and* SAMUEL A. MUSA

Colonel Giles Kyser, USMC, is Military Assistant to the Assistant Secretary of Defense for Special Operations and Low Intensity Conflict. Matt Keegan is a Visiting Fellow in the Center for Technology and National Security Policy (CTNSP) at the National Defense University (NDU). Dr. Sam Musa is Senior Research Fellow in CTNSP at NDU.

In 1994, Rudolph Giuliani assumed duties as the mayor of New York, taking over a city with one of the highest crime rates in America—a problem he promised to address. To meet this challenge, he expanded the number of police officers on his force, surged them to neighborhood beats, and enabled them to overcome unfamiliarity with the local geography and demography by arming them with information technology solutions, providing each beat cop with a type of "virtual longevity" normally requiring months to develop.[1]

Half a decade later, a similar situation faced the Chicago Police Department. Chicago also leveraged information technology effectively, surging the "equivalent of 300 officers on the street."[2] The Chicago system, the Citizen and Law Enforcement Analysis Reporting (CLEAR) system, created this "virtual surge" and arguably contributed to an unprecedented drop in violent crime within Chicago. At the time (October 2005), the *Chicago Sun-Times* noted that "Chicago officials and academics have credited the city's murder decline to police targeting of gangs, drugs, and guns."[3]

The parallels between the problems experienced by two major cities where gang violence, organized crime, and illicit financing overwhelmed local security forces, and the challenges facing our coalition forces in Iraq, are striking—as is one potential tool to address those challenges.

In 2007, Iraq and Afghanistan find themselves torn by insurgency, sectarian violence, and terrorism. Instead of gang violence, warlords, tribes, sectarian death squads, and terrorist cells dominate urban landscapes akin to New York and Chicago. Instead of drugs alone, terrorist financing includes narcotics, extortion, and highly developed financial networks using porous borders and symbiotic affiliations to protect major actors. Instead of just guns, the forces arrayed against the coalition include improvised explosive devices and heavy weapons. In an especially chilling development, insurgent efforts not only continue but also increasingly extend across the borders between the two countries where thugs, terrorists, and opportunists support the chaos serving as a foundation for their individual causes.[4]

In this violent no man's land between those contending for power sit our forces and the Iraqi populace whom we have sworn to protect. Our rotating, shifting, and surging forces are unable to develop their situational awareness rapidly enough to penetrate the insular demographic within which the terrorist operates, and the Iraqi people are unable to expose the enemy from within that demographic. The terrorists swim within familiar waters, not as another fish—as Mao might describe—but as predators ready to devour anything threatening their existence.

Background

Two key phrases mentioned above comprise the foundation for potential crossover of police techniques into counterinsurgency operations: *insular demographic* and *situational awareness* (SA). For the Solider in Al Anbar and the cop in Chicago, the ability to peer through the insular demographic—to know who is who, who belongs, and who does not; to see through disguises or aliases—unlocks the door to basic security. Similarly, strong situational awareness—the ability to recognize the presence of the abnormal or absence of the normal—provides an indispensable and intuitive warning mechanism.

A closer look at four factors preventing our forces from developing the intuitive and concrete sensing necessary to penetrate an enemy's defenses lends to understanding why law enforcement technology may provide a unique solution.

Force Rotation. Without technical enhancements, units require 30 to 60 days of consistent presence to develop comprehensive SA in an area in order to gauge conditions, patterns, and personalities for intuitive force protection and defensive operational effectiveness. Exploiting that SA in an offensive manner requires longer periods within one region. According to Servicemembers recently returned from in-theater, force rotations within a specific region vary from as short as 8 to 10 weeks to as long as a full rotation, depending on conditions on the ground and the requirement to reinforce success or

parallels between the problems experienced by two major cities, where gang violence, organized crime, and illicit financing overwhelmed local security forces, and the challenges facing coalition forces in Iraq, are striking

Iraqi police discuss daily patrol

1st Combat Camera Squadron (Andy Dunaway) prevent failure—as in Baghdad today, where forces from other parts of the country moved to the capital to saturate the area of operations. Fire brigade operations such as this within a region will predictably result in some degree of defensive SA but will arguably fall short of the offensive SA necessary to challenge the enemy.

Demography/Language Unfamiliarity. Even after developing intuitive capabilities and a degree of SA, coalition forces' inability to speak the language and discern nuances of demographic patterns limits the discriminative application of force contributing to winning over the populace. In other words, a local will know by accent, dress, or actions that someone is not from that area. Accordingly, unless teamed with a local, trusted, and uncorrupted informant network or an attached military translator, coalition forces will have little to no idea who they are encountering, and the enemy will be able to continue to hide in plain sight and intimidate those they draw their anonymity from while friendly units inadvertently offend, inconvenience, and humiliate potential allies.

Insurgent/Terrorist Mobility. Highly porous borders between Iraq and Afghanistan and their respective neighbors, combined with interprovince mobility and geographic tribal striations, significantly challenge coalition force capability to limit movement of terrorist/insurgent forces. Internal examples such as residents of Mosul arrested in Takrit, of Afghani fighters in Iraq, or even the arrest of a foreign fighter once detained on the Afghanistan-Pakistan border in the United States highlight the problem coalition forces face every day.[5]

Detainee Movement Requirements. Following the Abu Ghraib incident, political pressures created the impetus for the implementation of new detainee transfer processes. Unless significant reason is established at the battalion level permitting extended interrogation, detainees must transfer to the next higher echelon facilities within a short time. Command policy sets that period, and the enemy remains well aware of it by virtue of information gathered from those released. Currently employed technology does not allow the squad/checkpoint to have a clear detain/do not detain choice because certain technology only exists at the battalion level and higher, and even then only through cumbersome processes with latency constraints. Squad/checkpoint level confirmation, aside from a lucky hit on a watch list, is rare. The operational requirements of such immediate transfer, and the limited insight into detainee history at the point of encounter (the checkpoint or arrest point), effectively limit actual opportunities for detainee interrogation and information exploitation to only that which is gathered beyond the 18-hour window. Discussions with regional veterans indicate that the aforementioned limitations are known by the insurgents, terrorists, and criminals.

With this knowledge, insurgents, terrorists, and criminals understand that waiting the prescribed period closes the coalition force's limited window of opportunity to exploit their capture. The window closes because informal and formal communications methods warn a detainee's associates, who then "go to ground." The highly perishable intelligence that a detainee may possess decays by the time higher headquarters interrogates the suspect. More importantly, those within the detainee's network go into hiding as the fact of detention becomes apparent. In effect, the process cycle time itself suboptimizes the coalition forces' ability to act on perishable intelligence.

Having examined the four factors preventing friendly ability to develop situational awareness in an offensive manner, we need to look at solutions that might help overcome those constraints. Police methods such as those used in Chicago could assist our forces in executing missions in Iraq and Afghanistan, but for this analysis, we focus on a simple police information technology solution. Biometric technology attached to a transactional database utilizing existing communications infrastructure could create a virtual surge extending the effectiveness of the individual warrior or policeman and lifting the burden of exposing the terrorist from the populace. Biometrically exposing an enemy heretofore invisible to the Western eye and protected by those around him whom he intimidates into silence offers the way to penetrate the insular demographic. Such a police solution could help to create a more secure environment for the Iraqi and Afghan people.

A Northrop Grumman proprietary system—the Biometric Automated Toolset (BAT)—provides the foundation for a technological enhancement to the current environment in Iraq and Afghanistan. However, BAT currently is not available at the checkpoint/squad level, so important information is not in the hands of those who need it most: the Soldier or Marine on the checkpoint. Conversely, when one considers systems such as the one currently used in Chicago, the technological answer seems simple. But we must examine whether such successfully applied capabilities can overcome encounter-point demographic challenges, as well as the constraints imposed by rotation-driven SA

> *perishable intelligence that a detainee may possess decays by the time higher headquarters interrogates the suspect*

Soldier enters data gathered from patrol with Iraqi police

982d Combat Camera (Tierney Nowland)

limitations, insurgent and terrorist mobility, and detainee movement requirements.

Because many of the tactical level operations currently conducted by coalition and Iraqi forces more closely resemble police work than traditional warfighting, adopting police techniques may help overcome stability and support operations problems. The conventional force-on-force operations for which the world's (and our) militaries were designed ended within months in Afghanistan and Iraq, and force requirements migrated toward constabulary and counterinsurgency capabilities. Many conventional units found themselves functioning in a police role for which they were untrained and ill equipped. Likewise, Iraqi security forces (to include police), whose local knowledge and cultural familiarity provide instant SA, cannot yet assume full responsibility for such operations. Consequently, coalition forces continue to conduct nontraditional, nonconventional missions within a culture whose willingness to accept policing by outsiders is problematic at best.

CLEAR and Associated Techniques

Juxtaposing this background with the success of the Chicago Police Department initiative drives our problem statement: How can the integration of police database and biometric identification capabilities improve stability and support operations in Iraq and Afghanistan?

Modern American metropolitan police forces leverage information technology to overcome deficiencies in actionable intelligence when prosecuting law enforcement operations against gangs, drug cartels, and other organized crime. Biometric identification—using high-resolution hand, facial, or retinal scanning—eliminates the criminals' ability to disguise their identity regardless of demographic background or to fool captors. The complementary use of police systems and biometric scanning capability at the tactical level (squad), associated with appropriate sub-battalion level authorities and thresholds for action, will create conditions that will mitigate many limitations and act as a force multiplier for friendly units in exactly the same fashion as it has for U.S. law enforcement organizations. Such a capability, if deployed with patrolling formations, could be left with Iraqi security forces for continued use to ensure little loss of continuity once American forces begin to reduce their presence.

coalition forces continue to conduct nontraditional missions within a culture whose willingness to accept policing by outsiders is problematic at best

The Chicago Police Department's CLEAR is an example of the type of processes and technology that could enable friendly forces to enhance regional security. It comprises a database/data correlation/data mining/knowledge system based on Oracle's commercially available 9i database and the associated 9i Developer suite. It combines with a front-end biometric collection capability enabling the rapid collection, determination, and dissemination of detainee information. CLEAR utilizes commercial-off-the-shelf (COTS) software and links to multiple national identification databases such as the Federal Bureau of Investigation (FBI) Integrated Automated Fingerprint Identification System (IAFIS), which represents a proven technology in daily use with the Chicago Police Department.

Military Police dog searches for explosives in Iraq

30th Space Communications Squadron (Molly Dzitko)

A key element distinguishes CLEAR from prior systems to include BAT. Specifically, CLEAR operates/associates automatically. Predecessor systems operated in a "push" method requiring operators to take collected information and push data files manually to selected databases. Once the data arrived at the next database location/next step in the workflow, manual matching added up to 48 hours to the cycle time. Transactional design allows CLEAR to perform information retrieval, link analysis, file updates, and synchronization automatically without human intervention. This permits cycle times as low as 3 minutes from the point of encounter to the database and then back to the point of encounter while simultaneously increasing the overall accuracy and timeliness of the information.

The arrest-to-booking process constitutes CLEAR's most pertinent function to squad level operations at encounter points (whether conducting checkpoints or detaining personnel during raids or sweeps). For Chicago, using Crossmatch Technologies MV–100 as the biometric collection device, and Computer Deductions, Inc., software, an officer (or a Soldier) can collect various forms of identification from an individual. The form of identification can be any combination of inputs or a single input ranging from swiping identification cards and hand-typed information to real biometric inputs such as (facial) photographs and fingerprints (up to 10 if in concert with Homeland Security Presidential Directive 11).

Once inputs are gathered, the handheld unit transmits the information to the squad car (or Humvee), which then transmits it to higher headquarters and to databases within the FBI, such as IAFIS. Data arrival triggers transactional automatic scans of an Oracle database mining for any pertinent data on the detainee such as ticket history, fines, outstanding warrants, aliases, physical markings (such as tattoos), a list of known associates, a mapping of any crimes committed, and a multitude of other essential data points. Automatically, the data transmit back down the chain to the MV–100 within 3 to 5 minutes, enabling the officer (or Solider) to act accordingly.

Simultaneous with the transactional process, data collection continuously expands the known data universe. Much of the information gathered every day links into the data analysis tool, permitting scrutiny of daily information and development of key statistics easily portrayed through reports or overlaid onto maps. These reports and maps permit higher headquarters to evaluate near real-time intelligence associated with changing criminal activities and make appropriate force adjustments as needed—much like our units in Iraq do with far less sophisticated data. The Chicago Police Department used this to track organized crime, gang-related violence, and crime patterns in a manner that had the same effect as surging hundreds of officers onto the street. It is obvious that the technology and proven methods used in Chicago apply similarly to military decisionmakers tracking shifting patterns of terrorist, insurgent, or sectarian violence in-theater.

Civilian police train in riot control techniques

2d Communications Squadron (Joanna Kresge)

At the squad level, rapidly understanding a detainee's true identity, the threat revealed by that identity, known associates, and the areas in which he operates could trigger proactive responses. Most importantly, immediate, verifiable information provides the foundation allowing our forces to retain the initiative to a greater degree than before. That initiative arguably will prevent a predictable response that often constitutes the first step in a complex ambush. Moreover, instead of waiting 18 hours for transport to higher headquarters, the response from the system (BAT) at that level, subsequent interrogation, and manual cross-matching of data, a sub-battalion level unit could rapidly act on perishable intelligence that links the detainee to known associates located in the same vicinity. "Pulling the strings" associated with such links allows friendly forces to roll up enemy networks that previously would use their cultural anonymity to hide in plain sight.

At the higher headquarters level, the inputs from a CLEAR-like system could further populate the BAT system (as well as the Defense Department's Automated Biometric Identification System [ABIS] database and the FBI's IAFIS database to assist in global counterterror operations) while generating daily analysis of field actions. This daily intelligence enables rapid redeployment to head off notable trends in insurgent redeployment as noted by detainee history from a particular area. Automated pattern presentations and superior communications among coalition forces would allow the forces to act well within the insurgents' decision cycle and force them to reconsider, change, or cancel operations to a degree only previously achieved by physical saturation of an area because they will need to expend greater resources on their own force protection.

Theory to Practice

Until recently, using a CLEAR-like system to support the arrest-to-booking process in the U.S. Central Command theater at the squad level only begged the question: *Can it work in practice?* The answer is most definitely *yes*. As depicted in the February 8, 2007, *Wall Street Journal* article entitled "Snake Eater," a subset of the CLEAR system saw action in Iraq and not only proved its direct impact on mapping human terrain, but also provided an undeniable psychological effect on a previously burgeoning insurgency.[6] Major Owen West, USMC, brought an MV–100 and COPLINK loaded on a personal computer into the Khalidaya area just north of Baghdad. From one night of operations, not only did Major West succeed in applying the MV–100 and COPLINK, but he also executed a psychological operation that made the insurgent reconsider where he was operating. Major West's replacement continues to employ the Snake Eater subset of CLEAR, while a second front saw the field testing of the system's complete functionality. From February 26 to March 1 at Camp Roberts, California, the Tactical Network Topology exercises tested CLEAR system architecture. The test assessed the ability of a CLEAR-like system (communication architecture with a layered database) to produce actionable intelligence during Marine Corps Snap Vehicle Checkpoint operations. Multiple scenarios tested the system. First, at checkpoints manned by special operations personnel, the specially configured MV–100 personal digital assistant (PDA) was used to take two fingerprints, a mug shot, and other demographic data. There were two options, Full Encounter ID or Fast ID. Major West and his squad used these same options and configurations as part of transition training for an Iraqi brigade in the Al Anbar province.

In the Camp Roberts exercise, the PDA had a limited number of records stored in the device for potential initial matching. If there was no match, the data transmitted to

automated pattern presentations and superior communications would allow coalition forces to act well within the insurgents' decision cycle and force them to reconsider, change, or cancel operations

MP shows Iraqi police officer how to use database

Fleet Combat Camera (Jeremy Wood)

a relay vehicle or Humvee, and the data then transmitted to the Tactical Operations Center and the second match took place at the server (laptop). The server had the database of the local population. The data then transmitted via virtual private network to the Biometric Fusion Center for access to the ABIS emulator database resident in the FBI's Clarksburg, West Virginia, center (home of IAFIS and ABIS). The center constituted a test database to prove capability while protecting the security of the real ABIS. The response from the ABIS emulator (match or no match plus additional data) retransmitted to the server at the Tactical Operations Center. All the information returned then to the PDA for action.

A battlefield medical scenario and a full blue-red force scenario with checkpoints established at the recommendation of the Tactical Operations Center comprised additional tests for the CLEAR-like system. Furthermore, CLEAR successfully integrated with Tacticomp,[7] which constituted the relay communications from the vehicle to the Tactical Operations Center for the latter scenario. The system continued to work well. This Tacticomp system is available in a number of the Humvees and will provide added capability to the Hand-held Interagency Identity Detection Equipment system (the PDA addition to BAT). The key point is that the Tacticomp infrastructure exists in Humvees today and comprises a proven link for the CLEAR subsystem, obviating the need for additional equipment installation in already cramped vehicles.

The response times for Fast ID from data entry at the MV–100 PDA to the ABIS emulator and back ranged from 1 minute 28 seconds to 2 minutes 47 seconds. For the Full Encounter ID, the response time ranged from 2 minutes 16 seconds to 3 minutes 35 seconds. All of these times include the time it takes to enter the data on the PDA, which ranged from 37 seconds for Fast ID to 1 minute 25 seconds for Full Encounter ID. The system provided fast response based on a single fingerprint as well as a single facial print. The special operations personnel took these measurements at the checkpoint and developed valuable feedback. This connectivity to the ABIS emulator and ultimately the real ABIS system will provide valuable information on insurgents in theater to Major West's replacement and that unit's associated Iraqi brigade. Moreover, their operations will exploit the more complete functionality of CLEAR.

The significant advantage of the CLEAR-like system is that it does not require secret-level, Secure Internet Protocol Router (SIPR) connectivity and therefore can remain with our coalition partners without concern over security. At some time in the future, this system will complement the existing BAT system and its SIPR connectivity and database and expand U.S. force capabilities through simple connectivity integration. Simultaneously, the system will retain its unclassified capability, enabling use by allied forces or members of the law enforcement community without SIPR access. This integration will incorporate the existing databases into one overall architecture that may be able to provide solutions to the squad-level Soldier and the beat-level police officer as both protect and serve.

the CLEAR-like system does not require Secure Internet Protocol Router connectivity and can remain with coalition partners without concern over security

Recommendations

Enabling the warfighter with proven law enforcement COTS technology to complete nontraditional constabulary/policing missions defines the ultimate objective. Taking a proven solution from the streets of Chicago, testing it for battle-readiness, and rapidly integrating it with existing solutions (that is, BATS and IAFIS) may be a way of spreading the small scale success that Major West had in Khalidaya across the region. No matter which system is selected, the key tenets of the path forward should be to:

- avoid confusing biometric collection capability/equipment with the essential heart of the solution, which is the database, data mining, knowledge management system that turns biometric data into actionable information without relying on human intervention
- investigate incorporating best practices in police database/information technology and associated processes into ongoing squad level operations in Iraq and Afghanistan
- populate and integrate all known criminal databases to enable all counterterrorist and law enforcement agencies to overcome terrorist demographic and mobility challenges
- test CLEAR or other similarly mature law enforcement COTS solutions in Iraq and Afghanistan
- integrate as a complementary solution to BAT (with its SIPR access), while keeping a CLEAR-like, nonsecure Internet solution segregated for use by Iraqi forces once coalition forces redeploy
- use the capability placed in Iraq and Afghanistan as a feeder for U.S.-based systems, thereby enabling another level of domestic capability to protect the United States.

After 8 years in office, Mayor Giuliani saw a dramatic drop in crime by applying his theories on countering crime in New York.[8] With 4 years already behind us in Iraq, and public opinion leaning toward a significant reduction in U.S. forces engaged there, a proven law enforcement force multiplying tool that could enhance counterinsurgency and counterterrorist activities as our troops try and police the region should be applied. The major similarity that the Giuliani situation has to Iraq is that time, money, and force levels all are stressed. Instead of losing time by recreating existing COTS capability, why not take a lesson from the streets of Chicago and apply it in the streets of Baghdad and Kabul? We have asked our troops to police the world; let's give them the proven tools to succeed. **JFQ**

NOTES

[1] See <http://en.wikipedia.org/wiki/Rudolph_Giuliani#1993_campaign_and_election>.

[2] See <www.oracle.com/customers/profiles/PROFILE4257.HTML>.

[3] Michael J. Sniffen, "Murder rate at a 40-year low: Chicago alone had 150 fewer killings," *The Chicago Sun-Times*, October 18, 2005.

[4] "Afghan rebels may have help from Iraq," Associated Press, February 17, 2007.

[5] See Paul J. Shannon, "Fingerprints and the War on Terror: An FBI Perspective," *Joint Force Quarterly* 43 (4th quarter, 2006), 78.

[6] Daniel Henninger, "The Snake Eater: Give our troops the tools our cops have," *The Wall Street Journal*, February 8, 2007.

[7] Tacticomp is a wireless, Global Positioning System-enabled military hand-held computer designed for field use. Its tactical modem allows automatic communication through field radios.

[8] See <http://en.wikipedia.org/wiki/Rudolph_Giuliani>.