



governmentattic.org

"Rummaging in the government's attic"

Description of document: Military Intelligence Professional Bulletin published at Fort Huachuca US Army Intelligence Center of Military Excellence (USAICoE), January-March 2009 issue

Requested date: 09-April-2014

Released date: 22-August-2016

Posted date: 26-September-2016

Source of document: TRADOC Office of the G-6
Freedom of Information Office (ATIM-IA)
661 Sheppard Place
Fort Eustis, VA 23604-5733
Fax: (757) 501-6509
E-mail: usarmy.jble.tradoc.mbx.hq-tradoc-g-6-atim@mail.mil

The governmentattic.org web site ("the site") is noncommercial and free to the public. The site and materials made available on the site, such as this file, are for reference only. The governmentattic.org web site and its principals have made every effort to make this information as complete and as accurate as possible, however, there may be mistakes and omissions, both typographical and in content. The governmentattic.org web site and its principals shall have neither liability nor responsibility to any person or entity with respect to any loss or damage caused, or alleged to have been caused, directly or indirectly, by the information provided on the governmentattic.org web site or in this file. The public records published on the site were obtained from government agencies using proper legal channels. Each document is identified as to the source. Any concerns about the contents of the site should be directed to the agency originating the document in question. GovernmentAttic.org is not responsible for the contents of documents published on the website.



DEPARTMENT OF THE ARMY
HEADQUARTERS, UNITED STATES ARMY TRAINING AND DOCTRINE COMMAND
950 JEFFERSON AVENUE
FORT EUSTIS, VIRGINIA 23604-5700
AUG 22 2016

Office of the Deputy Chief of Staff, G-6

This is in response to your Freedom of Information Act (FOIA) request made on April 9, 2014 to the Public Affairs Office (PAO) at Fort Huachuca, Arizona. The PAO sent the request to The Directorate of Human Resources FOIA office at Fort Huachuca, Arizona. Your request is for "following issues of the Military Intelligence Professional Bulletin published at Fort Huachuca US Army Intelligence Center of Military Excellence. January - March 2009 (I ask that this issue of MIPB be reviewed for release) October - December 2009 (I ask that this issue of MIPB be reviewed for release) October - December 1999 July - September 1998 July - September 1997 July - September 1995 April - June 1995 January - March 1995". On August 15, 2015 you were sent all of the requested documents but the January- March 2009 issue of the MIPB. The request was processed, referred to U.S. Army Training and Doctrine Command (TRADOC). TRADOC received the package on August 18, 2014, and assigned activity control number FA 14-00178.

As requested, enclosed are the responsive TRADOC records, referred from the Fort Huachuca, Arizona, FOIA Office. Portions of the records have been redacted, and the FOIA exemption that prohibits the information disclosure is cited.

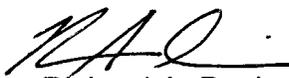
FOIA exemption (b)(7) protects records or information compiled for law enforcement purposes, *i.e.*, civil, criminal, or military, including the implementation of Executive Orders or regulations issued pursuant to law. This exemption may be invoked to prevent disclosure of documents not originally created for, but later gathered for law enforcement purposes. With the exception of parts (c) and (f), this exemption is discretionary. If information qualifies for exemption under (7)(c) or (7)(f), there is no discretion in its release.

This decision is considered a partial denial of your FOIA request. General David G. Perkins, Commanding General, U.S. Army Training and Doctrine Command, is the Initial Denial Authority (IDA) and by position I am the delegated IDA. You may appeal this partial denial of release to the Secretary of the Army. You should address any such appeal to: U.S. Army Training and Doctrine Command, Office of the G-6 (ATIM-IA), 661 Sheppard Place, Fort Eustis,

VA 23604-5733, and it will be forwarded to the Army General Counsel for final disposition on behalf of the Secretary of the Army. To meet the deadline for the appeal, the appeal letter must be received by this office and forwarded to the Secretary of the Army within ninety (90) days of the date of this partial denial letter. You have the right to seek dispute resolution through our FOIA Public Liaison, Alecia Bolling, at: (703) 428-6238, usarmy.belvoir.hqda-oaa-ahs.mbx.rmda-foia-public-liaison@mail.mil.

Point of contact is the Government Information Specialist, (757) 501-6529, usarmy.jble.tradoc.mbx.hq-tradoc-g-6-atim@mail.mil.

Sincerely,



Richard A. Davis
Senior Executive
Deputy Chief of Staff, G-6

Enclosure

FOR OFFICIAL USE ONLY

MIPB

Military Intelligence Professional Bulletin

January-March

2009

PB 34-09-1



FORENSICS

CRIM

FOR OFFICIAL USE ONLY

SCENE

FROM THE EDITOR



“Finding the specific silver needle in a stack of silver needles . . .”

This is the theme running through this issue of **MIPB**. Just as the U.S and its Coalition partners explored the applications of emerging Biometric techniques to counter the challenges in combating terrorism and extremism, so does the department of Defense (DOD) in its expanded use of Forensics beyond the traditional applications.

Mr. Dee, Director, Defense Biometrics, OSD AT&L (DDR&E), states in his Letter to the Field, that “the MI community was among the first to recognize the potential value of forensic technology in identifying and accurately classifying our anonymous foes. It continues to be a leader in not only advancing the technology, but also in embracing the training and the concepts and policies that make forensic technology useful to the Warfighter.” In partnership with the U.S. Army Doctrine and Training Command Capability Manager–Biometrics and Forensics (TCM–BF) here at the U.S. Army Intelligence School, Fort Huachuca, Arizona, this issue of **MIPB** offers an overview of where Forensics is today in areas of interest to the Warfighter. TCM-BF is the Army use advocate to PM DOD Biometrics and designated Forensics PM. It coordinates closely with other Service and Branch proponents to enable, facilitate, and champion the development of Biometrics and Forensics across the doctrine, organization, training, materiel, leadership, personnel and facilities (DOTMLPF) spectrum throughout the DOD.

This issue defines the “What” of Forensics and explains the connection between it and Biometrics. Organizations involved in the development of Forensics from theory to application are identified and discussed. You will find practical information in the tactical, operational, and strategic domains along with points of contact for unit training events. A CD contains valuable references, resources, and guidance in the Forensics arena.

I would like to thank Shirley Kim and David Wikoff for their superlative efforts in partnering with the **MIPB** staff to create this issue.



Sterilla A. Smith

Sterilla A. Smith
Editor

FOR OFFICIAL USE ONLY

MILITARY INTELLIGENCE

January - March 2009

Volume 35 Number 1

PB 34-09-1

Commanding General

Major General John M. Custer III

Deputy to the Commanding General

Mr. Jerry V. Proctor

Deputy Commander for Training

Colonel Dennis A. Perkins

Director, Directorate of Doctrine

Colonel Michael J. Arinello

Chief, ISR Operations Analysis

Division

Mr. Chet Brown

MIPB Staff:

Editor

Sterilla A. Smith

Associate Editors

Shirley Kim
David Wikoff

Design Director

Patrick N. Franklin

Design and Layout

Patrick N. Franklin
Lawrence Boyd

Cover Design

Lawrence Boyd

Issue Photographs

Courtesy of the U.S. Army

Purpose: The U.S. Army Intelligence Center and Fort Huachuca (USAIC&FH) publishes the **Military Intelligence Professional Bulletin (MIPB)** quarterly under the provisions of **AR 25-30**. MIPB presents information designed to keep intelligence professionals informed of current and emerging developments within the field and provides an open forum in which ideas; concepts; tactics, techniques, and procedures; historical perspectives; problems and solutions, etc., can be exchanged and discussed for purposes of professional development.

Disclaimer: Views expressed are those of the authors and not those of the Department of Defense or its elements. The contents do not necessarily reflect official U.S. Army positions and do not change or supersede information in any other U.S. Army publications.

By order of the Secretary of the Army:
Official:



JOYCE E. MORROW

Administrative Assistant to the
Secretary of the Army
0905801

GEORGE W. CASEY JR.

General, United States Army
Chief of Staff

FEATURES

- 5 **Letter to the Field**
by Mr. Thomas P. Dee, Director, Defense Biometrics, OSD AT&L (DDR&E)
- 7 **White Paper — Biometric and Forensic Support to Irregular Warfare**
by TCM-BF
- 12 **Evidence Collection in the OIF Detention Operations Environment**
by Captain Kevin L. Weise
- 14 **Forensic Enabled Intelligence**
by Michael Shattuck
- 16 **LEP: Law-Enforcement Professionals and the Army**
by Captain Timothy K. Hsia
- 20 **Making Battlefield Forensics Work for US: Turning Forensic Evidence into Tactical Intelligence** by Lieutenant Colonel Mike Holmes
- 28 **CEXC Biometrics: Identifying the Bombmaker Networks**
by Erik Berg
- 31 **Training the Force to Identify the Unknown Threat: NGIC's Battlefield Forensic Training** by Captain Ryan Campbell
- 34 **The Biometrics Task Force in Support of Forensic Science**
by Kasey Wertheim
- 42 **Computer Forensic Support to DOMEX in the War on Terrorism**
by David Ferguson
- 47 **The Coalescence and Convergence of the Forensic, Intelligence, and Biometric Communities** by Kasey Wertheim
- 51 **The Role of Forensics in the Iraqi Judicial System: Targeting Insurgents**
by Erik Berg
- 59 **Biometrics and the "Multiple Use Dilemma": Enabling Post 9/11 National Security by Understanding a New Technology Tool** by Hollie Ryan
- 67 **The Forensics Executive Steering Group: Strength through Membership**
by Captain Shawn McMahon
- 73 **USACIL RBOC: Providing Support to the Warfighter and Expeditionary Forensics** by William G. Doyne
- 77 **TRADOC Capability Manager - Biometrics and Forensics**
- 78 **Acronyms**

Departments

- 2 **Always Out Front**
 - 3 **CSM Forum**
 - 83 **Contact and Article Submission Information**
 - 84 **MIPB on IKN**
- Inside Back Cover: Forensic Resource CD

FOR OFFICIAL USE ONLY

ALWAYS OUT FRONT



by Major General John M. Custer III
Commanding General
U.S. Army Intelligence Center and Fort Huachuca

This issue of MIPB focuses on Forensics and how this capability is currently shaping the War on Terrorism and what the future of forensics is across the range of military operations. Only in the past decade have the technologies emerged and matured to enable our forces to achieve this capability. I am convinced that the proliferation of biometrics systems coupled with the development of forensics collection and exploitation facilities in Iraq have made a major contribution to successes in operational theaters. Biometrics and forensics are proven technologies, honed during the most dangerous operations against insurgents and terrorists in Fallujah and across the battlegrounds of Operations Iraqi and Enduring Freedom (OIF/OEF).

You have heard me describe current intelligence operations as being significantly more difficult than finding a needle in a haystack. But it is more like trying to find a silver needle in a stack of six million silver needles. Expeditionary forensics in concert with identity tracking has now proven that we can put a neon flashing arrow on the specific needle we are looking for and deal with it decisively.

When one considers that the Department of Defense (DOD) has traditionally used forensics to gather evidence, facts and data to use in a court of law, one sees that we have made remarkable progress. In order to combat a highly intelligent and adaptive enemy, we have expanded our forensic capability to play an integral role across the spectrum of the War on Terrorism, including intelligence functions, operational activities, force protection, personnel recovery, host nation legal support, and identity superiority functions. The ability to rapidly exploit sensitive sites, items, and information has significantly aided U.S. and Coalition forces' intelligence operations, resulting in the identification and elimination of enemy threats. Using forensics on the battlefield gives warfighters the ability to "identify insurgents, terrorists, and/or enemy combatants; link them directly to equipment, documents or devices, and provide the documented basis for force protection measures, targeting, support to prosecution, sourcing, and support to medical activities."¹

Documented successes with various forensics capabilities on the battlefield have stimulated much conversation within the military community. OIF and OEF have validated the importance of forensic science to the military decision process across all echelons of warfare from near real-time actionable intelligence for tactical commanders to products relevant to Combatant Commanders, Services, the DOD, and National activities.

In March of 2004 a man was arrested for videotaping U.S. convoys. The offense was not overly significant and not particularly illegal. But he was detained and interrogated. The interrogators declared that he was of low intelligence value and low threat to Coalition forces. They released him. (S) (U)

Further intelligence later determined that he was a bomb maker cell leader who taught other insurgents how to build, emplace, and carry out attacks on U.S. forces. He was a major leader who was released because traditional intelligence approaches determined that he was of low intelligence value, and low threat value. A target package was later constructed in his honor, but it would have never been discovered if it weren't for Soldiers on the ground executing effective site exploitation.

(Continued on page 4)

FOR OFFICIAL USE ONLY

Military Intelligence



CSM FORUM

by Command Sergeant Major Gerardus Wykoff
Command Sergeant Major
U.S. Army Intelligence Center and Fort Huachuca

“This one time, in Iraq...”

You may recognize this line as the Soldiers' version of “Once upon a time...” What usually follows is a highly descriptive and realistic account of an event or scenario told by a more experienced Soldier as he attempts to capture the attention of his subordinates. Used as a teaching tool to reinforce the rigors of warfare, war stories have always served a distinct purpose in “greening” the next generation of Soldiers. As I progressed through the ranks, I recall many stories told by my Leaders which caused in me mingled feelings of awe, fear, a heavy dose of anticipation and, often times, skepticism. Passed off as the “real deal,” many were truly as beyond belief as “Jack and the Beanstalk”.

Remarkably, the war stories of today's Intelligence Soldiers also sound beyond belief. The incredible tasks we are asking our newest generation of Soldiers to accomplish is astounding! The topic of this issue, Forensics, is a great illustration of the rapidly changing, powerfully effective, and mutually beneficial technologies our warfighters are using to gain leverage. Known by many labels—sensitive site exploitation, battlefield forensics, expeditionary forensics—forensics exploitation, when coordinated across the full spectrum of disciplines, delivers ownership of the battlespace and successful operations.

The use of forensics in the Department of Defense has migrated from traditional to nontraditional. Examples of traditional forensics use include criminal investigations, casualty identification and examinations. The emerging technologies allow us the ability to use forensics in intelligence, Counterintelligence, battlefield forensics, and document, media, and computer exploitation. This capability has never been seen before! The expertise required to coordinate actions and successfully process evidence within a captured sensitive site may come from many domains. From exploiting personnel documents, electronic data, and material captured at the site, to analyzing biometric or weapon data in timely fashion, forensic collection causes our Soldiers to constantly assess the importance of speed versus the accuracy or reliability of the information. In addition, all this must be done while neutralizing any threat posed by the site or hostile actions in the vicinity of the site.

Military Intelligence (MI) has never operated in a vacuum. By our carefully crafted collaboration with law enforcement, as well as other branches of the military, two disciplines have been brought together whose aims some formerly thought to be mutually exclusive. If specific criteria are met, then MI and law enforcement/criminal investigation can mutually support the warfighter provided extra care is taken to ensure the integrity of both parties. We are achieving success upon wild success in this area.

A great example of the marriage of MI and law enforcement can be found in a relatively new concept: Evidence-based Targeting. Since the acceptance of the new Status of Forces Agreement (SOFA) in Iraq, Coalition forces are now working regularly with Iraqi Security Forces and the Iraqi Judicial System (IJS). All Soldiers' actions follow the laws of the IJS from patrolling the streets to capturing suspects and prosecuting them. The parameters of the new agreement force our Soldiers to share more intelligence and information with Iraqi forces in order to obtain evidence-based warrants from the IJS prior to actioning any targeted individuals. Coalition forces are still allowed to defend themselves; however, they must be prepared to turn over any captured individuals, equipment, etc. to competent Iraqi authorities within a much shorter time frame than was previously required. These new policies cement the need for strong, accurate

ALWAYS OUT FRONT

(b) (7)(E)

The USACIL LP and DNA examiners provided expert witness testimony via secure VTC to an Investigative Judge for the Criminal Court of Iraq. The trial for the accused Iraqi terrorist is expected to begin shortly.

(b) (7)(E)

The U.S. Army Intelligence Center and Fort Huachuca is designated by the U.S. Army Training and Doctrine Command as the lead for Biometrics, and has chartered and convened the Biometric and Forensics Integrated Capabilities Development Teams. Biometric and forensics technologies have truly changed the way we fight and win on today's battlefields. I am confident that we are on the cutting edge of this emerging capability and along with our partners from the DOD, forensics applications will be developed that will continue to serve commanders, protect our Soldiers, and further our nation's interests. 

Endnote

(b) (7)(E)

Always Out Front!

CSM FORUM

and detailed target packages in order to obtain the proper warrant from an Iraqi Judge before any actions are taken against targeted individuals.

Because of the stronger target packages and increased IJS involvement, detained individuals will be much more likely to be prosecuted to the full extent of the Iraqi Law. Many resources will be saved because Coalition and Iraqi Security Forces will not have to chase down as many of the same targets over and over again. This will also reduce the recidivism rate (the same criminals committing multiple crimes across the country), since captured individuals will stay in custody instead of being released right away to commit more crimes. 

NCOs Lead from the Front!

FOR OFFICIAL USE ONLY

LETTER TO THE FIELD

Forensic Science and Technology

by Thomas P. Dee, Director, Defense Biometrics, OSD AT&L (DDR&E)

Forensics is one area in which the Department of Defense (DOD) is applying capabilities and technologies typically used in law enforcement to fulfill national security and counterterrorism applications. While forensic science is traditionally known as applying scientific knowledge and methodology to legal problems and criminal investigations, the War on Terrorism is fundamentally reshaping forensic science. The DOD redefines forensics as, "The application of multi-disciplinary scientific processes to establish facts."

Forensic sciences such as latent prints, DNA, firearms and tool marks, forensic document examination, digital evidence, and forensic pathology and odontology have been used primarily for legal and law enforcement applications, but have also significantly impacted military operations, particularly intelligence operations.

As many Americans have seen in nightly news-casts brought into our living rooms, the combatant commander, Soldiers, and Marines have learned that the same science we apply to identifying, catching, and convicting common criminals is extremely useful in identifying enemies, insurgents, and terrorists and scientifically linking them to other people, places, things, organizations, and events.

In particular, the rapid forensic exploitation of sensitive sites, items, and information has significantly aided U.S. and Coalition forces' operations, resulting in the identification and elimination of enemy threats through disruption, targeting, and prosecution.

Challenges and Capabilities

The capability to extract actionable information through forensics exploitation of recovered materials will be critical to the nation's security in the 21st century. New technologies will be required to enable military forces to recognize, preserve, collect, ana-

lyze, store, share, and process materials across the range of military operations.

At the request of the Under Secretary of Defense for Acquisition, Technology and Logistics, and as tasked by the Joint Chiefs of Staff, the U.S. Army Training and Doctrine Command (TRADOC) is conducting a Forensics Capabilities Based Assessment as a first step in defining and integrating future forensic capabilities. Parallel development of the science and technology (S&T) that enables forensics operations will ensure that our technology base will be poised to support our future forensic programs.

On 15th October 2008, the Director, Defense Research and Engineering (DDR&E) hosted a three-day Forensic S&T Workshop in Arlington, Virginia to develop a Strategic Plan. The purpose of this workshop was to engage S&T leadership, establish an S&T baseline for the Forensic Program, map that baseline to our desired future capabilities, and enable a DOD S&T roadmap that defines transition paths to formal acquisition programs. The workshop was held in work group format, with each group reporting back to all attendees and DOD/Interagency leadership at the end of the workshop. Over eighty people were in attendance.

DOD attendees of the workshop included representatives from the Service research laboratories, DOD S&T organizations, Technical Support Working Group, Joint Improvised Explosive Device Defeat Organization, law enforcement, biometrics and intelligence communities, and the defense forensic labs. Other organizations represented included the military criminal investigation organizations, and the Joint Expeditionary Forensic Facilities, as well as TRADOC and the U.S. Army Military Police School.

Interagency attendees consisted of representatives from the National Institute of Justice, Department of Energy labs, National Institute of Standards and

Technology, Department of Homeland Security, and other federally funded research labs.

At the conclusion of the workshop, the way ahead was discussed. It included the production of a report detailing the work group discussions and identified capability gaps, a DOD S&T strategic plan to map future strategies, and the drafting of a charter to be used to create the Forensic S&T Working Group. The outcome will be briefed at the Forensic Executive Steering Group and presented to the Services S&T Executives.

As the Principal Staff Assistant for Defense Biometrics to the Secretary of Defense, the DDR&E is committed to advancing the technologies, systems, processes and organizations which bring this much needed capability to the field. In conjunction

with the Joint Staff and Services, we are committed to developing the validated requirements, policy, and programmatic and budgetary discipline that will bring this important enabling technology into the mainstream of DOD capabilities.

The Military Intelligence (MI) community was among the first to recognize the potential value of forensic technology in identifying and accurately classifying our anonymous foes. It continues to be a leader in not only advancing the technology, but also in embracing the training and the concepts and policies that make forensic technology useful to the warfighter. I am pleased that the MI community has chosen to give this emerging technology such a prominent place in this professional journal. ✦

FORENSIC FOCUS



FOR OFFICIAL USE ONLY

Military Intelligence

White Paper

Biometric and Forensic Support to Irregular Warfare

15 January 2009

“...the application of forensics science capabilities provides tremendous, but mostly untapped, potential to identify, track and prosecute enemy persons.”

*John J. Young Jr.,
Director, DDR&E
25 July 2007¹*

Executive Summary

The recent DOD Directive on Irregular Warfare (IW) provides official recognition that IW is as strategically important as traditional warfare. The Directive outlines a number of goals and responsibilities aimed toward improving IW proficiency across all DOD Components—to make DOD “...as effective in IW as it is in traditional warfare.” Notable among these goals are:

- ◆ Identify and defeat irregular threats from both state and non-state actors.
- ◆ Support a foreign government or population threatened by irregular adversaries.
- ◆ Create a safe and secure environment in fragile states.
- ◆ Conduct (among a host of other things) support to law enforcement.²

Identity Superiority, Biometric Enabled Intelligence and Forensic Enabled Intelligence strongly support these goals, by allowing us to identify both state and non-state actors through their bio-signatures and the forensic material they leave behind. Biometrics and forensics enable us to track and target these individuals by providing actionable intelligence to maneuver commanders and by aiding situational awareness. Perhaps most importantly in the longer term, biometrics and forensics lay the groundwork for a successful transition to civil authority and civil law enforcement by providing evidence to prosecute wartime combatants in criminal courts.

(b) (7)(E)

1. (b) (7)(E)

2. (b) (7)(E)

3. (b) (7)(E)

4. (b) (7)(E)

5.

6. **Medical Forensics.** *Medical Forensics provides studies of injuries to improve the development of medical training and first aid, which leads to better armor and force protection.*

These Biometrics and Forensics programs complement each other to establish irrefutable personal identity, and ties individuals to places, events and things with scientific facts gained through observation and analysis. This serves to support the DOD IW goals by identifying threat individuals, separating those in-

dividuals from the remaining population and supporting law enforcement. All of these capabilities help to create the safe and secure environment necessary to allow for the political and public infrastructure to operate effectively, as well as provide the services necessary for a government to establish effective popular support.

Scoping the Problem: IW

IW is the violent struggle amongst state and non-state actors for legitimacy and influence over a population.³ In order for one side or faction to win, they must gain the loyalty and support of the population. How they gain this support is immaterial—whether through fear and intimidation or by convincing the people that they can best provide their basic needs—but once they have gained the support of the popular *centers of gravity*, the contest has been won.

Irregular combatants are largely drawn from the population they are trying to influence and win—IW is seldom led or instigated by outside forces. Although outside forces may support and supplement the combatants, or even subvert them to their own ends, the actual combatants themselves are usually indistinguishable from the local population. To exist, irregular forces must therefore be able to blend in with that population. For irregular forces to thrive and succeed, the population must actively support them.⁴

To defeat irregular forces, one must separate them from the population. This should be done in two ways: ideologically, and physically.⁵ One accomplishes the first by convincing the population they are better able to provide for their needs than the irregular forces. The recent “Awakening” in Iraq’s Al Anbar province is an example of this dynamic. As Al Qaeda and their allies inflicted casualties and violence against the local population, they alienated themselves from the people. The local Arabs turned to the Marines for help—thereby handing victory to the Coalition Forces.⁶

But seldom are irregular forces as short-sighted as Al Qaeda was in Al Anbar province. Irregular forces are usually able to exploit the natural divisions present in any society to find a segment of the population willing to support them and provide cover.⁷ When this occurs, one must then be able to physically separate them from the population—like using a fine-toothed comb to rid a person of lice. It is time consuming, painstaking work that bears constant repetition to get right—and it can be very painful for the population you are trying so hard not to alienate, because it requires a certain amount of state intrusion into their private lives to search, segregate and clear through the areas where the irregular forces are known or believed to operate.

Given the nature of IW, these two measures are often conducted simultaneously: one isolates and separates the irregular forces from their popular base of support while at the same time convincing that population that the current regime will do a much better job of leading and providing for them than will the irregular forces. In order to make this balancing act work, we need a mechanism that helps us to easily identify who the irregular forces are in order to avoid false arrests and detentions. We also need a way to prove in court that the people we detain are guilty of violence “beyond a reasonable doubt”. In this way, we not only prove the justice of our own cause, but also “drive a wedge” between those we detain and try, and the populace.

Biometrics and forensics provides the evidence we need to produce that “wedge”.

Specific Programs

“Within DOD, multi-disciplinary forensic sciences contribute to sensitive site exploitation, identifying, tracking and targeting enemy forces, examining crime scenes, prosecution of offenders in court systems, and the identification of human remains and manner of death. Capabilities to collect, process and analyze deoxyribonucleic acid (DNA), firearms signatures, tool-marks, and trace evidence have all been employed either within the Central Command AOR or in-CONUS to help identify persons of potential interest.”⁸

LTG James D. Thurman
US Army G-3/5/7
25 April 2008

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

Fingerprint collection, matching and analysis is only one example of how forensically collected biometrics can contribute to the fishnet of information that leads to the capture of enemy forces. Additional biometrics modalities are DNA, voice patterns, iris and retina patterns, facial recognition and other distinct signatures of the human body. Once we have an enemy biometric signature, such as a fingerprint, he or she can no longer afford to enter a checkpoint or be detained. In recent interviews of units recently returned from the battlefield, biometrics is repeatedly cited as key to disrupting the enemy's freedom of movement, and suppressing their communications and networking.⁹

"Among the most valuable data submitted to our defense wide biometrics enterprise are the latent fingerprints collected from enemy weapons and from various other surfaces during sensitive site exploitations. But latent fingerprints are but one product of a comprehensive forensics capability."

*John J. Young Jr.,
Director, DDR&E
25 July 2007¹⁰*

(b) (7)(E)

In the proposed Forensics DOD Directive, the Air Force assumes Executive Agency over digital and multimedia forensics.¹¹ DOMEX is one of the biggest producers of battlefield collection and actionable intelligence in Iraq and Afghanistan. (b) (7)(E)

(b) (7)(E)

b. FM 2-24 Counterinsurgency: "Documents and pocket litter, as well as information found in computers and cell phones, can provide critical information that analysts need to evaluate insurgent organizations, capabilities, and intentions. TAREX (Target Exploitation) and DOCEX are also a great benefit to HUMINT collectors in substantiating what detainees know and whether they are telling the truth."

c. Allied Joint Publication 2.5(A): Defines a document as "any recorded information regardless of its physical form or characteristics including, but not limited to, all written material, whether handwritten, printed or typed; painted, drawn, or engraved material; video, sound or voice recordings; imagery, computers and computer storage media such a floppy, compact digital versatile and hard disks, flash drives, portable memory devices, magnetic tape and associated material including punched cards, punched paper tape and printed output; reproduction of the foregoing, by whatever process."

(b) (7)(E)



(b) (7)(E)

(b) (7)(E)

Trace evidence compares two samples to find common markings and to see if they are linked.

(b) (7)(E)

(b) (7)(F)

(b) (7)(E)

(b) (7)(E)

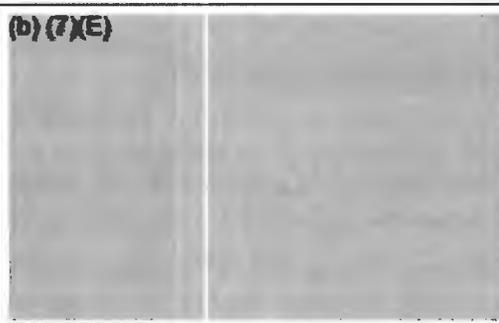
(b) (7)(E)

5. (b) (7)(E)

◆ (b) (7)(E)

Physical Science helps answer difficult questions. Where did the bullet come from? What was the range? How deep was the bomb buried? Was it at a checkpoint? What was used as an aiming stake? Some of these questions can not be determined solely from the material examined at the lab. Furthermore, the physical science applied to answering these questions can help build better armor for our troops, identify enemy capabilities and determine how to train our troops to search and monitor areas for enemy conduct.

(b) (7)(E)



6. Medical Forensics. *Medical Forensics provides studies of injuries to improve the development of medical training and first aid, which leads to better armor and force protection.*

Medical forensics is relevant regardless of the type of warfare, but certainly in IW. Medical forensics includes such sciences as Odontology, Anthropology, Pathology, Toxicology, Serology and more. In Vietnam medical forensics revealed that 90 percent of soldier deaths that occurred prior to reaching the medical facility were related to blood loss. This sparked a change in first-aid training and in the medical corpsman on the battlefield. Medical forensics reduced that number to 60 percent. Similar modern day studies led to the creation of speed tourniquets that can be applied within 30 seconds. This reduces danger to the injured, and reduces the amount of attention needed from the firefight to apply it.

(b) (7)(E)

“Additional potential resides in the exploitation of trace evidence, drug chemistry, serology, anthropology, odontology, pathology and toxicology. The rapid forensic exploitation of sensitive sites, items, and information has significantly aided U.S. and coalition forces’ intelligence operations, resulting in the identification and elimination of enemy threats through disruption, targeting or detention and subsequent prosecution.”¹²

*LTG James D. Thurman
US Army G-3/5/7
25 April 2008*

Conclusion

Biometrics and Forensics complement one another to help identify the key leaders and operators of insurgent movements or in IW. In doing so, these capabilities provide the maneuver commanders who will be decisively engaged in the IW fight with *actionable and targetable intelligence* that will help them to disrupt and dismantle the networks the insurgents need to sustain their effort.

These capabilities also serve to provide vital information to assist with force protection. (b) (7)(E)

It also provides the key element of “predictive intelligence analysis” to the targeting process and disruption of enemy operations.

Studies of IW consistently focus on the advantages irregular fighters naturally employ to blend with the local population . . . Biometrics and Forensics negate that advantage.

Dave Wikoff, CTR, Harding Security
Forensics Subject Matter Expert
TCM-BF

Mike Holmes, CTR, Oberon/Stanley
Forensics Operations Officer
TCM-BF

Footnotes

2. DOD Directive 3000.07, “Irregular Warfare”, 1 December 2008, accessed on 8 December 2008 at <http://www.dtic.mil/whs/directives/corres/pdf/300007p.pdf>, 1-3.

3. Ibid.

4. Bard E. O’Neill, *Insurgency & Terrorism; From Revolution to Apocalypse*, Second Edition (Washington D.C.: Potomac Books, Inc., 2005), 93.

5. David Galula, *Counterinsurgency Warfare: Theory and Practice* (Westport Connecticut: Praeger Security International, 2006 (first published in 1964)), 61-63.

6. Dr. Stephen Biddle, “Stabilizing Iraq from the Bottom Up,” Statement before the U.S. Senate Committee on Foreign Relations, Second Session, 110th Congress, 2 April 2008. Accessed from the Council of Foreign Relations Website on 10 December 2008 at <http://www.cfr.org/content/publications/attachments/Biddle%204-2008%20Testimony.pdf>.

7. Bruce Hoffman, *Inside Terrorism* (New York: Columbia University Press, 2006), 242-243.

10. DDR&E Memorandum, 25 July 2007, 1.

11. Capstone Concept of Operations for DOD Forensics, OSD AT&L DDR&E, 18 July 2008.

12. Office of the Deputy Chief of Staff, G-3/5/7 Memorandum to Commander, TRADOC, 25 April 2008, 2-3.



EVIDENCE COLLECTION IN THE OIF DETENTION OPERATIONS ENVIRONMENT

by Captain Kevin L. Weise

Introduction

Although most of the detainees in the various theater internment facilities (TIFs) in Iraq are already charged with the commission of crime, the fact of the matter is that some of them will commit additional crimes while detained. It is possible to have an attempted escape, a detainee-on-detainee assault, a conspiracy, an assault on a guard, or even a murder. All of these are crimes punishable under Iraqi law. The collector of evidence in the Operation Iraqi Freedom Detention Operations environment should focus on one thing: Getting a conviction at the Central Criminal Court of Iraq (CCCI).

The CCCI was created on 13 July 2003 by CPA Order #13. It serves as the only Iraqi court with federal jurisdiction over any crime committed in Iraq. The Court's jurisdiction relies on the 1969 Iraqi Penal Code, the 2005 Anti-Terrorism Law, and the 1971 Iraqi Criminal Procedures Code. The Court is based on a civil law system, much like what one would find in France, rather than a common law system that we have here in the U.S. To the lay person, this means that instead of a grand jury indictment and a trial by a judge and a jury of your peers, the Iraqi suspect defendant goes before an Iraqi investigative law judge. The judge can then either dismiss the charges or refer the case to trial in front of a panel of three Iraqi judges who hear the case without a jury and either dismiss the case or render a conviction and a sentence.

Evidence Collection

The key then is to present a rock-solid case to the investigative law judge who drafts the report which hopefully refers the case to trial. Thus, the investigator must tailor his evidence collection procedures

to assist the prosecutor in presenting a case that is compatible with what the Iraqi judges are expecting to see in order to refer a case to trial and then for the trial court to issue a conviction.

In Iraq, one thing is certain: More evidence means a longer sentence. This is very different than what we know about American jurisprudence. In application, a simple formula has been devised to obtain referral to trial with resultant convictions and longer sentences. In addition to physical evidence, the judges expect photos, video, diagrams of the crime scene, witness statements, and more photos.

Regarding photographs, the best ones are those that include the detainee. In other words, take a picture of the detainee at the scene of the crime. Included in that photo should be any other relevant evidence. For example, in the case of a detainee-on-detainee assault, take a picture of the suspect detainee next to any blood splatters or other evidence of the assault. If the detainee has blood on his person or his clothing, pictures should be taken of him wearing the bloody clothes before he has been cleaned and sanitized. Video of this scenario, in addition to the pictures, is encouraged.

The more pictures that are taken, the better! In the case of an attempted escape, take pictures of the detainee next to the hole in the fence or in the tunnel. Get a picture of him holding the wire cutters or the shovel. Take a picture of him at his recapture covered in dirt from digging. Take a picture of anything that will make the scene more understandable to the Iraqi judges.

Iraqi judges are also very interested in scene diagrams. In a detention environment, I recommend

that units pre-print basic diagrams of the various compounds under their jurisdiction for handy, immediate use by investigators. More detailed scene sketches and diagrams can be fashioned at the scene to drill down on specifics. Include things like locations of weapons, instruments of the crime, victims, witnesses, and guards in the diagram. Remember that Iraq is on the metric system, so make things easy for the judges to understand, use meters and centimeters on the diagram instead of feet and inches.

Among the most important pieces of evidence are the statements. As military practitioners, we are accustomed to the standard "sworn statement" that all of the U.S. Armed Forces use in one form or another. For the CCCI, this is not good enough. The statements are good enough to refresh a witness' memory, but the CCCI requires live witness testimony. However, the statements are still part of the record, so get good ones. Ideally, your statements should be from Iraqi nationals. Get the standard sworn statement from the guards, but get Arabic statements from the Iraqi correctional officers (ICOs) and from the suspect's fellow detainees and the detainee victim, if there is one. Culturally, these statements will go far with the judges.

Most importantly, get a written statement from the detainee suspect. Iraqi detention facilities are not in America and the detainees are not Americans. They don't have a right against self incrimination. If the suspect will not write a statement, write it for him based on the facts that your investigation uncovered and ask him to sign it. If he refuses to sign the statement, write "Refused to Sign" on the document and make it part of the record. If he agrees to sign the statement, **take a picture of him signing it.** Although such statements are generally not admissible in court unless taken in front of an Iraqi police officer or judge, they can be used to impeach the suspect's testimony at the investigative hearing or the trial. If you have an ICO at the scene, have him witness the suspect's statement and then get a statement from him too. All statements, at a minimum, should include the five Ws (Who, What, Where, When, and Why.)

The Crime Scene

You may have noticed that I haven't spoken very much about physical evidence. I don't want to give

the reader the impression that physical evidence is not as important as what we have discussed so far, but in a TIF many factors will conspire against the intrepid investigator to taint or destroy your physical evidence. The previously mentioned floor plan diagram will get you a referral to trial and a conviction. The actual physical evidence will go very far toward getting a longer sentence for the defendant.

But there are a lot of "ifs" in a TIF. By the time the investigator gets to the scene, it is often more than several minutes old and any number of other detainees have contaminated it and any number of guards have responded to quell the situation. The well trained guards will protect the scene as best they can, but they are often not the military occupational specialty (MOS) qualified Military Police who are trained in crime scene protection. They are Soldiers, sailors, and airmen of other MOSs and are trained in maintaining the good order and discipline of the facility and treating detainees with dignity and respect.

The investigator must also remember that the crime scene is usually in a section of the compound that must be put back into service in relatively short order. By this I mean that crimes in the TIF will usually occur in one of the detainee living spaces necessary to maintain the detainee population such as the detainee sleeping area or the detainee latrine. Thus, evidence must be collected quickly at the scene and you will usually only get one shot at it.

Conclusion

The final word in this basic primer on evidence in the detainee environment is to think outside the box. Don't feel confined to thinking like an American when you are gathering evidence in a TIF in Iraq. Take lots of pictures, draw diagrams, get lots of statements, gather and protect what physical evidence you can, and your suspect will get a nice long sentence at trial. ❁

Captain Kevin Weise is a graduate of Pennsylvania State University and the Thomas M. Cooley Law School. While deployed with the 177th Military Police Brigade and TF 134, he was the Staff Judge Advocate of Theater Internment Facility Camp Remembrance II, Baghdad, Iraq, from July 2007 through April 2008. He currently resides in Michigan and is a Judge Advocate in the Michigan Army National Guard and is the JAG Regional Accessions Coordinator for the Midwest.



Introduction

(b) (7)(E)

(b) (7)(E)

As he departs the compound with his appointment slip in his pocket, an entire enterprise has already begun to work.

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

The Match

(b) (7)(E)

The subject's mask of anonymity has been ripped away, and beneath it lies an enemy.

(b) (7)(E)

(b) (7)(E)

(b) (7)(F)

An Iraqi trying to gain access to a U.S. facility is scanned with the PIR 2.3 Iris scanner.

Two incidents with one link—Forensics. And now, one less bad guy on the streets.

Starting from Fact

A forensically acquired link enables intelligence professionals to drive collection based upon factual information. A latent fingerprint match places the subject inextricably in contact with the matched object. This forensic fact can greatly enhance the effectiveness of standard screening and interrogation procedures.

When an interrogator enters the booth with our Cropper visitor, he has an important edge. He can quickly determine the subject's level of cooperation and indicators of deception. (b) (7)(E)

Confronted with the forensic facts that confirm his complicity, the subject will be far more likely to cooperate.

Building the Networks

The value of forensics to intelligence is more far reaching than one-to-one matches, as in the example of our Cropper visitor. Forensics allows intelligence analysts to link groups, organizations, and people together. And again, the links are based on forensic facts, not analytical inferences. (b) (7)(E)

(b) (7)(E)

Conclusion

Forensic science is making a difference not only in helping to defeat the insurgencies in Iraq and Afghanistan, but in helping to secure our Homeland.

(b) (7)(E)

Note: Forensic is generally a legal term pertaining to use in the court of law. In the context of this article, the term deals with the Forensic Science of matching latent fingerprints to people.

Michael Shattuck is a contractor for Pragmatics, INC working for the National Ground Intelligence Team Biometrics Program providing Contract Advisory and Assistance Support (CAAS). Michael spent a year in Baghdad supporting DOD Biometrics and is also a first lieutenant in the U.S. Army Reserve.

FORENSIC FOCUS

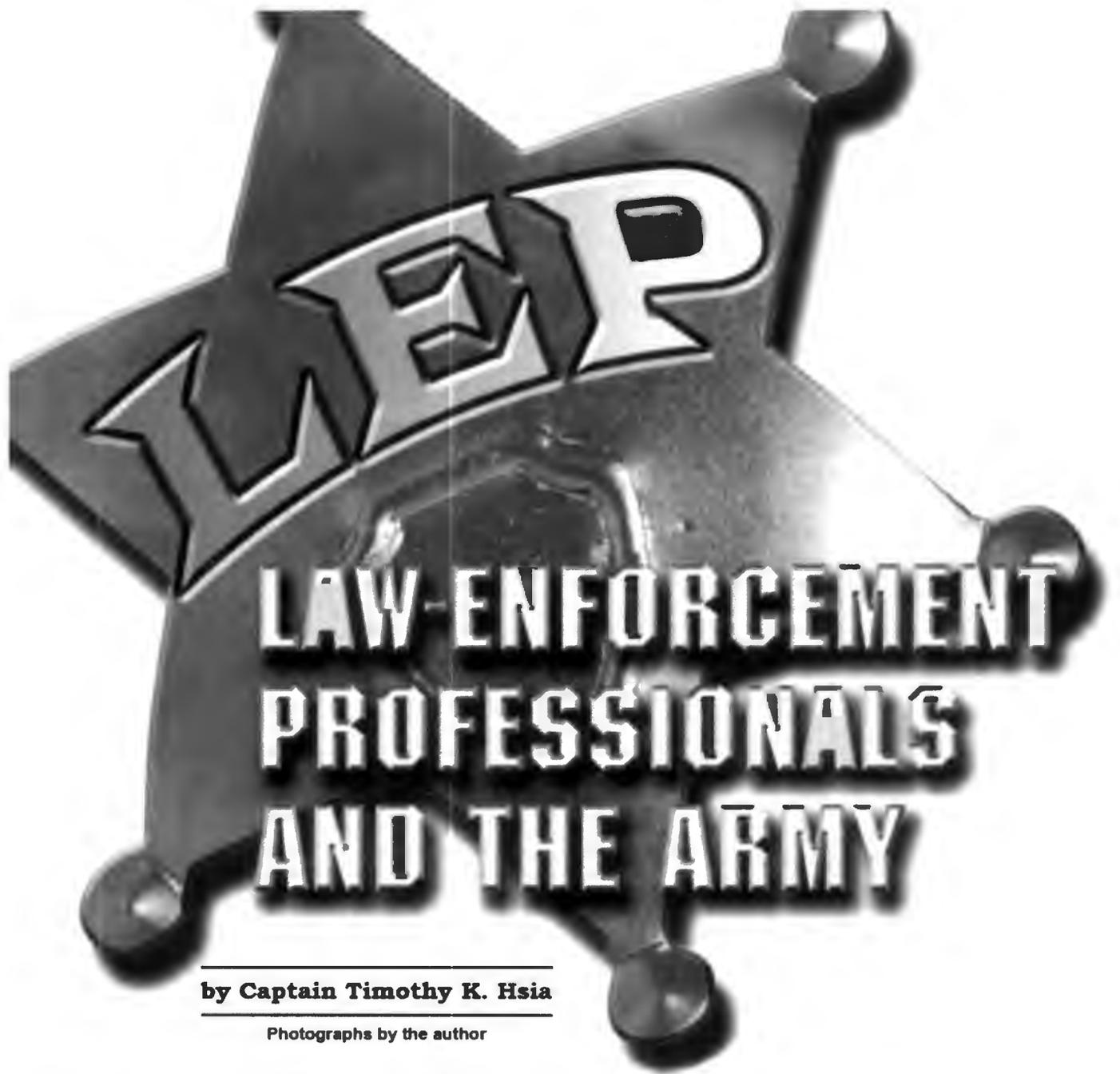
(b) (7)(E)

Latent

Record

(b) (7)(E)

(b) (7)(E)



by Captain Timothy K. Hsia

Photographs by the author

The current conflicts in Afghanistan and Iraq have greatly tested the Army's manpower and equipment. The Army has responded to the constantly changing threat environment by researching new technologies and by better equipping soldiers with the latest gear in order to increase the survivability and lethality of deployed units.

But the emphasis in adapting to new threats posed by the enemy is not strictly limited to technological advances or equipment. The military has augmented units with additional enablers, such as

"From ARMY Magazine, July 2009. Copyright 2009 by the Association of the U.S. Army. Limited reprint permission granted by AUSA."

**"IT'S A FORENSIC
BATTLEFIELD."**

*—Donnie Young,
law-enforcement professional*

specialized nonmilitary teams. One example is the much publicized and controversial human terrain team. Other enablers in Iraq, however, such as law-enforcement professionals (LEPs), have embedded with units and are currently influencing the operational picture within Army units. These contracted former law-enforcement individuals have assisted military units in numerous capacities, from instructing soldiers to hone their tactical questioning techniques to aiding platoons with sensitive sight exploitation (SSE) after raids.

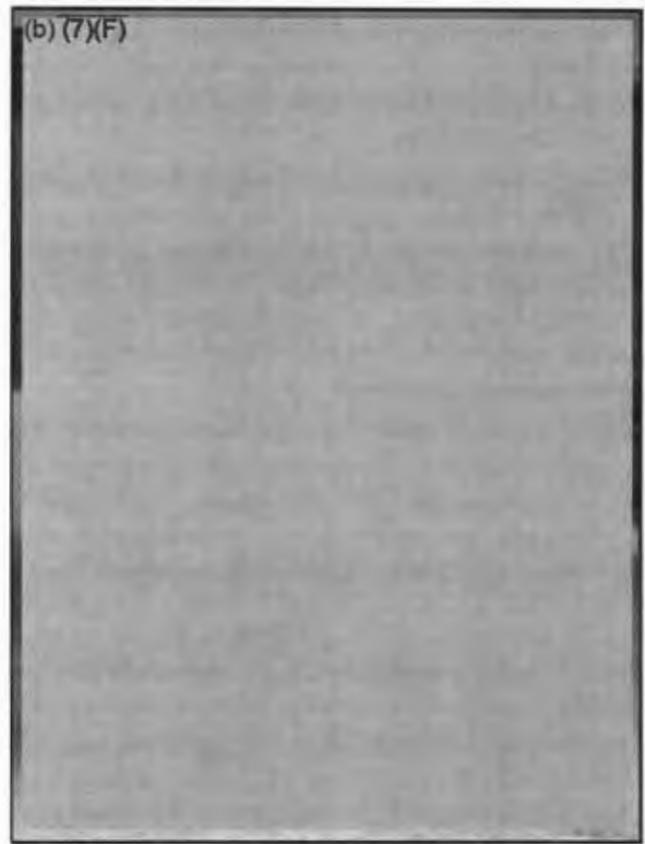
The LEP program resulted from the Army's awareness that too much actionable and incriminating evidence was being lost because of soldiers' lack of police skills. Soldiers inadvertently committed several basic lawenforcement mistakes while on patrols. These mistakes ranged from failing to gather up properly all available evidence from a scene and soldiers inadvertently placing their fingertips on captured equipment, to failing to follow a logical course of questioning when interrogating a suspect. In essence, the Army realized that in counterinsurgency, soldiers on the ground needed additional assistance with collecting, refining, data mining and extrapolating intelligence as the result of a raid or from a cache. This collected intelligence, which might have otherwise been lost because of hastiness, could then potentially lead to the capture and defeat of remaining insurgent cell leaders. The solution to the Army's predicament of how to better equip units with the skill sets necessary to capture insurgents and criminals was to hire former law-enforcement professionals. These LEPs would assist military units in further reducing the loop between actionable intelligence and operations.

The LEP program is the brainchild of the Joint Improvised Explosive Device Defeat Organization (JIEDDO). The LEP objective is to provide "the capability to conduct criminal-enterprise analysis in order to facilitate methods to identify, monitor, penetrate, interdict and suppress criminal networks in support of the C-IED [counter-improvised explosive device] mission." According to the JIEDDO web site, LEPs' "insights into the techniques and patterns of gangs and organized crime have significantly improved commanders' efforts to target IED networks."

LEPs are contracted civilians, all of whom have at least secret-level security clearances. There are currently around 95 LEPs in Iraq and 30 in Afghanistan.



Law-enforcement professionals (LEPs) embedded with 4th Brigade, 2nd Infantry Division, collect evidence at the scene of a house-borne improvised explosive device in the Diyala River Valley, Iraq. Contracted civilians, LEPs provide soldiers expertise and training in collecting, refining and extrapolating intelligence



(b) (7)(F)

The LEP program is divided into those who serve at the brigade level (LEP 1) and those embedded to battalions (LEP 2). LEP 1 individuals focus on criminal analysis, including targeting and tracking insurgents. The majority of these individuals have backgrounds in federal law enforcement and include FBI agents, Drug Enforcement Agency agents, Secret Service agents and even retired border-patrol agents.

LEP 2 individuals are seasoned law-enforcement policemen who have worked with various urban police departments across the United States, including New York City, Chicago, St. Louis and Los Angeles. Many LEP 2 individuals have worked as undercover operatives, have expertise in cases relating to street gangs and large-scale criminal enterprises, and have often been involved in federal task forces.

Before deploying to Iraq or Afghanistan, LEPs train in Virginia for roughly two months, focusing on IED defeat in terms of targeting and researching common enemy tactics, techniques and procedures that deployed soldiers encounter. LEPs have an initial one-year contract but can opt to extend it. The LEP program initially had LEPs embedded with a unit six months prior to deployment, but this was found to be too time-consuming for LEPs who would end up being separated from their families for up to 18 months at a time.

Some soldiers are guarded when first introduced to LEPs. Soldiers occasionally incorrectly assess LEPs as possible criminal-investigative detectives who are sent in by superiors to analyze and question soldiers' actions while on patrols. This wariness quickly dissolves after LEPs join the soldiers in numerous combat patrols.

When LEPs approach a site, they are often more circumspect, patient and attuned to the details than the average soldier. For the soldier, the capture of the detainee has typically been viewed as the end of the tactical operation. After a raid, a soldier's adrenaline subsides, fatigue begins to creep in and subordinates are anxious to head back to base for a warm meal. Although tactical victory has been achieved with the capture of a detainee, victory can be fleeting if soldiers on the ground do not properly catalogue evidence and ask probing tactical questions. Only when a detainee and a site are properly exploited can the tactical victory translate to operations of strategic value. LEPs, in sharp contrast to soldiers, view the capture of the detainee as the beginning of the operation. To LEPs, this is when work must be done immediately in order to collect additional intelligence, refine detainee packets or conduct link analysis between previous sites and current operations.

Military units now use the number of captured detainees as a rubric for success. What body counts were to the Vietnam era, detainee numbers are to today's soldiers. What separates good military units



A LEP and soldiers of 3rd Squadron, 2nd Stryker Cavalry Regiment, sift through debris to collect evidence. LEPs are often more patient and attuned to details than the uninitiated soldier, whose mission has traditionally been capturing detainees rather than cataloguing evidence.

from average ones is their ability to see that captured insurgents are tracked after the point of detention. A detainee released immediately after being captured essentially nulls the unit's actions in detaining the individual in the first place. Detainees are often released by higher headquarters several days after being captured because of weak detainee packets. Roughly more than one out of 10 detainees captured is eventually released. In certain units, one out of five Iraqis detained is eventually released for multiple reasons including poor evidence handling and lack of incriminating information.

Compounding the military's problem of capturing and detaining violent insurgents is the fact that many insurgents have become immunized to American military police methods and interrogation techniques. After five years of American presence, many hardcore insurgents have become schooled in the U.S. military's operating procedures concerning detainees. Insurgents simply clam up, or worse, they spread dissension and lies in order to further obfuscate our intelligence. Captured Iraqis have sown further confusion into U.S. military intelligence by seeding spurious reports. It is often impossible to comprehend what exactly is happening in a specific locale by simply reading intelligence summaries. Different detainees will spout different stories concerning who is working against Coalition forces. In essence, in some areas of Iraq and Afghanistan, the war has devolved into a pseudo-gangland setting where each sect or cell competes against the other by seeking to portray the other sect or group as guilty.

LEPs have assisted military units by cutting through this fog of insurgency. They heavily scrutinize detainee packets before packets are passed on to higher commands. Military units have found LEPs to be most effective as intermediaries between their intelligence section and their staff judge advocate section. LEPs are best positioned to review detainee packets because they understand exactly what information is needed in order to put away a detainee, while also providing a link to intel sections by highlighting certain trends that could possibly be analyzed to facilitate operations and intelligence briefs.

The success of LEPs is also unit driven. Certain units have had success with LEPs because they acknowledge inherent weaknesses within their intelligence sections and tactical human intelligence teams. On the other hand, some units still see LEPs as merely an encumbrance, with little to contribute.

The skills that LEPs possess are not beyond the means of the typical infantry soldier. Nonetheless, these are skills that must be learned through continual practice. SSE requires rigorous discipline and a calm, analytical mental state. Such attributes are difficult to achieve immediately after a direct-fire engagement or while a detainee's wife or children are crying in the courtyard. Still, soldiers with the aid of LEPs have greatly improved their police and investigative skills. Today's soldiers are versatile and understand the importance of biometrics, fingerprints, tactical questioning, and detailed descriptions concerning raids and captured insurgents. These skills, complemented by cultural understanding, are greatly contributing to the success of the American military at the ground level.

Embedded LEPs have also served as instructors in the units to which they are assigned. They have heightened the awareness of both leaders and soldiers of the detectivelike approach the military must use when approaching sensitive areas such as an IED blast site, discovered cache or mass gravesite. Traditionally, combat infantry units have developed internal standard operating procedures that have emplaced organic enemy prisoner of war (EPW) teams within each platoon. The EPW team is modeled and best designed for conventional wars. Infantry platoons need to go further than having EPW teams—they also need to develop organic SSE teams. Units preparing to deploy to Iraq should emphasize the need to develop these teams at the platoon level in



LEP Young trains Afghan police and soldiers in marksmanship. Embedded LEPs serve as instructors, and the success of the program is evident in the careful way soldiers gather available evidence, handle captured weapons and avoid mixing their fingerprints with those on insurgents' equipment.

order to incorporate skills relating to law-enforcement personnel that are used on a daily basis in the Army's present conflicts.

The current LEP program has succeeded in accomplishing its stated mission. As a result, the program managers are escalating the program so that more LEPs are introduced and embedded into military units. The success of the LEPs is evident on a daily basis. (b) (7)(E)

Another added component LEPs have provided is the mental approach and the paradigm of having a longer time horizon. LEPs temper the soldierly instinct to desire instant results. Instead, soldiers now understand that sometimes catching criminals and insurgents requires a longer time horizon. The conflicts today in Iraq and Afghanistan require soldiers to have a Dick Tracy skill set. Infantry soldiers must not only close with and destroy the enemy—they also need to ensure that evidence collection and detainee packets are thorough and detailed.

Captain Timothy K. Hsia is a graduate of the United States Military Academy. He is an Infantry officer assigned to the 2nd Stryker Cavalry Regiment.



Making Battlefield Forensics Work for US: Turning Forensic Evidence into Tactical Intelligence

by Lieutenant Colonel Mike Holmes

Introduction

There doesn't seem to be much crossover between tactical intelligence and the crime scene investigations we watch on the television show "CSI." The battlefield is typically not a place where lab-coated technicians can leisurely examine neatly isolated crime-scenes cordoned off with yellow police tape. And as bright and intelligent as our young analysts are, they are not trained scientists with specialized equipment.

But what we see on television is not an accurate reflection of forensic collection, investigation, and analysis. The dramatic emphasis on brilliant police work, scientists, and loads of bright, shiny technical kits hides the fact that there are a number of simple and effective tools we might easily use on today's battlefield. Incorporating some of these tools—especially in this counterinsurgency (COIN) fight—will help us provide our maneuver commanders with more a detailed and accurate intelligence assessment of the environment, and fast, accurate and targetable intelligence.

Forensics Defined

The recently published Department of Defense (DOD) Forensics Concept of Operation defines forensics as "the use of multi-disciplinary scientific procedures to establish fact."¹ This simply means examining evidence or material using the scientific method (critical thinking), and then analyzing it to confirm or deny what actually happened "on the ground." We already use this same thought pro-

cess to fuse the information we currently gain from our human and technical sources, the overall concept should not be new to us. The goal of DOD forensics is to "individualize, identify, associate, and scientifically link people, places, things, intentions, activities, organizations, and events to each other."² We analyze and incorporate forensic material into our intelligence fusion to help round out or complete our intelligence picture. This forensic process may be as simple as using photographs to help reconstruct the site of an attack or ambush, or as complex as uncovering latent fingerprints to make a match in the biometric database with a known individual. In all cases, it adds depth to our holistic intelligence analysis and can help to prove or disprove hypotheses on the enemy's most probable or dangerous course of action.

Forensics should be classed as Measurement and Signature Intelligence (MASINT), because it involves quantitative and qualitative analysis of a wide range of data which we derive from both technical collection (voiceprints, iris scans, etc.) and physical collection (latent fingerprints, DNA, blood spatter, tool marks, etc.) to establish fact. Other than the fact that most of the forensic material we collect is produced by human beings, there is no conceptual difference between the thought processes we use to analyze this material, and that which we collect from machines or technical devices. We are simply measuring the biological signatures produced by the human body.

Forensics Application on the Battlefield

We can apply forensics on the battlefield with a much lower profile than most police departments and crime labs for several reasons. The first is that police are held to a much higher standard of proof in order to gain a conviction in court. This is a major difference between the two functions of Law Enforcement and Military Intelligence, and it drives a lot of legal discussion between what is an appropriate level of proof to target a person in combat and what is appropriate to prosecute a person for a crime in civil society.

Police operating within a civil society and in a constitutional framework must wait for a crime to occur before they can level charges against a person. The basis of police work is to detect, solve and punish crime *after it has occurred*, and must by its very nature be *reactive*. Police dissuade potential criminals by their presence and reputation for effectiveness in solving crimes and prosecuting cases. Once a crime is committed, police restore justice by apprehending the criminals and bringing them before the court for trial. At trial, they must prove guilt “*beyond a reasonable doubt*.”³

Criminalists working in a crime lab spend a lot of time and energy making sure that their analysis is based on fact and free from errors. Any gaps in procedure, even something as simple as a break in the chain of custody or a missed testing procedure, can be used by a defense attorney to cast enough doubt on the case to sway a jury. For this reason, criminalists and forensic scientists are well drilled in documenting everything and showing their work. As a result, law enforcement forensics is precise and usually slow, with lots of back-checks to ensure accuracy and to leave no loopholes a defense attorney might exploit to cast doubt in the minds of the jury. Speed—which is not terribly important if the accused is already in custody—is sacrificed for accuracy and the sure knowledge that society is punishing the right suspect.⁴

Conversely, as Soldiers, our task is to destroy the enemy’s capacity to make war. If intelligence can identify and locate the enemy’s pressure points—or high value targets—before he has a chance to use them, then so much the better. We are actually *expected* to be proactive (Nathan Bedford Forrest

would have said, “*To get there firstest with the mostest.*”) Combat intelligence works on *probabilities*—not established facts. For targeting purposes, accuracy is reduced to determining the highest probability and speed may mean the difference between winning and losing. In this environment, forensic analysis need only provide a best estimate. The only jury that needs convincing is the Targeting Board—the only judge is the maneuver commander.

For forensics to work on the battlefield, the old aphorism that “*The Best is the Enemy of the Good Enough!*” is valid. Police work demands the best in order to protect the constitutional rights of law abiding citizens. Warfighting requires only the “*good enough*” answer to provide us with actionable intelligence and targeting information.

A second point that differentiates us from police is that we are not responsible for enforcing narcotics and drunk-driving laws. More than 75 percent of the evidence evaluated in U.S. crime laboratories is drug related.⁵ Accordingly, our domestic crime labs spend significant time and budget on toxicology equipment which is unnecessary for battlefield intelligence. Police have a valid reason to analyze and detect the presence of drugs in various materials, but we don’t. Therefore, some of the more technically complicated and delicate pieces of equipment that are commonplace to law enforcement forensics are superfluous to us. Having neither the burden of drug and alcohol testing, nor the need to prove our forensic analysis in court gives us a lot of freedom. It also means that we do not need the same level of education in order to do some of the basic forensics procedures and incorporate them into our intelligence collection and analysis. But it will require some additional training and tools, and perhaps most importantly, critical thinking to make it work and, as always in this era of “emerging doctrine”, a good dose of creativity.

The Six Forensic Functions

To effectively incorporate forensics into our intelligence cycle, we must first master basics: recognize, preserve, collect, analyze, store, and share.⁶ None of these are radically different than anything we already do. We can adapt already existing processes to fit the needs fairly easily, and there are courses and training resources available for some of the more esoteric skills that are required.

Battlefield Forensics Challenge

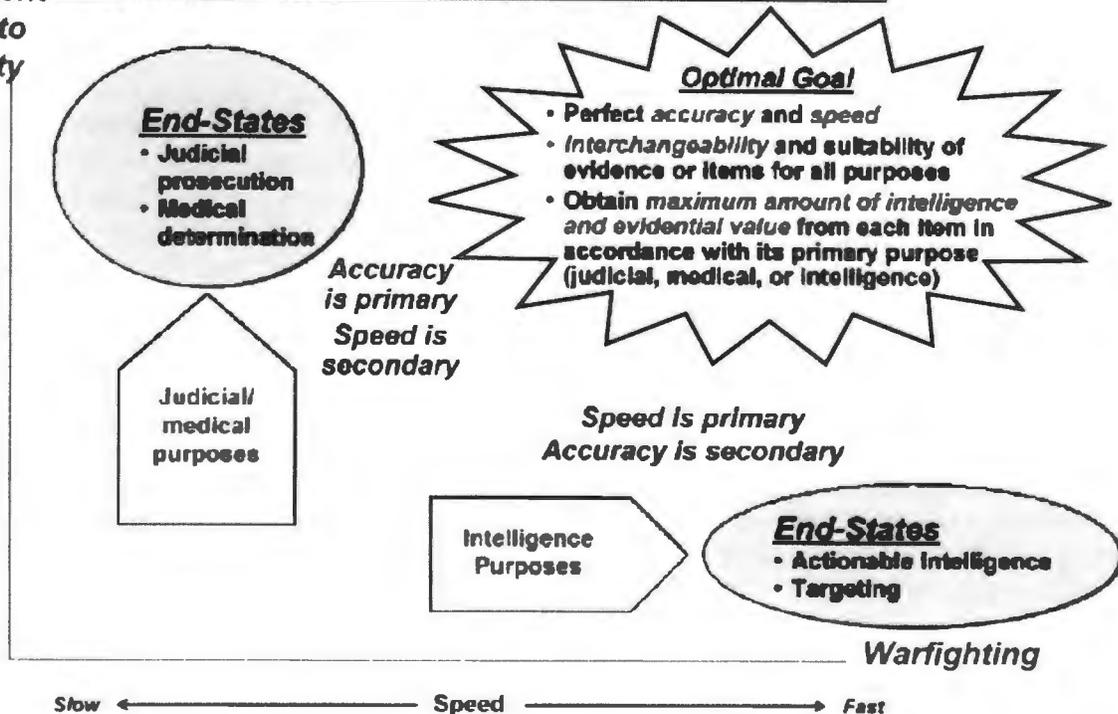
Speed versus Accuracy!

Law Enforcement
& Transition to
Civil Authority

High

Accuracy

Low



Recognize. The first forensic function is to recognize which items possess potential forensic value.⁸ When police investigate a crime scene, they have the leisure of time and security. They can put up the yellow tape and poke around looking for anything useful to help solve the case, and they can keep the scene as isolated and pristine as they like for as long as they need. Our lives are a little more difficult on the battlefield. Assuming we are not actually being shot at or exposed to the threat, we may have only minutes to assess the scene, photograph it, and scoop up what we want before the tactical commander says we must go. In order to make the best of whatever limited time we have, our collectors must go into each situation with a good set of priority information requirements (PIRs) or Forensic Collection Requirements. (You can already see “FCRs” coming down the acronym trail, can’t you?)

Forensics collectors must, at a minimum, copiously photograph the entire area that we can use

later to help their memories. Eyewitness testimony is a notoriously fickle and fleeting thing, subject to the stresses of sleep deprivation, shock, and Post Traumatic Stress Disorder.⁹ Photographs allow us to accurately record the moment, and analyze it later at our leisure. A series of photographs which tell a story can be taken relatively quickly by Soldiers with minimal training, but they have to know what to look for and it is our responsibility to tell them.

Just as with any PIR, we need to direct our Soldiers to look for things that will fill the gaps of our knowledge and allow the commander to make a decision on a course of action. (b) (7)(E)

The collectors need to have their collection requirements prioritized so that if the time and conditions do not allow, they can focus on the most important forensic material.

The more time-constrained the environment is, the more important it becomes for the forensics collectors to know what it is that you need in order to complete the intelligence picture.

Preserve. The second forensic function is to preserve, which involves protecting materials and data from the point of collection and for as long as they potentially hold intelligence or evidentiary value. The material we collect may some day wind up as evidence in a criminal court, perhaps even long after we have gone home. Therefore the materials we collect must be protected and preserved by available and reasonable measures to prevent contamination, loss or alteration.¹⁰

The first step in this process is to establish and maintain a chain of custody for every piece of material we take from a site. In concept, this is not very different from that which we already do with materials from detainees. The Provost Marshal or Judge Advocate officer can provide assistance in writing a standard operating procedure that is functional, and still preserves the evidentiary value for future use. We might also want to consult with the local crime lab and see what procedures it uses as a guide. The lab can provide us with some ideas on how to preserve the material from decay and decomposition as well, important things to know when collecting body parts, fluids and DNA!

Collect. We will need the most help and training with the third forensic function—collect. Just as one might think, this is the recovery of and accounting for any materials from a site, to include the documentation and the recording of contextual information, as conditions allow. This may even include some limited processing of certain items or areas of the site in an effort to detect additional relevant or hidden material or information. This may also include presumptive chemical testing, such as for explosive residue or for blood and body fluids, to confirm or deny the presence of relevant forensic material.¹¹

Human nature may drive us to try and control forensic collection ourselves and keep it internal to the S2 section, but common sense and a candid examination of our troops-to-task will show this is not possible. We do not now, nor will we ever, have

enough intelligence Soldiers to allow some of them to be spread around the battlefield with our maneuver Soldiers looking for forensic material. The only realistic way to get the “asset coverage” we need is to let our maneuver units do it. We need to train our infantry/armor/cavalry/engineer/artillery (have I left anyone out?) Soldiers on how to correctly collect forensic material, and bring it back to us in a useful, and useable, condition.

Happily, there are significant resources to help us do this. The Army already has a nascent forensic training program, targeted towards training maneuver Soldiers on how to collect forensic material in a combat environment. It is taught by a mobile training team (MTT) that will come to your location, and there is no cost to the unit except to dedicate thirty of its Soldiers for four straight days of uninterrupted training. Currently, the Battlefield Forensic MTT is sponsored by the National Ground Intelligence Center (NGIC), but in 2009 it is transitioning to the U.S. Army Intelligence Center at Fort Huachuca. The current program is forty hours of instruction crammed into 4 (10 hour) days, and focused on IED defeat. It covers tactical site exploitation and scene evaluation, forensic material recognition, photography, documentation, proper handling of materials to preserve biometric data, basic latent fingerprint collecting, and tactical questioning. It also includes training on the Handheld Interagency Identity Detection Equipment (HIIDE) if there are local HIIDE instructors available to leverage.¹²

Alternatively, the U.S. Marine Corps has an excellent set of training support packages (TSPs) on site exploitation.¹³ Either of these options is good, obviously hands-on instruction can be effective, but time consuming. A better option might be to supplement the MTT training with the Marine Corps package to allow for follow-on and refresher training.

Another place to go for additional training, and for more in-depth discussions on how to collect, analyze and correctly store your forensic material is the local law enforcement agency (LEA). Most major police activities have some sort of crime lab, and most of them are accredited to national standards so their procedures and processes will be largely uniform. Establishing a good working relationship with these activities would be an excellent place to start any S2 section training or orientation on what forensics is and how it can help us. Additionally, many LEAs

employ a corps of civilian crime scene technicians who specialize in forensic material collection and can cross train with the forensic collectors.

Analyze. The fourth forensic function is analysis, which may range from recognizing valuable forensic material on the site to in depth examinations in a lab or forensic facility. Regardless, forensic analysis attempts to scientifically link materials, people, places, things, intentions, activities, and events. It involves scientific instrumentation and equipment to compare known materials and information with unknown or unidentified materials, and the results may require interpretation and further analysis.¹⁴

To accomplish this task, we should first ensure we have established a system within our intelligence processes to account for the new information and data which forensics will provide, and a way to incorporate that information into our *Intelligence Fusion*. We should start with ourselves and assess our own abilities to *think critically* about our environment, our enemy, and the clues he leaves behind that give us vital insight into his composition, disposition and intent. This is not necessarily difficult, but we have not been trained especially well (or extensively) on how to think forensically. As a result, there is no uniformity across the force. Critical thinking is already a part of many of the various curricula at Fort Huachuca, but there needs to be much more of it, and it should be taught at lower education levels so our junior Soldiers begin their careers with some guidance and awareness for *how to analyze*.

But until doctrine and training do catch up, there is much that we as leaders can do to fill in some of this gap. First we should create a culture within our intelligence sections where we openly formulate, explore, discuss and evaluate ideas and information. In over eighteen months as the senior Division Analysis and Control Element (ACE) observer/trainer at the Joint Intelligence-Combat Training Center, I was able to observe and explore a variety of styles, methods and tactics, techniques, and procedures for producing intelligence. One of the best indicators I had for whether a group was doing well and “getting it” was simply to observe the activity of the students. If the ACE was quiet and orderly, with everyone’s face buried in a computer screen, it was seldom a good sign. Conversely, if the action

in the ACE was dominated by a group of people sitting around a table with various chart packs and notepads, looking very much like a scene from the play “*Twelve Angry Men*,” it was usually a VERY good sign!

Computers and mental models are great tools, but they will never replace a fact-based discussion between two sentient beings, at least not in any of our lifetimes. We can get data from computers, and assemble them in ways that are perhaps easy to visualize, but seldom (if ever) will we get a conclusive answer to anything but the simplest of logic problems. And bearing in mind we are ultimately targeting human beings, we are seldom presented with the simplest of logic problems!

If we are going to collect and analyze forensic material from the battlefield, we will be presented with an array of information which often just won’t fit with our preconceived ideas. We must be nimble enough in our thought, and rigorous enough in our criticism, to incorporate this information into the whole of the fusion process. We then must constantly evaluate it against all of the other information we receive from our other sources. Perhaps it is not too early to say that at some point, we might even incorporate forensics into a MASINT cell within the ACE.

To use the forensic material we plan on collecting, we need to develop our own tools and think through each problem for ourselves. We will need to progress past the point of *deductive reasoning*, where all of the steps are laid out for us and we can make predictions and test our hypotheses; to *abductive reasoning*, where some of the steps are missing and we are forced to arrive at plausible hypotheses using a fragmented mosaic of sometimes not very-well connected facts mixed with valid assumptions. It is a bit like the difference between simple mathematics, and algebra where we must solve for the unknown.

And as we think through the problem, we should bear in mind that good ideas do not have any military rank attached to them. If we open our process to active discussion and debate, then we must accept that sometimes the E-4 does indeed have a better grasp on the problem than the O-4, the real test of leadership is how well we use the assets (and ideas) we control, not in how often we are “right”.

Store. The fifth forensic function is to store. While battlefield forensics allows for a “quick and dirty” approach, at some point our strategic and operational goals will force a transition back to civil authority. As we transition from military to civilian control, we must expect increasing restrictions on our ability to act proactively. Although our analysis will not be held to the scrutiny of a judge and jury, the forensic material we collect may some day end up as evidence in a court case. Therefore, we will need to ensure that we collect, transport and store this material in such a way that it maintains its value for future civil court cases. This includes keeping an accurate chain of custody, and keeping any biological material from decomposing.

Materials and associated information should be maintained until their disposition has been fully adjudicated or resolved. The policies and procedures we develop in conjunction with the Provost Marshal or Staff Judge Advocate should dictate proper disposition. The effect of this function is that we may find our storage lockers rapidly filling up with a lot of old, and often not very nice, material. Moving this rapidly out of our custody and into the law enforcement community’s evidence lockers as soon as we are done with our analysis is the goal here. The less time it spends in our control, the less chance it will be called into question later in court.

Share. The sixth forensic function may be the most important—share. Information and intelligence that never makes it out of the S2 section is worse than worthless. Our commanders and Soldiers perhaps went to great risk to bring us this material, and we owe it to them to get our analysis back out to the force as rapidly as possible where it will do some good. This includes not only our own commands, but also any others who might have need of it. This has been covered in numerous articles and briefs, but the point cannot be made strongly enough that once we have made our analysis, share it with anyone else who might need to know it.

Forensic Material

The types of forensic material we are likely to encounter varies widely with the enemy and the environment, but there are some commonalities that we should be prepared to analyze and process.

(b) (7) (b) (7)(E)

This is neither as complicated nor as expensive as it sounds. These microscopes are more complex than the ones we may have used in high school Biology, but they are certainly able to be packed in a hard-case and set up in austere locations.

Every scene is likely to have some sort of body tissue or fluid left behind. (b) (7)(E)

DNA can positively identify an individual and also tell us a great deal about other things we might not otherwise be able to know without actually interrogating that individual and cross checking with known facts. (b) (7)(E)

Before we knew how to use DNA for evidence, Police used blood typing, and often there is a pretty good amount of that lying around. Blood typing does not give us the kind of conclusive evidence we can use in court to positively identify a person, but it does help us narrow down the field considerably, and it is something you can reasonably do yourself with proper training and minimal equipment. DNA is more precise than blood typing, and provides the positive identification needed to make convictions in court. By sticking to the aforementioned rule that, “The Best is the Enemy of the Good Enough”, we can use blood typing to screen individuals and at least exclude them as possible targets. The blood sample doesn’t necessarily have to be blood from bullet or combat wounds. (b) (7)(E)

And of course, there is still perhaps the oldest and most sure way of tying a person to the scene of the crime—fingerprints. An LP is nothing more than a print which isn't seen. It is the residue from the friction ridges on the finger or palm print left behind when a person touches something. The good thing about fingerprints is that they are unique to an individual, unlike DNA. (If you are an identical twin, your sibling will have the exact same DNA as you, but different fingerprints.) (b) (7)(E)

Having said this, LPs can also be extremely tricky to work with, especially when all you can get are partial prints or smudges. But, again remembering our burden of proof is much less than our police brethren, we don't need to be as picky—after all, we won't be taking these prints before a jury, just to the Targeting Board and the commander. Finding, developing and lifting LPs for later use is something which is taught in the aforementioned Battlefield Forensic Course, and while not terribly easy, it can be taught and learned with a little patience and practice. Using the emerging biometric technologies and Biometrics Automated Toolset (BAT) and HIIDE, we should soon be able to scan in LPs we have lifted from a scene, and check them for matches already in the database, or enter them into the database as an unknown to be matched later. The thing we must keep in mind, and continually remind our law enforcement brethren, is that we are not trying to build an airtight case, just a target package. Our analysis of the match does not have to be perfect, just close enough.

Getting Results!

We have now wandered far from what we can reasonably expect to do for ourselves during S2 section training time. To get the training proposed here, we will need to convince the S3, and probably the commander. To bolster our case, we might point out to them that one MTT can train up to thirty Soldiers, and that if each maneuver battalion had thirty Soldiers trained to collect forensic material, then there would be enough to sprinkle around each line company for the tremendous amount of work to be done. Forensic evidence, like any other evidence or information, tends to become more accurate in volume the more collectors we have in the field, the more bad guys we are likely to capture and kill,

which should go some ways towards convincing our commanders to support our efforts in this. The payoff is worth it in Coalition lives saved and terrorists caught or killed. Consider the following examples.

(b) (7)(E)

(b)
(7)
(E)

(b) (7)(E)

Commenting, FBI Director Robert Mueller said, "Identifying and reconstructing timing devices, explosives and producing an analytical product that is distributed throughout the military or throughout law enforcement in the U.S. may well enable us to prevent the use of those devices in the future."¹⁵

Daily, as our biometric databases grow and more evidence is collected, the number of success stories showcasing forensic material providing targetable intelligence increases exponentially. Given this increase, and the relative ease with which you can incorporate this capability into your current bag of S-2 tricks, why not explore the opportunity?

Conclusion

Nothing here is meant to suggest that we can create our own miniature crime laboratories, or that intelligence Soldiers will ever magically become forensic scientists. However, some of the simpler tasks of forensic collection and analysis are well within our competency and ability to accomplish with a little extra training, some small amount of equipment, and careful thought. But, we must keep in mind that, unlike the police, we are looking for the highest probabilities, not "proof beyond a reasonable doubt." We should temper the expectations of our commanders accordingly. The additional training which is readily available to our Soldiers is worth the effort if it results in faster mission accomplishment. As someone once described to me, in a COIN fight our job is like finding the right needle in a pile of needles. Forensic Science can be a very helpful tool if we are looking for that kind of a target.

Endnotes

1. OSD AT&L DDR&E, Capstone Concept of Operations for DOD Forensics, 18 July 2008. Director of Defense Research and Engineering, Washington D.C., 1.

[Redacted]

3. Julian R. Hanley, Wayne W. Schmidt, and Larry D. Nichols, Introduction to Criminal Evidence and Court Procedure, 6th Edition (Richmond, California: McCutchan Publishing Corporation, 2006)

4. Richard Saferstein, Criminalistics: An Introduction to Forensic Science, 9th Edition (Saddle River, New Jersey: Pearson Prentice Hall, 2007) 16.

5. Ibid., 248.

6. OSD AT&L DDR&E, Capstone Concept of Operations for DOD Forensics, 5.

7. Figure courtesy of TRADOC Capability Manager for Biometrics and Forensics (TCM-BF), Fort Huachuca, Arizona, 8.

8. OSD AT&L DDR&E, Capstone Concept of Operations for DOD Forensics, 6.

9. Laura Engelhart, The Problem with Eyewitness Testimony: A Talk by Barbara Tversky, Professor of Psychology and George Fisher, Professor of Law, Stanford Journal of Legal Studies, Accessed 15 November 2008 at <http://agora.stanford.edu/sjls/Issue%20One/fisher&tversky.htm>.

10. OSD AT&L DDR&E, Capstone Concept of Operations for DOD Forensics, 6.

11. Ibid., 6.

12. More information on the Battlefield Forensic MTT is available elsewhere in this issue of MIPB, or by calling the course manager at (434) 980-7128 or calling the TRADOC Capability Manager for Biometrics and Forensics at (520) 533-0303/DSN 821-0303.

(b) (7)(E)

[Redacted]

14. OSD AT&L DDR&E, Capstone Concept of Operations for DoD Forensics, 6-7.

15. CBS Evening News, *Forensics ID Bomb Makers in Iraq: FBI Uses Breakthrough Forensics to Track Homemade Bombs*, 17 January 2006. Accessed on 24 November 2008 at <http://www.cbsnews.com/stories/2006/01/17/eveningnews/main1216945.shtml>.

Lieutenant Colonel Mike Holmes is S2 for the 49th Theater Information Operations Group, Texas Army National Guard. He has served in a variety of assignments, to include brigade and battalion S2, and was an Intelligence liaison and U.S. Arresting Officer for the British led MND-SE in Basrah in 2005. A full-time civilian employee of Oberon Associates, he currently serves as the Operations Officer at the TRADOC Capability Manager for Biometrics and Forensics at Fort Huachuca, Arizona. He holds an MA in Diplomacy with a concentration in International Terrorism from Norwich University, and is a graduate of U.S. Army Command and General Staff College. He may be reached at mike.holmes1@us.army.mil.

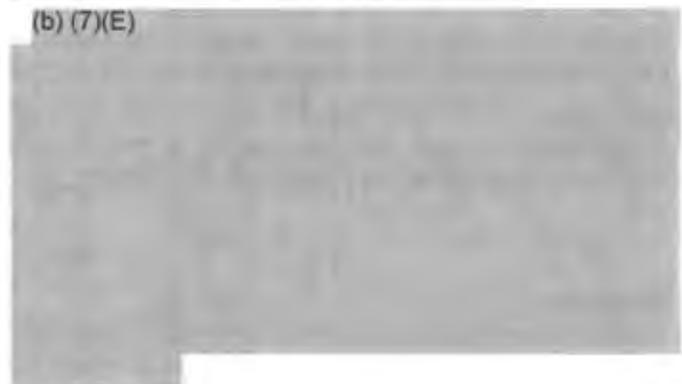
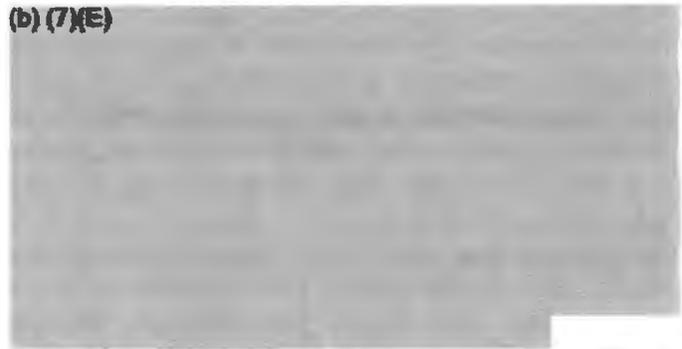


Introduction

The Combined Explosives Exploitation Cell – Iraq (CEXC-I) at Camp Victory is a unique collection of U.S. Army, Navy, and Air Force, British and Australian Army, and civilian subject matter experts working together to exploit and analyze improvised explosive device (IED) related material in order to identify and target bomb makers. The laboratories that form the umbrella known as CEXC-I work end to end, examining and exploiting different material properties as it is collected throughout Iraq.



Entrance to the CEXC complex at Camp Victory, Iraq.



Material flows into the CEXC-I triage 24 hours a day, 7 days a week. The labs process an average of 36,000 items a month. CEXC-I is staffed by thirty-four personnel including a Navy O-5 (who commands CEXC-I); EOD technicians; two Federal Bureau of Investigation (FBI) agents; one Alcohol, Tobacco, and Firearms agent; electrical engineers, and—in the Biometrics Lab—forensic technicians and photographers, and latent print examiners.



First Full Service Biometrics Lab

The National Ground Intelligence Center (NGIC) first proposed a full service Biometrics Lab for Iraq in July 2004. In December 2004, a single forensic technician was allowed to deploy to Iraq as an experiment. This first effort experienced many challenges and a few failures, but after ninety days the program proved to be a valuable tool which led to the recovery of forensically valuable material including fingerprints, one of which was subsequently matched to an insurgent. By June 2005, the Department of Defense (DOD) recognized the value of this fledgling program and provided additional funding from the Joint IED Defeat Organization (JIEDDO) to supplement the NGIC initiative. JIEDDO provided funding for a latent print examiner and a forensic photographer. Demand for analysis grew quickly as word spread throughout the battle space about CEXC-I and what it was able to accomplish. It wasn't long before NGIC was looking for funding to fill requests for additional personnel trained to biometrically exploit the material coming in from all over Iraq.



CEXC-I Biometric Laboratory.



EFP cache processed end to end in less than 48 hours.

JIEDDO has funded this program over the last several years and by August 2007 the Biometric Lab's staff grew to fourteen. In the month of January 2008, the CEXC processed a record 48,000 items and recovered more than 600 latent prints.

The concept of forensically exploiting IED related material spread to the Afghanistan Theater of Operations in March of 2006 when a Biometrics Lab was established within the CEXC complex in Afghanistan (CEXC-A). The lab was staffed by a forensic technician and photographer, and a latent print examiner. In September 2008, NGIC was asked to double the biometric staff in CEXC-A due to increasing amounts of material being turned in for processing.

Exploiting IED-Related Material

(b) (7)(E)



(b) (7)(E)

(b) (7)(E)

Conclusion

CEXC-I, in conjunction with the BOD in Clarksburg, West Virginia, produces an average of 34 identifications every month. That's 34 potential threats to the U.S. and its Coalition partners that were once anonymous bomb makers and insurgents who will not be able to enter into the U.S.

A sustained success rate like this is bound to draw favorable attention, and imitation is supposed to be the ultimate form of flattery, so it's reassuring to see the CEXC concept spreading. In late 2007, DOD decided to copy the methods developed by NGIC and the CEXC Biometric labs. In 2008, DOD began deploying additional labs within Iraq Theater of Operations for processing non-IED related material. These labs, called Joint Expeditionary Forensic Facilities (JEFFs), are being deployed in the hopes that they will realize the same success enjoyed by the CEXC Biometrics laboratories in Iraq and Afghanistan. (b) (7)(E)

Looking forward, the DOD

Forensic Intelligence Program and the CEXC concept are likely to become permanent expeditionary capabilities that can be deployed anywhere in the world on short notice, ready to strip the mask of anonymity from future adversaries. ✱

Erik Berg is currently working for Harding Security Associates as a latent print examiner and is assigned to the NGIC. His work has been featured on documentary television shows such as The New Detectives, 60 Minutes, and Forensic Files. His expertise includes photography, computer based imaging, latent fingerprint identification and crime scene investigation. He deployed to Iraq in September 2007, after 22 years in law enforcement, to work in the Biometrics Laboratory at the CEXC-I at Task Force Troy. In December 2007, Erik was promoted to the lab's Director. During February and March 2008, the Biometrics Lab recovered 2,344 latent prints of value from IED related material, and a record number of those (104) were identified during the same period. Erik can be contacted at (434) 951-4730 or via email at eberg@harding-security.com.



Introduction

With the beginning of Operations Enduring Freedom (2001) and Iraqi Freedom (2003), the U.S. military faced a new kind of war. Rather than waging conventional battles force-on-force, American Soldiers found themselves fighting an insurgency. Capitalizing on their anonymity, the insurgents effectively engaged U.S. forces with improvised explosive devices (IEDs) and rapidly disappeared back into the crowd, with little chance of being identified. (b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

NGIC Forensic Initiatives

In early 2004, recognizing this need to precisely identify and target the individuals responsible for attacks on U.S. troops, the National Ground Intelligence Center (NGIC) pioneered a solution for the Department of Defense (DOD), developing a strategy which incorporated unique collection and forensics exploitation techniques. (b) (7)(E)

(b) (7)(E)

(b) (7)(E)

NGIC also created the first weapons intelligence teams (WITs) to ensure that as much material of intelligence value as possible was being collected from the battlefield so that CEXC could forensically exploit the items for quick identification and targeting of the insurgent networks. In order to train the WITs, NGIC deployed DOD police officers with experience in detective work, crime scene processing, and SWAT operations. In December of 2004, the first of these hires deployed to Iraq to train the initial iteration of WIT. This training focused on how to quickly assess a scene, prioritize areas of interest, document through photography, collect material of intelligence value, collect

known and post mortem prints, and conduct latent print processing using proven "law enforcement concepts" that had been adapted to the battlefield environment.

Although CEXC immediately saw an increase in collection as a result of the newly trained WITs, the fledgling program still posed several challenges that had to be overcome. These issues related not just to forensic/collection training, but also to developing the critical infrastructure elements needed for efficiently transferring data and manpower between CONUS and OCONUS wartime efforts in order to achieve successful and real-time results. However, NGIC consistently adapted its program to meet these challenges, and the WITs it has since trained in both Iraq and Afghanistan have proven instrumental in the fight against the hidden enemy.

As the commanders on the ground began to understand the value of denying anonymity to the enemy, they requested that more units outside of the WITs be trained on the concepts of battlefield forensics and biometrics. NGIC rapidly addressed this need, establishing another training program designed for "door kickers" to augment the WIT capability. The building blocks for the training were already established, but the program needed to be tailored to address the specific obstacles faced by the warfighter.

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

- ◆ (b) (7)(E)
- ◆ (b) (7)(E)
- ◆ (b) (7)(E)
- ◆ (b) (7)(E)
- ◆ (b) (7)(E)
- ◆ (b) (7)(E)

Since 2005, NGIC has provided battlefield forensics training to over 1,200 service members, resulting in the collection of over 800,000 items. These collections have directly led to the recovery of tens of thousands of latent prints, the identification of hundreds of insurgents on the battlefield, and the capability to provide targeting support, force protection, and stronger homeland security. Furthermore, CEXC forensic cases presented in the Central Criminal Courts of Iraq have a record of 100 percent conviction.

Conclusion

The success of NGIC's endeavor in battlefield forensics is indicative of the Center's ability to adapt quickly in the face of a complex and constantly evolving threat. NGIC maintains this edge by conducting weekly teleconferences with the CEXC forensic lab, WITs, and counterinsurgency units, so that it can keep abreast of all material (old and new) collected on the battlefield. This constant dialogue with theater, together with NGIC's regular rotation of training personnel in and out of theater, provides the necessary intelligence and technology to stay ahead of the enemy and ultimately save lives.

As the next step in its effort, NGIC will conduct training at the Army combat training centers during Fiscal Year 2009, equipping over 1,000 deploying warfighters and 30 rotational brigade combat teams with the capability to collect forensically relevant material on the battlefield, material which will subsequently be used to target the individuals that pose a threat to our troops. Anonymity is one of the greatest weapons of an insurgent, and in denying this anonymity, battlefield forensics and biometrics have the potential to radically shift the paradigm of today's wars. Through its groundbreaking initiative, NGIC has supplied the critical capability that the warfighter called for, and the Center will continue to refine its program in the future to ensure that the needs of the Soldier on the ground are always met. ■

(b) (7)(E)

(b) (7)(E)

Captain Ryan Campbell has been the Deputy Chief of Forensic Operations and Training at NGIC, Charlottesville, West Virginia for a year. During this time he has been involved in the training of over 500 warfighters and over 100 leaders in battlefield forensics, the successful integration of training into the National Training Center, and has worked to establish an effective plan to ensure all units requesting training are supported. Previously, he served as a battalion intelligence officer within the 3IBCT, 10th Mountain Div (LI), where he spent an extended tour in Afghanistan, and as a company executive officer at Goodfellow AFB, Texas.



Introduction

The Biometrics Task Force (BTF) executes the Secretary of the Army's Department of Defense (DOD) Biometric Executive Agent responsibilities by leading DOD activities to program, coordinate, integrate, and synchronize biometric technologies and capabilities while operating and maintaining the DOD's authoritative biometric database to support the National Security Strategy. The BTF supports the Services and combatant commands by providing rapid responses to biometric submissions in support of force protection and the War on Terrorism. Part of this support involves efficiently and effectively searching biometric signatures developed by DOD agencies or organizations via forensic chemical or physical means. Biometric signatures such as latent fingerprints are generally visualized through chemical means using forensic science, digitized through image capture, and formatted as biometric files. These files are transmitted and searched through biometric systems to identify previously collected samples as well as registration for searching against biometric samples collected and submitted in the future.

In 2004, DOD developed and deployed its Automated Biometric Identification System (ABIS). As a mirror of the Federal Bureau of Investigation's

(FBI) Integrated Automated Fingerprint Identification System (IAFIS), the primary biometric modality for one-to-many searching is fingerprints. The ABIS processes Electronic Biometric Transmission Specification standard ten-fingerprint (tenprint) and latent print (LP) transactions against repositories of previous tenprint submissions and unsolved LPs. The Next Generation ABIS (NGA) 1.0, scheduled for deployment on 30 January 2009, will include the additional biometric modalities of palm, face, and iris for storage and matching.

The results of biometric searches are often vetted through the Intelligence Community (IC) for action as match reports. Because the LP process has a forensic beginning, a biometric middle, and an intelligence ending, it is important for all three communities to understand each component in order to maximize this process for the greater good. The focus of this article is on the biometric center that allows for the rapid identification of previously unknown threats.

Traditional LP Examination (LPE) Mission

Forensic science has traditionally supported the legal prosecution of criminals in U.S. or military courts of law. Federal, state, and local crime labora-

tories processed evidence while considering the end goal of sworn testimony. Because of the strict nature of the legal environment, forensic science has naturally evolved under a very controlled and stringent framework. Traditional forensic practitioners are respectful of control and “chain of custody” of the evidence from the first crime scene responder through the entire process.

Although this mindset is ideal for the U.S. legal system, it isn’t a very efficient process. There are many requirements of this process that are cumbersome in all but the most thorough applications. Although some aspects, such as chain-of-custody forms, can be easily adapted to the battlefield, other processes cannot. For example, in general crime scene processing, most items of evidence collected for further exploitation are completely documented prior to handling. This generally involves photography or video as the scene was preserved, follow-up with assigning each item a unique numbered evidence marker, photography of the evidence with the marker from a distance (from mid-range and close-up), and usually obtaining a final close-up photograph with a scale next to the item. Another example involves the traditional forensic process of thorough, sequential, multi-disciplinary processing of items. Within the U.S. legal system, there is often time for an item to proceed through the trace analysis section, the DNA section, the questioned document section, etc.

The reasons for this strict adherence to process and protocol are well founded in traditional case law. During court, the prosecuting authority has to build an air-tight case that doesn’t even leave a “reasonable doubt” in the mind of a juror deciding on guilt or innocence. Each case fact could introduce such doubt, so every case fact must be solid. There can be no room, for example, for a defense attorney to claim that a piece of evidence was planted at the scene or that a fingerprint was lifted from something other than what it was labeled as being lifted. Although the goal of “beyond a reasonable doubt” is necessary for legal proceedings, a lesser standard for certain aspects of the process may be acceptable for some military and intelligence applications.

A New LPE Mission

In the U.S. Central Command theater of operations, it has become necessary to explore every en-

abling technology to defeat the asymmetrical warfare tactics of terrorists. Because of the time and effort requirements to apply forensics in the traditional manner, it had never been applied on the battlefield to defeat an enemy prior to 2004. The Armed Forces Institute of Pathology has used forensic science to identify the remains of fallen soldiers, but true battlefield forensics was introduced as a new concept in concert with a push for more intelligence.

The main thought in taking certain facets of forensic science “forward” was simply that some additional capability was better than no capability at all. Previously, soldiers would simply leave or destroy items in place. Some items, like improvised explosive devices (IEDs), were collected for other types of processing. Expeditionary collection techniques were introduced to U.S. Marines and Special Forces who regularly encountered caches of items of interest. Instead of destroying the items, they were taught to collect items that, if they yielded LPs or DNA, would provide actionable intelligence on that individual. As with any intelligence, it significantly degrades with time, so the emphasis was on expeditionary exploitation even if traditional forensic ideals such as thorough, sequential processing were sacrificed.

This new approach has worked so well that two individuals per day remain in custody or are prosecuted based in part on biometric identification. Since 2004, nearly 2,000 LP identifications have associated nearly 1,000 separate terrorists as having touched items of interest. Over a dozen death sentences have been handed down in the Iraqi legal system as a direct result of LP identifications on items of interest. Numerous high-value individuals whose LPs appear on multiple items of interest have been successfully targeted as a result of intelligence that would never have been obtained if it weren’t for this new application of forensic science on the battlefield.

Continuous ABIS Operations

Even with forensic processing forward, an enterprise biometric system is necessary in order to search the biometric impressions developed on the battlefield. It doesn’t do much good to have a perfect human signature if you can’t search it through a file to make a positive identification. In 2004, the Biometrics Fusion Center (part of what became the

BTF) developed and deployed the fingerprint segment of the ABIS. An ABIS differs from commonly recognized AFI systems in that it includes other biometric search algorithms, such as face, iris, palm prints, etc.

ABIS Operations maintains a 24/7, year round support effort for DOD operations in multiple areas of operation. The branch is staffed with highly qualified and certified tenprint and LP examiners who provide feedback to submitting partners quickly and efficiently. ABIS Operations is also system and file type “agnostic”. Although the BTF recognizes the value of biometric standards (and in fact leads the DOD community in refining them), it also recognizes that, in a time of war, we cannot restrict incoming data not meeting a pre-determined standard. As an example, the FBI requires its customers to submit a complete tenprint record that has a minimum resolution (500 pixels per inch (ppi)). The ABIS Biometric Examination Services Branch (BESB) has accepted files and obtained positive results from submissions with as few as one fingerprint image and at resolutions as low as 200 ppi.

While the ABIS is designed to be a “lights out” (no human intervention) system when it comes to searching tenprint enrollments against the existing tenprint database, there are many lower quality tenprint files that can’t automatically be determined as an identification or non-identification. These are known as “yellow resolves” and require a human examiner to make the final determination. Currently, approximately 12 percent of all enrollments have to be reviewed by a human examiner. NGA will reduce that number to about 3 percent when it is fully operational due to multimodal fusion logic within the system, which combines the scores of different modality searches. ABIS averages about 20,000 biometric enrollments per week (with a high of more than 32,000) and roughly 2,000 images per month from our continental U.S. (CONUS) and outside the continental U.S. (OCONUS) partners for formatting, encoding, and searching in the ABIS. These biometric images of LPs are not considered forensic evidence (that would be the actual developed print) because ABIS is considered a tool for making a positive association. If the identification is to be used for court purposes, the examiner who developed the LP will prepare a courtroom package to demonstrate the identification outside the auspices of the bio-

metric system. In other words, the ABIS is a tool to find a match, but it still takes the forensic examiner to testify to it.

Biometric images are assessed by qualified LP examiners at the BTF, formatted, encoded, and searched against the ABIS (as well as the FBI’s IAFIS). A list of possible candidates is returned for the examiners to review. For the ABIS system, that list consists of 10 candidates. For IAFIS, the list could be as high as 80 but averages 68 candidates per print. The reason for this is that the ABIS database is about one-thirtieth the size of the IAFIS database. To improve the accuracy of searching against the larger IAFIS database, the “penetration” of each file is limited to 30 percent of the database. With some rare pattern types or known finger positions, this may only require one search that produces 20 candidates, but for some LPs without pattern information, up to four searches are required with each response returning 20 candidates.

LP Case Prioritization and Processing

LP cases are submitted to the BTF with a prioritization. This prioritization is determined by the submitting labs and is based on (in part) the circumstances surrounding the event from which the evidence was recovered. For example, LPs developed on evidence recovered from an IED event that led to the injury or death of a Coalition Soldier would be given the highest priority while those from some documents found at an abandoned cache would get a much lower priority. The prioritization is color coded: red is the highest, yellow is moderately high, and green or white are the least sensitive for timeliness in response. When a red case comes into the BESB section, all work on other cases is stopped and full attention is devoted to the red case. Turnaround time for a red case is measured in hours, while yellow cases can take a day or two and green cases can take up to two weeks. Currently, the turnaround time on “first looks” for all casework is less than seven days.

Within each case, other task-based prioritization is practiced. The highest priority is activity that leads up to ABIS LP candidate comparison. The formatting task involves opening each LP in Adobe® Photoshop® and conducting a series of image processing steps to transform the camera image into a standard resolution and standard image type re-

quired by ABIS. Each LP is different, and often factors such as background surface will cause unique distortion that must be manually corrected for accurate searching. Examiners almost always conduct image enhancement to increase the contrast between the ridges and the furrows during the formatting process.

The next task at the same priority is to encode the formatted LP in software that allows the examiner to place markers over the unique ridge endings and bifurcations (minutia) that the system uses to search the database. The minutia template is used by search algorithms (along with other information) to sift through millions of other biometric templates and rank them in order of likelihood of a match. Once the top ten candidate list is returned from ABIS, the next priority is the first look from an examiner and verification of a match if necessary. Beyond that, the BTF operates under a lower prioritization of follow-up task work, which includes the following:

1. IAFIS "Top Checks." When an LP candidate from a search against the IAFIS system is above a certain score threshold, it alerts the BESB to check the results.
2. File Re-encoding. A second examiner will re-encode LPs for resubmission against the system in order to achieve a higher accuracy rate than just one examiner encoding the print. Re-encoding LPs has been shown to yield about 10 percent more identifications than single encodings.
3. ABIS "Second Looks." A second examiner will review the response lists that have already been looked at during the "first look" process in order to achieve a higher accuracy rate than just one examiner comparing the candidates. Second ABIS examinations have been shown to yield approximately 7 percent more identifications than single examinations of response files.
4. IAFIS "First Looks." An examiner will review the remainder of IAFIS responses.
5. Manual "First Looks." An examiner will compare additional unsolved LPs in the case with all of the fingerprints of a known offender in that case. This occurs when some but not all of the LPs "hit" in ABIS. Generally, making additional identifications to the same individual is considered a lower priority task than making new hits to pre-

viously unidentified individuals.

6. IAFIS "Second Looks." This task is just like ABIS second looks but applied to the IAFIS responses to achieve a 7 percent accuracy increase in this task.
7. Manual "Second Looks." This is a second look at manual comparisons that would follow Manual "First Looks" to achieve higher accuracy.

When an LP is run against the ABIS and IAFIS databases without identification, the image is stored in the unsolved latent file (ULF). As new tenprint enrollments are collected and submitted to ABIS, they are automatically searched against the ULF, and scores above a certain threshold are presented to examiners for review. This is important because individuals involved in actions against Coalition forces leave LP evidence on material collected at the scene even before they have been detained or otherwise enrolled. Biometrics are not always in the system for comparison when the LPs are encoded and submitted, so an initial run against a database that does not contain the subject's biometrics will not result in an identification. The "reverse" or "after the fact" search can result in an identification of a newly detained individual to the item from an event that occurred on an earlier date. Unsolved latent matches (ULMs) still occur today on LPs entered in 2004. These ULMs occur about 25 percent of the time that an identification occurs. The subject's biometrics have already been obtained 50 percent of the time, and a "direct" LP search produces the match. The remaining 25 percent of all identifications are made as a result of manual comparisons. The current size of the ULF is approaching 50,000 images. As the known database and the ULF continue to grow, the likelihood of identifications against any single file also increases. Furthermore, through data sharing agreements with the Departments of Justice and Homeland Security, and in the near future with the National Counter Terrorism Center and the Terrorist Screening Center, this database of critical LPs will continue to be used to secure our national borders by stripping away the anonymity that terrorists so desperately strive to maintain.

ABIS Metrics

In November 2004, a case with several LPs arrived at the ABIS Operations center in Clarksburg, West Virginia, for searching. This case resulted in the first LP identification against the DOD ABIS in the

War on Terrorism. Although only a limited number of cases would be submitted during the remainder of 2004, this small inauspicious start would soon give way to a massive influx of biometric LP images for searching. In total, there have been nearly 10,000 cases containing nearly 50,000 LP images processed by the BTF since 2004.

The average LP case is a project in itself. Although cases vary in the number of images received, the average is about 5 LPs per case. Each LP search returns 10 candidates from ABIS and an average of 68 candidates from IAFIS, yielding 780 separate comparisons per case for full adjudication (counting verification by a second examiner). To adhere to reasonable turnaround times, sub-tasks are prioritized to obtain the highest probability of success as early in the process as possible. In one case, an IED event occurred in theater, items were delivered to the OCONUS laboratory, LPs were developed, captured, and transmitted to the BTF, searched through ABIS, identified to a subject who had been previously detained, and a report was provided back to theater within just four hours in total. Generally, this process takes days or weeks due to more realistic delays between steps in this multi-organizational process. But the facts speak for themselves—the ABIS Operations center supports this joint process to meet the goal for on-time, prioritized matching processes in support of force protection and national security.

BTF S&T Coordination and C&T Evaluation/Integration of New Technologies

Within the BTF, the Strategy Division is responsible for establishing the strategic direction for DOD Biometrics activities and enabling the employment of biometric capabilities. The Strategy Division includes two branches, the Futures Branch and the Concepts and Technology (C&T) Branch that work together with the biometrics and forensics communities to develop and provide future biometric capabilities that support the forensic mission. The Futures Branch coordinates the biometrics Science and Technology (S&T) efforts across DOD while the C&T Branch facilitates the movement of those technologies into prototype or developmental efforts for transition to the enterprise.

The BTF plays an important role in forensics S&T by pursuing three primary objectives in the advance-

ment of biometric technologies to enable forensics. First, the BTF synchronizes biometric technologies and capabilities that interface with forensic technologies and capabilities across DOD. Second, it interfaces with government, industry, and academia to develop and exploit the forensic/biometric cross-over technology base for future DOD capabilities. Finally, the BTF supports the coordination of efforts between the biometric and forensic S&T communities. The Futures Branch and C&T Branch work together to assist the BTF in accomplishing the above objectives in support of forensics S&T.

In addition to coordinating biometrics S&T efforts, the BTF is supporting two projects that directly impact the forensics mission. The first project is to develop a Latent FlyKit Capability for the BTF. The goal of this project is to produce a field kit that will allow latent print examiners to quickly respond to an event (e.g., natural disaster), capture LPs, and submit them to ABIS for matching. The second project is to develop a rugged, portable LP workstation. The goal of this project is to develop a prototype device to digitally capture latent fingerprints in a tactical environment. Together, these projects demonstrate how the BTF is helping to advance biometric technologies to support the forensics mission.

TNT Partnerships

Since 2005, the BTF has partnered with the Naval Postgraduate School and the U.S. Special Operations Command in hosting Tactical Network Topology (TNT) experiments. TNT provides a research venue to support the near-term needs of the warfighter by evaluating and improving biometric capabilities and communication architectures used to collect, store, and transmit biometric data. Experiments and concepts conducted in the TNT emphasize wireless networks, unmanned/autonomous vehicles, sensor networks, situational awareness, net-centric applications, target tracking and identification, and biometric identification and verification. Measures of performance for each technology are collected by Special Operations Forces operators and engineers/technicians. Requirements gaps and technical shortfalls are then addressed and improvements are made for the next quarterly experiment.

The BTF uses the TNT environment to evaluate current and emerging forensic and biometric technologies in a simulated operational environment. The BTF's C&T Branch considers validated require-

ments and biometric capability gaps, gathers experimental biometric and supporting technologies, and weaves these technologies into operational events and scenarios with detailed objectives. The BTF assists experimentation partners, including various branches of the military, the combatant commands, industry, and national laboratories to conduct experiments. Actual assessments of the experiments are conducted by assessors, such as the West Virginia Army National Guard's (NG) 19th Group Special Forces, Special Operations Research and Support Element, and the Joint Interagency Training and Education Center (JITEC).

BTF experimentation in forensics has been a part of TNT for several quarters. Most of the forensic technologies center on alternate ways as well as more time efficient means to capture LPs. Technologies have shown ways to dust, lift, and digitally convert LPs, thus reducing time spent on a specific target. Other participating technologies have shown alternate ways to capture LPs from surfaces without using lift tape.

Although biometric experimentation in TNT is relatively new, it has grown to a point that necessitates expansion into Camp Dawson in Kingwood, West Virginia, and the Center for National Response (CNR) in southern West Virginia. Camp Dawson provides a realistic training landscape that affords participants the opportunity to meet certain challenges of their wartime missions. The facility is also used by the West Virginia Army NG, the Army NGs of other states, Army Reserve, Reserve Officers' Training Corps, and other Active and Reserve components of the Air Force, Navy, and Marine Corps. CNR is an operational component of the JITEC, which is an NG training activity operated by the Chief, NG Bureau and the Adjutant General of West Virginia. It is a flexible Weapons of Mass Destruction training complex that provides multi-scenario exercises for the military or joint operations with military and first responders.

BTF Test and Standards Conformance

The Test and Standards Conformance (TASC) Branch exists to plan, conduct, and report the results of events, tests, simulations, experiments, and evaluations of the nation's investments in biometric-enabled information technologies, programs, and products necessary to support the

U.S. Armed Forces. In that context, the continued objective is to rapidly test quality biometric technologies that satisfy user needs with measurable improvements to mission capability. In Section 112 of the Emergency Supplement Act, 2000, Public Law No. 106-246, the Department of the Army was designated as DOD's Executive Agent for developing and implementing biometric technologies. Accordingly, on 27 December 2000, Deputy Secretary of Defense Rudy de Leon signed a memorandum titled, "Executive Agent Appointment." In this memorandum, Mr. de Leon directed the Secretary of the Army to "establish a Biometrics Fusion Center to acquire, test, evaluate and integrate biometrics, and to develop and implement storage methods for biometrics templates." As such, the Biometrics Fusion Center's (now part of the BTF) testing capability was created. Since 2001, the TASC Branch has employed rigid testing plans and principles to ensure that the collection, enrollment, matching, storage, updating, and sharing of biometric technologies is accomplished in a secure, timely, accurate, usable, and reliable manner.

The mission of the TASC laboratory is to plan, conduct, and report the results of events, tests, simulations, experiments, and evaluations of biometric-enabled technologies to decision makers so they can ensure that our warfighters have the right biometric capabilities for success across the entire range of military operations. To accomplish this, TASC engineers apply basic test principles to discover, demonstrate, and evaluate biometric ideas, concepts, technologies, or products across the DOD Biometrics Enterprise.

DOD Directive 8521.01E, DOD Biometrics, defines the testing scope for the BTF and establishes conduct for biometric test activities. Conformance to approved biometric standards is paramount to the technology acquisition process. In addition to knowing the extent to which a technology is able to collect, transmit, store, retrieve, manipulate, match (if required), and display biometric and personal data, the BTF must also know that the technology will meet critical issues of mission performance, usability, information assurance, and supportability. Such assurances are provided as a result of the test and evaluation functions.

The TASC Branch evaluates technologies through conformance evaluations, scenario evaluations,

and informal tests, evaluations, or assessments. Examples of biometric testing done in the past include:

- ◆ Conducting biometric standards conformance testing for all products, programs, and services.
- ◆ Providing support to DOD acquisition organizations in developmental testing, systems integration, and/or independent verification and validation of biometric systems.
- ◆ Maintaining awareness of the biometric marketplace and evaluating commercial/government off-the-shelf products useful to federal government agencies.
- ◆ Supporting DOD operational test agencies for the conduct of formal developmental and operational test and evaluation activities that determine system effectiveness, survivability, and suitability.

Having evaluated more than 300 biometric technologies over the past eight years, TASC engineers have a vast understanding of the capabilities and limitations of biometric systems and devices deployed to support the War on Terrorism. Today, the TASC Branch is seeing more handheld collection devices preparing to provide a forward latent collection and matching capability as well as more local biometric matching systems with latent print capabilities. These systems will soon provide warfighters with a forward capability to collect, store, match, and share latent fingerprint images and information with enterprise systems according to DOD standards.

BTF Challenges

Although the BTF is maintaining a superior position with regard to identity dominance, there are still challenges to overcome. Limited bandwidth from theaters of operation to the enterprise ABIS system continues to plague response times back to the soldier. Forensic laboratories in remote locations have to use satellite technology to transmit very large digital case files for processing. Generally, it is more cost effective to conduct all biometric activity within CONUS. For this reason, most of the raw unprocessed camera images of the biometric are provided to the BTF for formatting. Although this is necessary for accurate processing, these images can sometimes reach 20 or 30 megabytes each, and some cases literally have hundreds of images of LP biometrics.

The workflow within the BTF is being re-engineered

for maximum efficiency. In 2004, Excel[®] spreadsheets and manual file systems were sufficient for the volume of casework, but the BTF is in the process of planning and implementing automated case management systems and central server job queues for comparisons. Although the transition period is ongoing, the BTF remains able to perform the highest priority task work in support of theater operations.

The lower priority task work, such as IAFIS examinations and 2nd level examinations, continues to become backlogged. New strategies are currently being explored, such as standing up a remote examination services capability, training and involving Wounded Warriors or their caregivers, and even involving examiners from other departments in the comparison task work. Although the current comparison backlog is approaching 10 million separate comparisons, these programs along with an aggressive staffing strategy are anticipated to bring the backlog under control within the next few years.

Finally, the challenge of forensic training and awareness will be an ever-looming battle in these early years of new battlefield forensic capability. There seems to be constant bombardment of traditional forensic ideals working against the new expeditionary battlefield forensic model. Commanders at all levels need to understand what battlefield forensics was intended to provide and how the very process to achieve those results may require falling short of some institutional laboratory forensic procedures and processes. They also need to understand how those forensically developed biometric signatures can be transmitted to the enterprise biometric capability for maximum value back to theater. Training our troops how to preserve and collect items of interest and conduct some limited exploitation of immovable items is a relatively straight-forward exercise that just requires the right sponsorship, staffing, and execution. Obtaining the doctrine and policy to support this new type of training is the current challenge.

BTF Future

There are some great future capabilities in store as the BTF continues to support the warfighter through maintenance and operation of the enterprise biometric capability. The upgrade to the NGA will allow more efficient matching of forensically developed biometric signatures. As we continue to identify pro-

cess bottlenecks, the root causes will be identified and corrective action will be undertaken to solve the actual issues. In fact, the BTF has formed a Tiger Team for the Enhanced Capture and Detention of Terrorists to troubleshoot some of the non-standard forensic and biometric issues that contribute to the wrongful employment of foreign nationals or wrongful release of detainees.

The BTF is forging new ground in research on placing LPs on watch lists. For good quality prints, there is demonstrated value in lights-out searching as long as follow-up human examination is employed for potential matches. Look for clearer delineation between automated face recognition and true face identification by trained personnel for absolute matching. There is a big difference between the standards for face recognition systems versus the image quality standards necessary for positive identification by a biometric examiner of the unique face characteristics, such as moles, freckles, small scars, unique texture, etc.

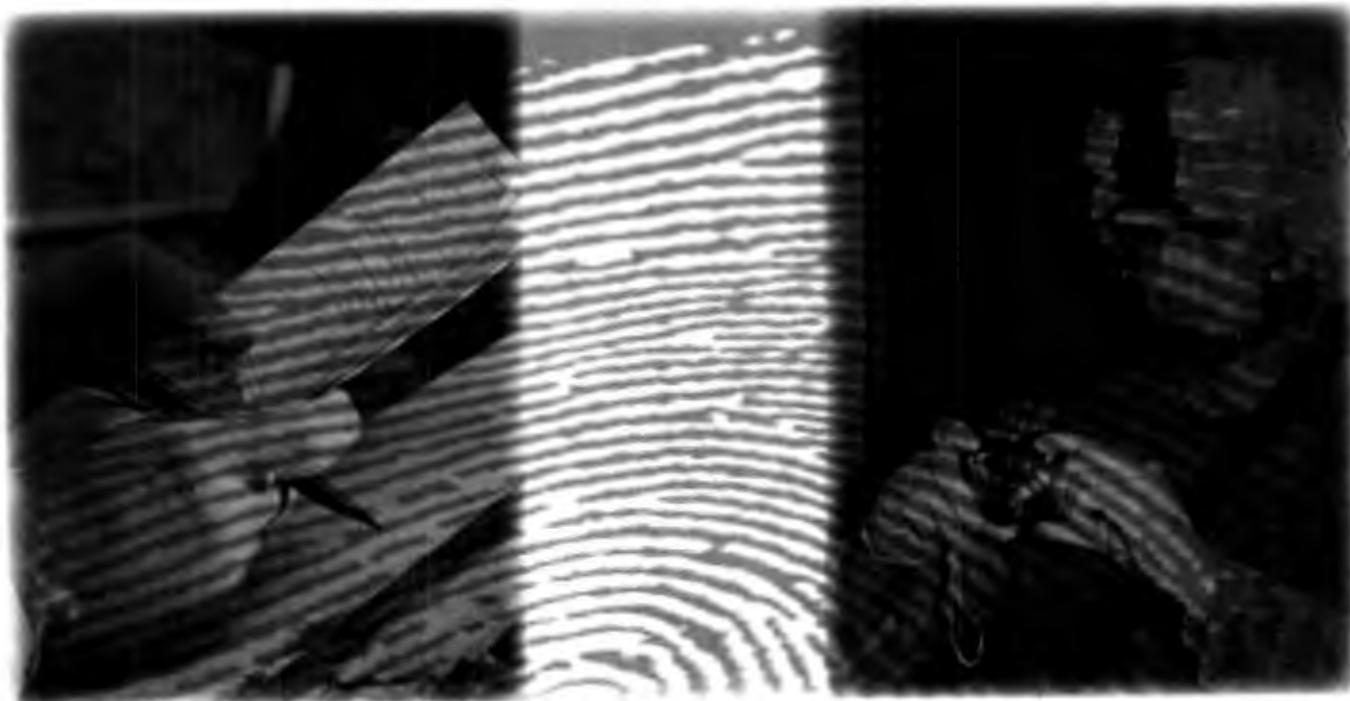
Conclusion

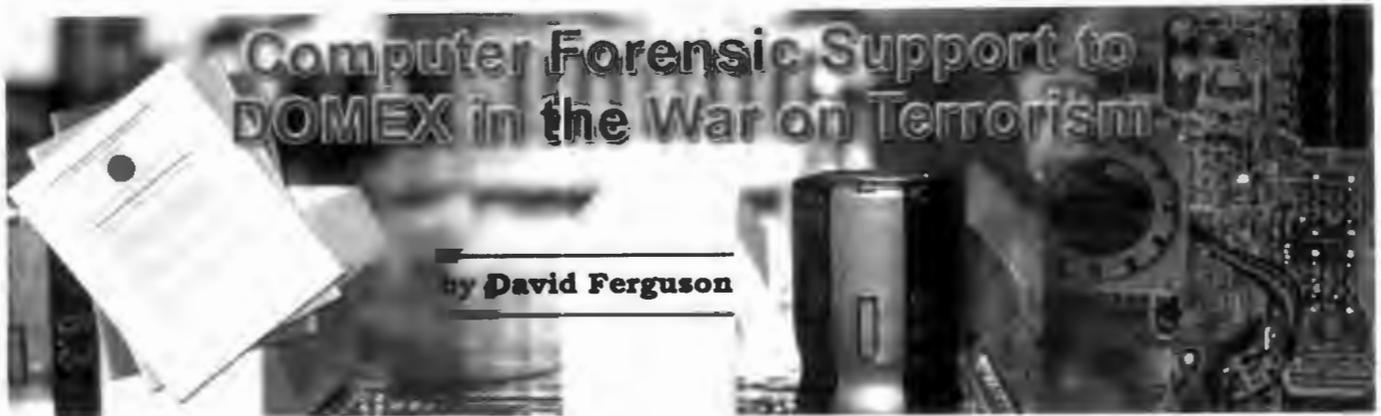
As the BTF looks toward the future, our mission is at the forefront: to lead DOD activities to program, coordinate, integrate, and synchronize bi-

ometric technologies and capabilities and operate the DOD's authoritative biometric databases to support the National Security Strategy. The BTF recognizes that forensic science is a major contributor of biometric signatures and serves as an enabler to the BTF in support of our critical mission. Through productive collaboration and coordination, the DOD forensic community and the BTF will continue to provide a valuable service to our men and women in uniform and to the agencies and organizations that protect our homeland from foreign and domestic terrorism. *

Kasey Wertheim is President and CEO of his own company, Complete Consultants Worldwide, LLC, supporting the DOD BTF by managing science and technology projects related to forensic science. He provides subject matter expertise to the DOD and is actively involved in the biometric and forensic communities. He spent seven years as a forensic scientist and crime scene analyst prior to becoming heavily involved in forensic technology. Currently, he serves as Chairperson for the Biometric Committee of the International Association for Identification (IAI) and is an IAI Certified Latent Print Examiner, Distinguished Member, and Editorial Board Member. He completed a short tour of duty in Iraq and Afghanistan as part of an IC laboratory improvement effort and spent one year on contract with NGIC.

FORENSIC FOCUS





Computer Forensic Support to DOMEX in the War on Terrorism

by **David Ferguson**

The views expressed in this article are those of the author and do not reflect the official policy or position of the Defense Intelligence Agency, the Department of Defense, or the U.S. Government.

Introduction

On February 6, 2008, a U.S. Military spokesman for the Multi-National Forces-Iraq revealed a series of videos from captured al-Qa'ida Network (AQN) media. The videos depicted children training to detain, kidnap, and kill innocent Iraqi civilians. U.S. officials said "the video was being released to illustrate al-Qa'ida's increasing willingness to use women and children to carry out its objectives."¹ The disclosure was covered by all of the major news outlets: CNN, Al-Jazeera, the New York Times, and many others. News releases like these are having an effect on al-Qa'ida's ability to recruit. This is one of the powerful ways that captured documents and media are affecting the battlefield today.



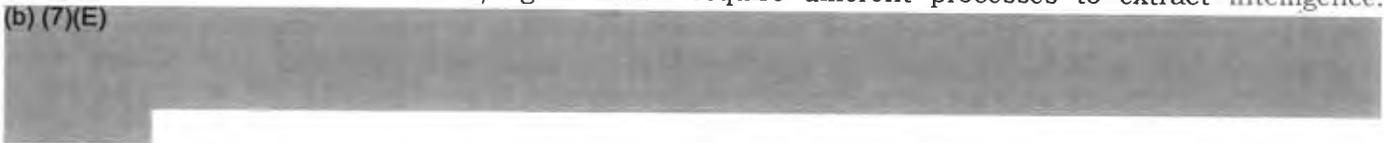
Stills taken from captured al-Qa'ida video.

Making sense of the papers and media captured in the War on Terrorism is the domain of Document and Media Exploitation (DOMEX/MEDEX). Intelligence Community Directive 302 defines DOMEX as "the processing, translation, analysis and dissemination of collected hard copy documents and electronic media, which are under the U.S. Government's physical control and are not publicly available." The implication of this definition is that these captured documents and media are not open source documents pulled from newspapers or the Internet.

Paper or Plastic?

Paper documents and electronic/digital media require different processes to extract intelligence.

(b) (7)(E)



(b) (7)(E)



Unlike documents, electronic media isn't immediately "consumable." It isn't possible to pick up electronic or digital material and read it. The extraction of documents, audio, video and photographs requires a methodical approach to get the most from the material with the least amount of resource expenditure. The exploitation of computer based media is the purview of MEDEX, a subset of DOMEX. MEDEX relies heavily on the science of computer forensics to extract this information.

Computer Forensics

To understand where and how the discipline and the science of computer forensics developed, one only has to look in a dictionary. There are two definitions for forensics, one has to do with debating and the other describes "the application of a science to a legal or law enforcement problem." To put it another way, computer forensics has developed into the science of collecting and analyzing digital data in order to present it in court as evidence. Typically, computer forensics is performed by a law enforcement agency or lab, such as the Defense Computer Forensics Lab, to prove or disprove an allegation of a violation of the law. Most of the time, these violations are traditional offenses such as fraud, sexual assault, etc.

(b) (7)(E)



(b) (7)



(b) (7)(E)



(b)



(b) (7)



(b) (7)



(b) (7)



(b) (7)



(b) (7)



(b) (7)



MEDEX

MEDEX applies computer forensic tools to the DOMEX space at least on the electronic/digital media and provides the intelligence function with information about the formation, organization, personnel, operation, funding, logistics, command structure, intentions, as well as other valuable information. The process modifies the computer forensics model to meet the needs of the combatant commander, mostly to increase the speed of obtaining of the information. As speed is of the essence, so some of the aspects of the rigorous law enforcement approach are dropped or modified to increase the speed.

The two best examples of digital information in the public domain are hosted at the U.S. Military Academy Counter Terrorism Center (CTC). The CTC takes documents released from the War on Terrorism holdings, performs unclassified analysis, and releases the results to the public. Two good examples are "Cracks in

*the Foundation: Leadership Schisms in al-Qa'ida 1989-2006*³³ and *“Al-Qa'ida's Foreign Fighters in Iraq: A First Look at the Sinjar Records.”*³⁴

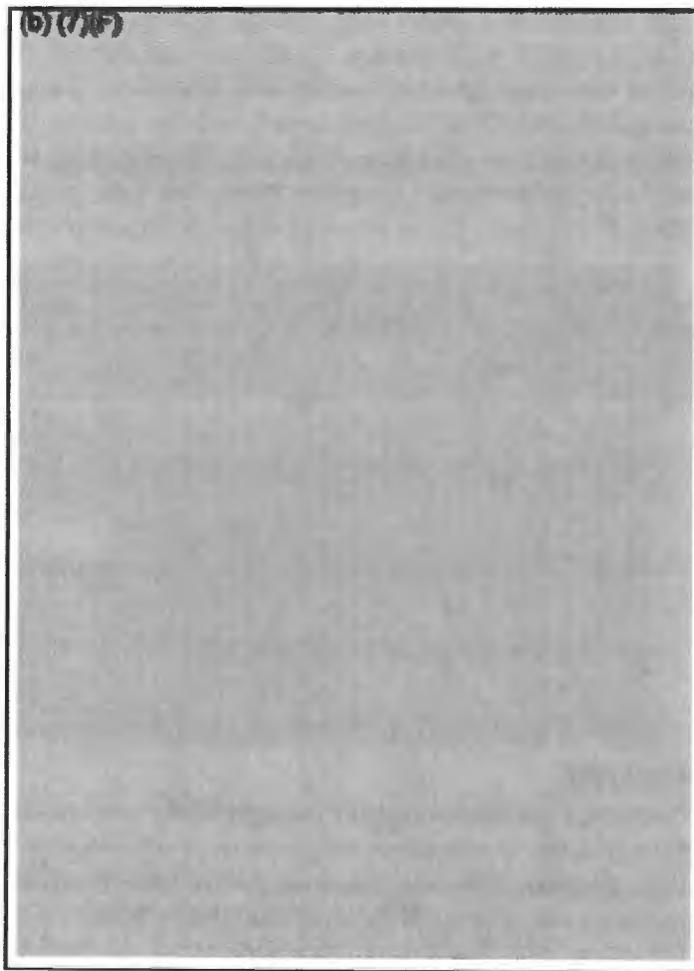
The former reviews a number of letters between members of the al-Qa'ida leadership, revealing their weaknesses. This includes letters like the one from Zawahiri to Zarqawi³⁵, telling Zarqawi to avoid using violence against the Iraqi civilian population or risk alienating it. It is a more strategic set of documents, whereas the latter is both strategic and tactical.

*“Bombers, Bank Accounts, and Bleedout: Al-Qa'ida's Road In and Out of Iraq”*³⁶ is an analysis of a collection of records released to the public through the CTC. The records contain biographical information on around 600 foreign fighters that are believed to have entered Iraq from Syria. The Sinjar Records include a biographical description of each person, and in many cases, photographs. The tactical importance is obvious; one can look for these individuals in detention and can check any new detainees against this list. An additional benefit is that every nation now has access to this information so it is unlikely that the 600 named in the records will be able to board an aircraft for the U.S. or Europe any time soon. Some of them are from Europe; if they ever get home they will not have a warm reception.

The CTC also had access to other bureaucratic information from this collection, here is its synopsis of the Sinjar Organization:

“The Sinjar documents provide a striking insider's view of the management challenges facing al-Qa'ida in Iraq's Islamic State of Iraq (ISI). The documents reveal leaders struggling to balance the control required to achieve their political goals against the security required to survive. The ISI, like any terrorist organization, faces a difficult task in a hostile operational setting. First, it must control the use of violence as a means to achieve their specified political ends. As the organization itself has acknowledged many times, too much violence or inappropriate fundraising efforts can damage the cause as much as doing too little. Second, the ISI must sustain itself with limited funds, placing a premium on financial efficiency and oversight. Third, the ISI must maintain this calibrated use of force in an environment where becoming known to Iraqi or American government forces leads to operational failure.

*These three tasks place conflicting demands on the ISI. The more the organization exercises control over its operatives—by using organizational tools such as tracking spreadsheets, expense reports, and standardized policy memoranda—the less secure it becomes. Exercising control in this manner requires additional communications that can be intercepted and creates direct links between senior leaders and operators who are more likely to be identified and captured by government forces. Moreover, because these documents often include names and provide evidence about operational practices, they make ideal raw material for intelligence organizations seeking to target the ISI. The ISI thus faces the same tradeoffs between security and control that have troubled terrorist organizations from the 1890s to the present. The Sinjar documents provide further insight into how al-Qa'ida's ISI is challenged by these tradeoffs.”*³⁷



(b) (7)(E)

The CTC report is an enlightening read and starts to crack open the door on what information can be gained with DOMEX.

What Can You Lose?

While the CTC report exemplifies the successful application of a computer forensic approach, all too often it is not used—and at a high cost, as the Colombian government experienced recently. The politically-sensitive raid on a Revolutionary Armed Forces of Colombia (FARC) outpost in Ecuador uncovered a laptop full of documents incriminating President Chavez of Venezuela.⁸ Unfamiliar with computer forensics, Colombian government officials turned the laptop on and began reading files, changing access times. As a result, the credibility of the information was significantly damaged. The article, “Chavez: Interpol Report a ‘Clown Show’”, demonstrates the damage of not following good forensic practices. (b) (7)(E)

An Approach

Many operators/intelligence personnel want to excise the “law enforcement centric” requirements of computer forensic procedures. The exploitation process must be fast, but it can’t be at the expense of the successful prosecution of the captured terrorists/detainee/war criminal. Over the last few years, almost all of the important material has ended up in a court system (U.S., Guantanamo, the World Court, Iraqi court systems, etc.) Often, the important information is not identified until the media is reviewed, and at times, this process can take several months.

(b) (7)(E)

When fighting insurgents, one approach is to work like the police. The police have been fighting organized crime for a long time and have had to seek out the bad guys moving “amongst the people as a fish swims in the sea,” to put it in the words of Mao Tse-Tung. Computer forensics is a crime fighting tool developed by the police that military commanders can use to reduce collateral damage.

Using computer forensics on the battlefield, however, presents many challenges. A firm legal frame work does not exist, there are no elements of proof, and the MEDEX technician/examiner generally does not speak the language of the material in question, so linguists and intelligence analysts often have to interpret the results.

(b) (7)(E)

(b) (7)(E)

(b)

(b) (7)

(b) (7)

(b) (7)

(b) (7)(E)

(b) (7)

Absent from this list above is a warrant, and in all likelihood, elements of proof; however, there may be a detainee that is suspected of some kind of insurgent activity. The MEDEX team needs the context information to do the same kind of focused search that is performed by a forensic examiner in the law enforcement realm. Without the context, it is really difficult to identify things of interest.

The chain of custody information is required to return the property back to the owners if they are released or to present as evidence at trial. In many cases, insurgents captured on the battlefield will face some sort of trial. A trial implies evidence, which necessitates the production of a chain of custody for any

evidence presented to the court. "Do no harm" falls right in line with returning the individual's property. If an operator turns on an detainee's computer and begins to review the files, the data will be poised for court. It is best to work from a copy. In fact, having that perfect copy in more than one place allows parallel exploitation. The chain of custody information can also be used to provide context, it is essential to maintain the link of how something was acquired to the media images so that they maintain their intelligence value. Without context, the data derived from a piece of media is of less value.

In a perfect world, copies of all captured media would be reviewed at a tactical, theater, and National levels. At each level, one would want to sift for different kinds of information. (b) (7)(E)

Also, the span of time that a copy of the data is of interest expands as it moves up the levels. At the National level, all data should be available for as long as the conflict is active. The importance of it changes, and older information has to be revisited from time to time, emphasizing the necessity of a complete, perfect copy for intelligence reasons. What is insignificant now may be relevant within a month or even a year. (b) (7)(E)

Conclusion

Applying computer forensics to the battlefield can provide the commander with an information source that has rarely been available in the past. This is particularly important in asymmetrical warfare. The critical information for operators and intelligence personnel to know is that many of the law enforcement procedures that take time add value and can make a big difference in the outcome of a campaign—or even a war.

Endnotes

1. "Al-Qaeda Video Shows Boys Training to Kill, Kidnap," USA Today, 26 Feb 2008 at http://www.usatoday.com/news/world/iraq/2008-02-05-camps-usat_N.htm. Accessed 23 October 2008.
2. "Chavez: Interpol Report a 'Clown Show'," CNN, 15 May 2008 at <http://edition.cnn.com/2008/WORLD/americas/05/15/colombia.computers/index.html>.
3. "Cracks in the Foundation: Leadership Schisms in al-Qa'ida 1989-2006," USMA CTC, September 2007 at <http://www.ctc.usma.edu/aq/aq3.asp>. Accessed 6 May 2008.
4. "Al-Qa'ida's Foreign Fighters in Iraq: A First Look at the Sinjar Records," USMA CTC at <http://www.ctc.usma.edu/harmony/pdf/CTCForeignFighter.19.Dec07.pdf>. Accessed 6 May 2008.
5. "Letter from Zawahiri to Zaraqawi," Office of the Director of National Intelligence at http://www.dni.gov/press_releases/20051011_release.htm.
6. "Bombers, Bank Accounts, and Bleedout: Al-Qa'ida's Road In and Out of Iraq," USMA CTC, at http://www.ctc.usma.edu/harmony/pdf/Sinjar_2_July_23.pdf. Accessed 25 Oct 2008.
7. Ibid.
8. "Seized Laptop Shows Chavez's Rebel Ties" ABC News, 5 March 2008 at <http://www.abcnews.go.com/International/wireStory?id=4390879>. Accessed 29 May 2008.
9. "Chavez: Interpol Report a 'Clown Show,'" CNN, 15 May 2008 at <http://edition.cnn.com/2008/WORLD/americas/05/15/colombia.computers/index.html>.

Employed by the Defense Cyber Crime Center, David Ferguson is Chief Scientist at the National Media Exploitation Center, where he works with the Defense Intelligence Agency and the Office of the Director of National Intelligence, Assistant Deputy Director for National Intelligence for Open Source. He gained his experience in DOMEX as the former Director of the Defense Computer Forensics Laboratory. Mr. Ferguson may be reached at David.Ferguson@dia.mil.

The Coalescence and Convergence of the Forensic, Intelligence, and Biometric Communities



Introduction

The asymmetrical nature of recent enemy terrorism related tactics has caused the Department of Defense (DOD) to closely examine every tool in its arsenal to stay ahead in the War on Terrorism. Within the DOD, the intelligence, forensic, and biometric communities have existed in support of different missions for quite some time. Although the roots of each community can be traced back over a century to very different beginnings, the battlefield of the last decade has witnessed the very real convergence of these three distinct communities.

Historical Aspects

The most familiar community to this readership was sparked in 1885 when an Army general was unable to answer an inquiry from President Cleveland for a relatively routine piece of information. The Military Information Division of the Army grew exponentially throughout the remainder of the 19th century leading up to its prominent role of intelligence gathering in the Spanish-American War and in every war in the 20th century.

The broad scope of the forensic community makes it difficult to pin down its beginning. Even as early as 287 B.C., legend tells of the Greek scientist Archimedes using the true density of gold to con-

duct a non-destructive examination of a crown and thus prove that it was a counterfeit. Principles from the modern field of medical examination were published in 1248 as a Chinese judge recounted how insects were used in a death investigation and how manner of death could be determined through systematic examination of physiological evidence. In 1862, an Army general brought forensic science to the Army through the establishment of the Army Medical Museum for the collection of anatomy samples, just three years later hosting the autopsy of Abraham Lincoln. Through many changes in name, scope, and mission, these forensic roots of the DOD are known today as the Armed Forces Institute of Pathology, DNA Identification Laboratory, and Medical Examination offices.

Considered the most mature of the biometrics, the use of fingerprints also has a rather hazy origin. Most texts cite the use of finger impressions as a means to prevent forgery thousands of years ago by the Assyrians and Babylonians, but there is much debate about whether their value for personal identification was recognized at the time. By the 14th century, there is documented evidence that Chinese merchants were using the footprints of newborns in ink and conducting comparisons of the impressions in order to positively establish identity. Systematic

multimodal biometric identification was pioneered by the Frenchman Alphonse Bertillon in the late 1800s as he established the uniqueness of different body measurements and combined them with photographs and fingerprints in the early 1900s to establish identity portfolios. Fingerprints have been used throughout the U.S. for criminal identification in the 20th century. Within the DOD, the most prominent use has occurred in the U.S. Army Criminal Investigation Laboratory, established in 1943.

Unique Aspects of Each Community

Given their separate and distinct histories as well as the evolution of their missions over time, each of these communities naturally has facets that are separate from the others.

The forensic science community is very concerned with traditional legal application of its products. Stringent aspects of scene preservation, evidence packaging and storage, documentation of items and actions, as well as knowledge of relevant case law are important within each forensic discipline. Strict adherence to sequential discipline processing as well as sequential chemical and physical processing within each discipline are paramount to achieve the ideals of thoroughness required by the legal system. Often, one type of forensic examination may reveal the necessity for another, requiring additional laboratory time to not destroy potentially useful evidence. The principle in forensic science of thoroughness at all costs, including time, is diametrically opposed to the principle in the Intelligence Community (IC) that the value of information decreases exponentially over time. It is far better to have 80 percent of the intelligence now than 99 percent of the information too late. Furthermore, the IC is interested only in the facts, not necessarily in knowing the exact chemical processes and underlying theories used to determine those facts.

There are also many of the forensic disciplines that have no bearing whatsoever on biometrics. Generally, identifying biological or physical signatures of a person are considered biometric while identifying signatures of an item are considered forensic. The biometric community is not interested in the impression evidence left by a gun barrel on a bullet, a tire in mud, or a pry-bar on metal. These aspects of forensic science are important, but they have no relevance to the biometric identification of an individual. Even if someone is captured wear-

ing the exact shoe that left an impression at a location of interest, it cannot be automatically inferred that he/she was the wearer of the shoe at the time the incident occurred. For these and other reasons, there will always be aspects of forensic science that are separate from the field of biometrics.

Likewise, there will always be aspects of intelligence that are separate from biometrics and forensics. Neither of the latter communities is concerned with techniques for eliciting information from sources or even with the use of their products for predictive analysis or calculating the probability of the occurrence of future events. Intelligence analysts are concerned with the “so-what” behind a biometric match or a forensic finding, but the objective nature of biometric matching and forensic identification prevents these communities from being concerned with how their products (identifications) are used. Other facets of intelligence that are of no obvious concern to the biometric or forensic communities include espionage, reconnaissance, interrogation, targeting, cryptanalysis, etc.

The biometric community is interested in the use of physical, biological, or behavioral characteristics of an individual to effect personal identification. In many cases, this interest centers on types of characteristics or uses of those characteristics that are not relevant to the forensic community or the IC. For example, neither of the latter communities would be interested in volumetric measurements of the chest cavity over time or the uniqueness of human cardio-electrical patterns. Nor would they be interested in some of the business functions facilitated by biometrics, such as physical access control, smart-card identity verification, or methods to obtain biometric population statistics. The IC might be interested in the information behind such endeavors, such as access logs that show when and where a particular individual attempted to gain access to a facility, but the actualization of the business processes necessary to support those functions are squarely centered in the biometrics arena.

Convergence

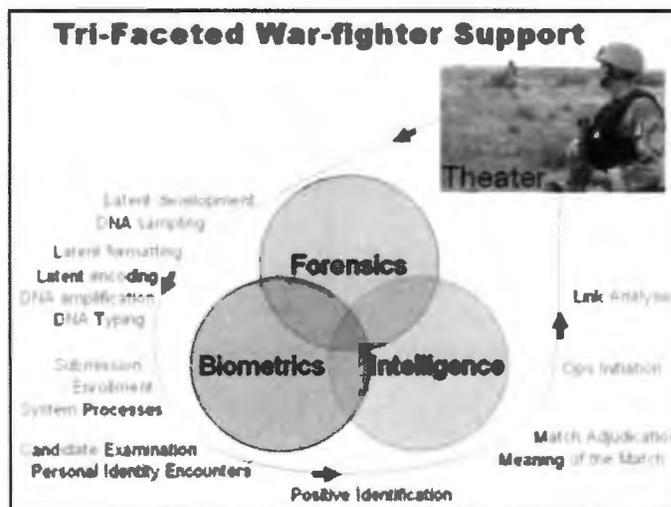
Although there are many areas that are exclusive to each community, other areas of these communities have begun to come together over the course of the last decade. Prior to 2001, there was no large-scale biometric collection within the DOD other than to conduct fingerprint checks against the FBI's

Criminal Master File for military applicant screening purposes. The collection of biometrics from adversaries and items of interest from sites to identify friend from foe progressed from a very specialized and small-scale intelligence activity to a large-scale joint Service function on the battlefield. There are elements of all three communities present in this new model of asymmetrical warfare.

It was the IC that first recognized and deployed the Biometrics Automated Toolset—a classified system capability to obtain multimodal biometrics of face, finger, and iris from a red force population in order to maintain a biometric identity dossier that is searchable independently for name or context (even though numerous contextual fields link back to the dossier). This foray of the IC into the biometrics arena represented the first large-scale convergence of these two communities within the DOD. Other more recent convergence includes DNA collection, matching and reporting, new requirements for efficiency of biometric collection timelines, the use of biometrics for target verification, biometric searching of covert face images against larger-scale repositories, and other classified tactics, techniques, and procedures.

The need for rapid intelligence has also forced together the communities of biometrics and forensics. Traditionally, forensic scientists have been the initiators of biometric system searches of the products of forensic analysis. However, as the IC has driven many of the collection capabilities in theater, it has been the biometrics and IC together that have answered the call for completion of real-time biometric system searches. Unlike the slow-grinding wheels of the U.S. legal system, the IC does not enjoy a built-in window of time measured in months or years for completion of biometric examination services. Terms such as “match-on-objective,” “Ruggedized miniature DNA extraction,” or “tactical latent matching” have never before been uttered in the forensic community. The rapid, OCONUS application of chemical and physical techniques to items of interest and the rapid processing of the resulting biometric information has required transformation of traditional ideals. Even after the convergence and coalescence of these communities, it will still be recognized that the requirements of the IC have reshaped the way forensic science enables biometric searching within the DOD.

What has resulted from the convergence of these communities is an expeditionary capability that rapidly uses forensic principles to develop and conduct biometric searches through the robust DOD biometrics infrastructure to generate real-time intelligence for the War on Terrorism. Throughout the process, certain principles from each community are used to achieve the end goal—support for our warfighters, force protection, and in some cases national security.



Overlapping Aspects of the Communities

The crystallization of the biometrics and forensics communities has been occurring at high levels within the DOD to establish a more formalized department-wide structure leading to more coordinated joint DOD capabilities. As these communities coalesce and definitions and tasks within each community come into focus across the Services and combatant commands, areas of overlap become points of contention. A prime example of this is the comparison of latent print and search candidates mentioned previously. Traditionally, these comparisons have been conducted by practitioners in the forensics community as a part of the time-consuming laboratory case process. Today we are seeing abbreviated expeditionary laboratory examinations and biometric image transmissions from theater, producing intelligence reports long before state-side laboratories obtain the items of interest for thorough processing. In fact, in some cases, this entire process has taken only hours.

This leads to natural friction between the IC that desires to maintain the efficiency of these OCONUS

operations and the forensic community that desires to standardize them according to traditional ideals. The Soldier on the battlefield can collect items of interest, but the standards used for that collection are still being defined. In the end, there will be a balance between the principles of thorough packaging, documentation, and chain-of-custody of "evidence" with the more chaotic "bag-and-tag" techniques defended under the banner of "better than nothing." Likewise, there will be a similar balance between the multi-disciplinary sequential all-encompassing approach to laboratory forensic processing with the more expeditious approach of the 80 percent solution "now." It will likely be some time before stakeholders from these two very different communities fully understand the perspectives of the other.

Conclusion

Until that time, these three communities continue to converge and coalesce as the overarching mission is being pursued. As boundaries between these

communities achieve sharper focus, additional tensions from different stakeholders will surely need to be resolved. At the end of the day, however, it is the ideals of pursuing freedom and liberty spoken so highly of by our men and women on the battlefield that will drive forward this convergence. The greater good of the end result will ultimately define the specific processes and procedures used to obtain it. ✪

Kasey Wertheim is President and CEO of his own company, Complete Consultants Worldwide, LLC, supporting the DOD BTF by managing science and technology projects related to forensic science. He provides subject matter expertise to the DOD and is actively involved in the biometric and forensic communities. He spent seven years as a forensic scientist and crime scene analyst prior to becoming heavily involved in forensic technology. Currently, he serves as Chairperson for the Biometric Committee of the International Association for Identification (IAI) and is an IAI Certified Latent Print Examiner, Distinguished Member, and Editorial Board Member. He completed a short tour of duty in Iraq and Afghanistan as part of an IC laboratory improvement effort and spent one year on contract with NGIC.

FORENSIC FOCUS



The training and application of investigative skills. From "Investigative Interface in Naval Intelligence" by Albert Deahl, MIPB, Winter 1976.

The Role of Forensics in the Iraqi Judicial System-

by Erik [unclear]



Targeting Insurgents

Background

Sadam Hussein and the Ba'ath Party, effectively eliminated Forensic Science from the Iraqi legal system soon after taking power. Fingerprints were used on voting records and other official government documents, but were never accepted as evidence in a criminal proceeding. Ba'ath judges instead expected to hear the testimony of two witnesses to a crime and photographs before they would find a defendant guilty of any criminal offense. Ba'ath Party members were often immune from prosecution, while Shiites and others were routinely imprisoned without evidence by the politically corrupted legal system.

The end result was that ordinary Iraqi citizens did not trust the legal system in Iraq. It's not generally known, but prior to the Ba'ath takeover, Iraq was actually a leader in Middle Eastern Forensic Sciences. Iraqi fingerprint experts were members of the International Association for Identification, an organization that represents the experts in fingerprint identification, shoe print analysis, crime scene reconstruction, photography and other disciplines designed to support criminal investigations around the world. All this history was lost during more than 30 years of Ba'ath rule, but some in Iraq didn't forget, and a few young lawyers were open to learning about a science their country once embraced.

The U.S. military ended the Hussein government and its corrupt legal system when it entered Baghdad on April 9, 2003. On April 22, 2004 the Coalition Provisional Authority rebuilt the legal system and created a new adjudicating body called the Central Criminal Court of Iraq (CCC-I). The CCC-I consists of two distinct branches—an investigative court and a felony court. It has national jurisdiction over all matters related to terrorism, organized crime, governmental corruption, acts designed to destabilize the government or any case where a defendant is unable to obtain a fair trial in a local court. The CCC-I was given authority to issue both arrest and search warrants, regardless of whether the case falls under the jurisdiction of the CCC-I or a lower court.

The Iraqi Constitution of 2005 created a parliamentary form of government with three separate and independent branches: Legislative, Executive and Judicial. The Judicial branch falls under the authority of the Higher Judicial Council, which has its own budget, appoints judges, investigates judicial misconduct and corruption, and oversees the entire judicial system within Iraq.

The Iraqi judicial system is based upon the Egyptian system, which in turn is modeled after

the French judicial system. Unlike *Common Law*, upon which both the British and U.S. legal systems are based, the Iraqi system does not recognize judicial precedence. Laws are not interpreted from precedent cases as with Common Law, they are applied as written. If the written law does not specifically prohibit the circumstances of the event, it is not a crime. Each judge may act independently and is not restricted by the rulings of other judges. One judge might accept the fact that fingerprints are unique to one individual while another judge does not. Some of the younger Investigative Judges at the CCC-I, with recent training in the capabilities of Forensic Science, readily accept fingerprint testimony and are willing to consider other scientific evidence such as ballistics and DNA, while the more traditional Judges are skeptical, demanding the sworn testimony of two witnesses who can identify the suspect.

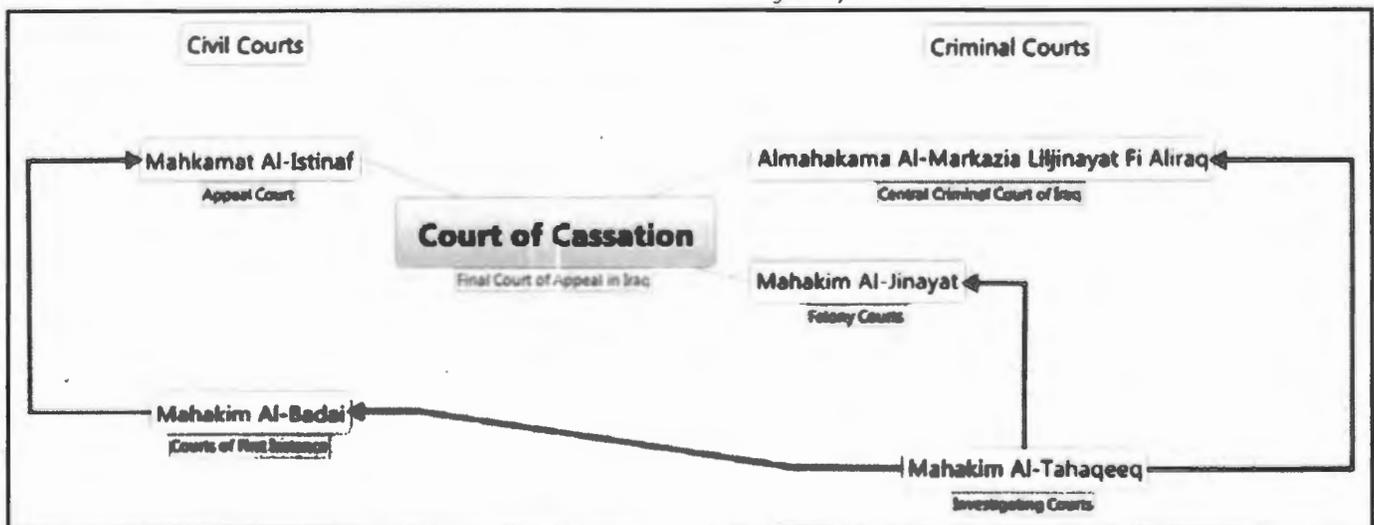
This inconsistency among the judges often leads to the practice of *Investigative Judge shopping*, when cases being presented are based upon fingerprint identification and lack either a confession or two witnesses to the crime. Truth is determined primarily through questioning of the accused by the Investigative Judge. He has sole discretion over what evidence is accepted for consideration and the rules of evidence are not strict.

The Investigative Judge is the finder of fact under the Iraqi system. Once all the witnesses have been heard and the evidence has been examined,

the judge determines if there is sufficient cause to believe the defendant is guilty, and whether or not the case should be tried by the Felony Court. If the Investigative Judge determines the case should go forward, a recommended charge and disposition is included with the case file before it is submitted to the Felony Court. That court can then accept or reject the judge's recommendations, or the court can ask for additional information, or it can dismiss the case altogether. However the Felony Court rarely goes against the Investigative Judge's recommendation.

Trials before the Felony Court are generally swift. The average trial lasts thirty minutes. The three judge panel hears testimony from the victim under oath. The panel then reviews the court file. If the accused denies the charge(s), defense witnesses are heard and any evidence offered by the defense is considered. The victim and prosecutor then offer petitions, followed by the accused who is the last person to speak. The judges then adjourn to deliberate, or they render a verdict and sentence. Deliberations rarely last more than 10 minutes. The verdict is announced publicly. Penalties under the Iraqi Penal Code include:

- ◆ Death Penalty.
- ◆ Life Imprisonment (20 years.)
- ◆ Imprisonment for a specific term (5–15 years.)
- ◆ Servitude (put to work for not less than 3 months, or more than 5 years.)
- ◆ Detention (not less than 24 hours or more than 1 year.)



The Iraqi Court System is divided into civil and criminal jurisdictions. The Investigating Courts work with police and citizens to determine if a case exists, who the responsible party, and which court has jurisdiction over the matter. The CCC-I has its own Investigative Judges, but will also accept cases referred by the Investigating Courts. The Court of Cassation is the court of final appeal in Iraq.

- ◆ Fine (up to 500 dinars.)
- ◆ Confinement in a school for young offenders.

The sentences handed down by the CCC-I normally fall within the first three.

Appeals are heard by the Court of Cassation and must be filed within 30 days of judgment. Death penalty cases are appealed automatically to the Court of Cassation, and must be forwarded to the court within 10 days of judgment.

Grounds for appeal include:

- ◆ Breach of the Law.
- ◆ Mistake in the application of the Law.
- ◆ Fundamental error in standard procedure.
- ◆ Fundamental error in the assessment of the evidence.
- ◆ Error in sentencing.

The U.S. military began collecting material from the battlefield for forensic exploitation in December 2004 in an effort to identify and track insurgents by using biometric signatures recovered from the collected material. Terrorists began to lose their anonymity and were targeted in military operations. Coalition Soldiers and Iraqi civilians were falling victim to improvised explosive device (IED) attacks in ever increasing numbers, but by the beginning of 2007 things began to change. Effective targeting of the bomb makers reduced the number of incidents, while the exploitation of Forensic Intelligence was reducing the overall effectiveness of the IEDs.

The detention and interrogation facilities throughout Iraq began filling up with terror suspects. The Coalition Forces were holding more than 22,000 detainees. A small portion of those (approximately 150¹) had been forensically connected to IED events, while hundreds more had been linked to events by other intelligence methods. Many were captured with bomb making materials in their possession.

Iraq's government was moving quickly to establish civilian control over law enforcement functions, and to re-establish the rule of law within its borders. The CCC-I was taking the lead in Iraq's efforts to hold insurgents accountable for their crimes. Judges at the CCC-I began to receive forensic training from latent print examiners working at the Combined Explosives Exploitation Cell (CEXC). They learned about fingerprints, how they are deposited on var-

ious materials, and why a fingerprint can be used to uniquely identify an individual. Even though the Hussein government used fingerprints extensively to sign documents and identify criminals and government officials, many in Iraq still believed it was impossible to determine the identity of a bomb maker from a fingerprint left at the scene of a bombing.

The Investigative Judges at the CCC-I take witness statements and prosecute cases from a variety of sources, but the majority are submitted by U.S. military lawyers working for Task Force (TF) 134. Lawyers search through databases and reports looking for the details of a detainee's arrest, in an effort to determine if an offense was committed that can be submitted to the CCC-I for criminal prosecution. Much of the information found is classified and can't be used as part of an Iraqi prosecution. Other cases lack witnesses, but despite these hurdles, the number of cases submitted for criminal prosecution continues to increase.

First Fingerprint Match Accepted for Charging at the CCC-I

(b) (7)(F)

Lawyers from TF 134 contacted CEXC and asked for their support to prosecute Affat under the Iraqi Criminal Statute for Terrorism. This was the first time CEXC was asked to deviate from its intelligence mission to provide expert testimony in a criminal proceeding. The request highlighted the challenge of protecting classified techniques and information, but also offered a new tool for removing insurgents from the battlefield.

After much discussion, CEXC agreed to provide unclassified exhibits and testimony. The case was submitted to an Investigative Judge at the CCC-I. During his statement to the Judge, Affat admitted that he had constructed the IED that wounded seven Coalition Soldiers. The Investigative Judge forwarded the case to the Felony Court for trial where Affat was sentenced to life in prison. Affat was transferred from Coalition custody to the Iraqi prison system.

First Conviction Based Upon a Fingerprint Match

(b) (7)(F)

(b) (7)(F)

As in the first case, CEXC provided unclassified exhibits to TF 134 attorneys and the case was submitted for charging. On September 24, 2007 a latent print examiner from CEXC traveled to the CCC-I to provide testimony to an Investigative Judge. The Judge asked specific questions about the IED, where it was found, where the fingerprint was found and how it was identified to Dulaimi. The Judge then told his clerk how to summarize the testimony and which parts to include in the court record. The witness remained seated on a black leather sofa, which serves as the witness chair, until the clerk had completed the handwritten record. The witness then signed the record, which is written in Arabic, and it was added to the court file as the witness's sworn testimony. The court file contains the statement of all witnesses and the defendant, as well as any photographs or diagrams. The latter two items are nearly as compelling to an Investigative Judge as a signed confession or the sworn testimony of two witnesses to the crime.

(b) (7)(F)

UNCLASSIFIED

(b) (7)(F)

Dulaimi's case was tried in November, 2007, by the three Judge Felony Court. Following a short deliberation, he was found guilty and sentenced to death.

First Iraqi Arrest Warrant Issued by the CCC-I for a Master Bomb Maker

(b) (7)(F)

Muthana was convicted of the crime on February 25, 1996 and was sentenced to one year in jail. It is believed that Muthana was studying Electrical Engineering at the time of his arrest.

Muthana didn't turn up again for ten years, when his fingerprints were matched to an IED in the Mosul area. Over the next two years CEXC matched him to a total of eleven IEDs, and there is reason to believe that he has constructed at least 75 others. NGIC designated Muthana as a high value target. Despite numerous attempts to find him, Muthana evaded

(b) (7)(F)

(b) (7)(F)

(b) (7)(E)

(b) (7)(F)

detection. The only picture of him is at 12 years of age. Analysts know he's from Mosul, and they know Iraq is a tribal-based society where people from one area tend to be known by or related to other people in the same area. Likewise, the Iraqi Police tend to know the people in their towns and villages.

As the CEXC Biometrics Lab Director at the time, I asked the counter-IED Targeting Program Analyst at CEXC if an Iraqi arrest warrant would be useful in getting the Iraqi Police to take an active role in locating and/or capturing Muthana. The analyst excitedly said, "Yes, how do we get one of those?" I said, "I have no idea, but I'll bet the Iraqis have a procedure for requesting one, so all we have to do is find out what that is." I contacted one of the attorneys at TF 134 that I had worked with on other cases, explained the circumstances and told him I needed an arrest warrant and wondered what the procedure was. His response surprised me. He said, "I have no idea, but I'll find out and get back to you." Ten days later he called back and said it took some doing as even the Judges weren't sure if the Coalition could request a warrant, but after some legal research it was determined that the issuance of an arrest warrant was within the discretion of an Investigative Judge. Further, the basis for granting a warrant was much the same as a referral to the Felony Court. A case would have to be prepared as if the accused were present. The case is then presented to the Investigative Judge along with witnesses and any available evidence. If the Judge determines that the case is sufficient to justify a referral to the Felony Court, an arrest warrant will be issued. In other words, the accused is tried in absentia. The procedure made sense in

(b) (7)(E)

(b) (7)(E)

an odd way. If an arrest warrant was issued and Muthana was arrested, the trial was over except for Muthana's own statement.

A thirty-two page exhibit was prepared along with an affidavit stating that I had examined Muthana's 1996 fingerprint record and compared those fingerprints to the latent prints recovered from IED material, which was collected at several IED events by weapons intelligence team and explosive ordnance detachment units, and that it was determined the latent prints were made by Muthana. The exhibit contained documentation and photographs of three events that had been matched to Muthana, as well as his fingerprint record and a chart showing how his fingerprints had been matched to those found on the IED material.

On January 13, 2008, I took a Blackhawk to the International Zone (IZ) and then travelled by vehicle to a checkpoint where I accompanied the attorneys through the wall and into the Red Zone. We walked swiftly through some trees and then across approximately 100 meters of open ground to a basement entrance to the court house. I sat in the hallway while the attorney tried to find out which Judge was going to hear our case. After about 45 minutes the attorney told me the Chief Investigative Judge was going to hear the case. We walked to the end of the hall and I sat down in a chair in front the Judge's desk. Unlike the other court rooms I'd been in, this Judge had a computer on his desk, a rack of file servers in the corner of his office. There was a large, flat panel TV on the wall opposite his desk, which was used for video teleconferences. There was a large window near the desk that looked out toward the IZ, which was covered with a curtain.

The Judge was very receptive. His interpreter lacked the English skills I had become accustomed to from other interpreters, but the Judge seemed to understand English quite well. I presented the case to the Judge and he commented frequently on how well documented each incident was and shook his head affirmatively when he examined the slides showing how the fingerprints had been identified. Halfway through the exhibit the Judge put the pages down on his desk and said to me in clear English, "I studied Forensics in Belgium," and then he turned in his chair and pulled out a book from a stack piled on the floor behind his desk. He held the book up and said, "This was my

text book" as he leafed through the pages, pausing to show me selected passages in Arabic. He put the book down and continued through the rest of the exhibit. When he finished he smiled at me and said, "Good job, very good job." The Judge then said to the attorney, "You have your Commander write a memo and I'll sign the warrant." The attorney asked if the Judge needed any more information, and the Judge said, "No, this is enough, good job." The purpose and content of the memo that was requested by the Judge was never fully explained to me. A memo was prepared by the attorney and signed by the TF 134 Commander.

(b) (7)(E), (b) (7)(F)



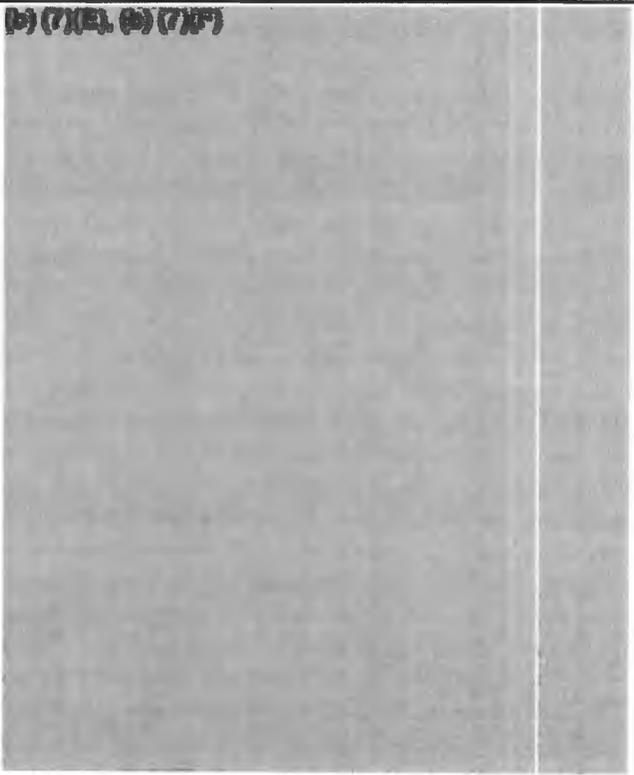
This was a long way from Mosul. Had there not been an Iraqi arrest warrant issued, it's doubtful this sighting of [REDACTED] would even have been reported. It was not widely known outside intelligence and special operations units that [REDACTED] was even a target, and it appears [REDACTED] was able to avoid biomet-

ric check points. He left the area three days before an infantry unit went out to do Biometrics Automated Toolset enrollments of everyone living in the former base. [REDACTED] is still at large and is still active.

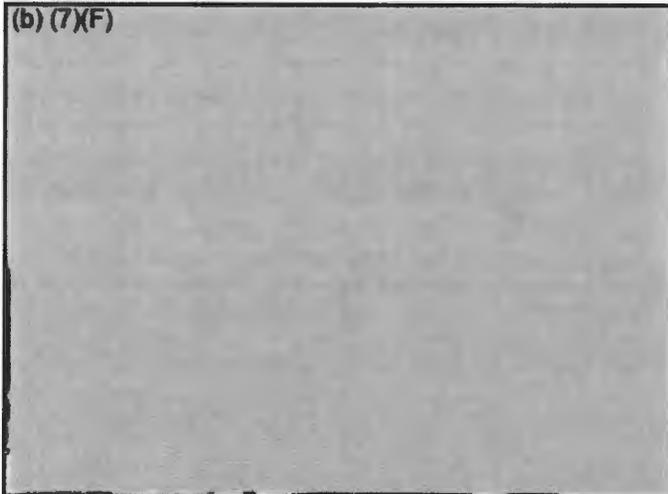
Since this warrant was issued, several other requests for arrest warrants have been submitted to the CCC-I. Multi-national Force-West has become very interested in obtaining arrest warrants issued for insurgents working in the Fallujah area. Iraqi arrest warrants can help to strip away another layer of anonymity and encourage the assistance of the Iraqi Police and citizenry. Removing an insurgent's anonymity is the first step towards removing them from the battlefield.

Iraqi Judges risk their lives every day, just going to work. Many of the Investigative Judges sleep on cots in their court room, and only return to their homes at irregular times and intervals. At the beginning of January 2008, one of the CCC-I's Felony Court Judges and his body guard were assassinated outside the Judge's house on their way to the CCC-I building. In March 2008, simultaneous bomb attacks were made on five Judges. All five avoided injury, but the intended message is clear. My ex-

(b) (7)(E), (b) (7)(F)



(b) (7)(F)



(b) (7)(F)



(b) (7)(E), (b) (7)(F)



The former Saddam Hussein Gift Museum is now home to the CCC-I. The building is located inside the Red Zone and is heavily guarded by both Iraqi Security Forces and U.S. Military Police. Criminal cases are presented by U.S. Military attorneys. The Judges, Prosecutors and Defense Attorneys are Iraqi and many are women.

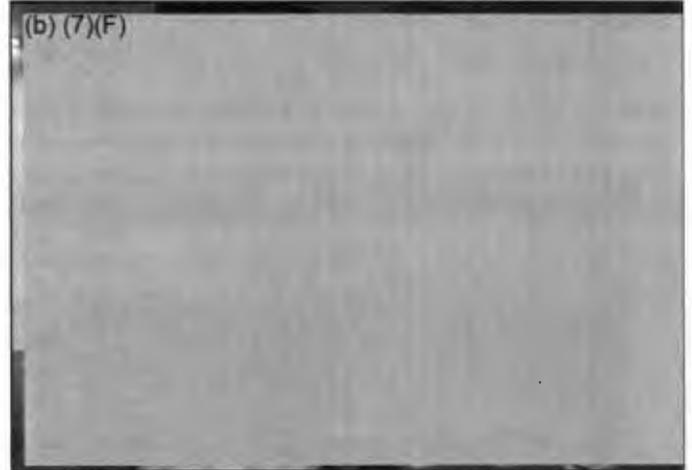
perience with the Iraqi Investigative Judges is that they are deeply concerned about their country and are dedicated to their profession and the Rule of Law in Iraq. They prove it every day by putting their lives on the line just going to work.

CCC-I

The CCC-I building originally housed the Saddam Hussein Gift Museum and Clock Tower. It was chosen to house the CCC-I because it was accessible to the Iraqi people living in the Red Zone, yet it's also close enough to the IZ to be accessible for the attorneys and Coalition witnesses travelling from the U.S. Embassy and beyond. Prisoners facing charges are transported to the CCC-I by U.S. Military Police. In the center of the basement floor is a large fountain that once greeted visitors to the Gift Museum with streams of water which fell from a metal sculpture that rose from a large pool built up from the floor. The stairs wrap around the fountain, rising up to the floor above. Visitors to the CCC-I who look down from the building's lobby now see a metal sculpture sitting alone in a dry pool. Looking up, the ceiling rises high into the base of a clock tower that once told foreign visitors and government officials the time in Baghdad from four different directions. Only the clock faces remain; they no longer tell the passing viewer the time. The hands were shot away in a forgotten battle with a sniper who used the clock tower as a vantage point.

There are a number of young children running around the lobby and hallways of the CCC-I. Many of these children are orphans and are brought to

the court house by court employees to keep them safe. Most of the U.S. Soldiers and attorneys working in the court house know these children by name and have worked out ways to communicate with them as they spend their days together. A small, improvised restaurant is located in the basement and serves a notoriously strong Iraqi coffee and a kind of sandwich the Iraqis call falafel.



A small restaurant in the basement of the CCC-I building serves Iraqi coffee and falafel, a kind of Iraqi sandwich.

Those accustomed to testifying on a regular basis in a U.S., or other Common Law court, might find the conditions at the CCC-I a bit surreal and perhaps a little hard to comprehend at first, but the CCC-I is a functioning legal system, with rules, procedures, and a staff of educated lawyers and support personnel who run it. The Senior Investigative Judge received Forensic training in Belgium. Some of the Judges are Christian, but the majority are

Muslim. Many understand a surprising amount of English, but all rely on a translator to avoid misunderstandings. However, don't be surprised if a Judge suddenly makes a humorous comment, or asks a clarifying question directly, in English. The fact that you have to wear body armor and a helmet while following variable security procedures in order to get to the building simply serves to remind that this court system is also functioning inside a war zone.

Conclusion

Iraq continues to move toward an independent government, and self-supporting army and criminal justice system. The U.S. Army Criminal Investigation Laboratory (USACIL) is sending added forensic laboratory capacity to Iraq in order to provide more support for DNA, ballistics, chemical analysis as well as biometrics. These laboratories fall under the purview of the Provost Marshal's Office in Iraq and USACIL in Georgia. The Government of Iraq has a Forensic Laboratory in Baghdad and is standing up an additional lab in the North. All of these labs will presumably be producing results that could support criminal prosecutions. These criminal cases would need to be submitted to the CCC-I or one of the local courts for prosecution.

Done right, the Coalition can be seen as an ally and resource to the maturing criminal justice system in Iraq. The Coalition is also in a position to offer training and support to Iraq's Forensic Laboratories. Done arrogantly, and without respect to the Iraqi

culture and history, we risk losing an effective tool for removing terrorist from the streets and battlefields of Iraq, and we create an opportunity for those terrorists to practice their tradecraft in the U.S. or elsewhere. Iraq has a legal system and it works for them. We must continue to learn about and understand that system, and support it where we can. We share a common goal: Identifying, capturing and prosecuting terrorists. Biometric Intelligence, like other forms of intelligence, can support many missions. It's good to know who the enemy is, but it's even better when you have a resource like the CCC-I, that is able to act on that intelligence and render the enemy safe. ✨

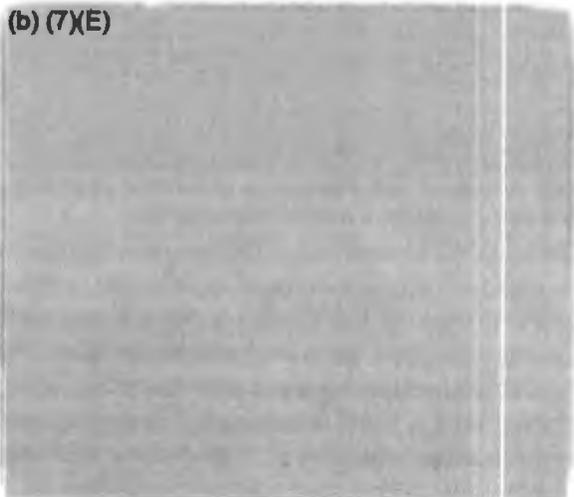
Endnote

1. The actual number is difficult to establish. Records range between 142 and 158, depending upon the source. Some individuals were identified, but never captured.

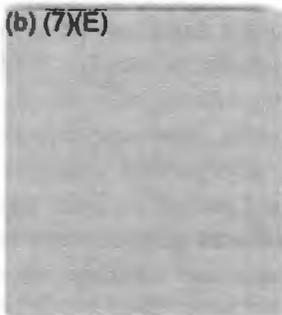
Erik Berg is currently working for Harding Security Associates as a latent print examiner and is assigned to the NGIC. His work has been featured on documentary television shows such as The New Detectives, 60 Minutes, and Forensic Files. His expertise includes photography, computer based imaging, latent fingerprint identification and crime scene investigation. He deployed to Iraq in September 2007, after 22 years in law enforcement, to work in the Biometrics Laboratory at the CEXC-I at TF Troy. In December 2007, Erik was promoted to the lab's Director. During February and March 2008, the Biometrics Lab recovered 2,344 latent prints of value from IED related material, and a record number of those (104) were identified during the same period. Erik can be contacted at (434) 951-4730 or via email at eberg@harding-security.com

FORENSIC FOCUS

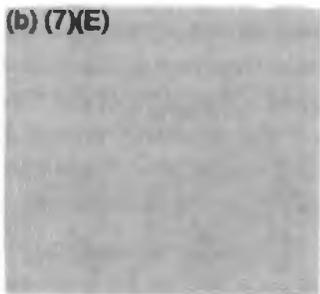
(b) (7)(E)

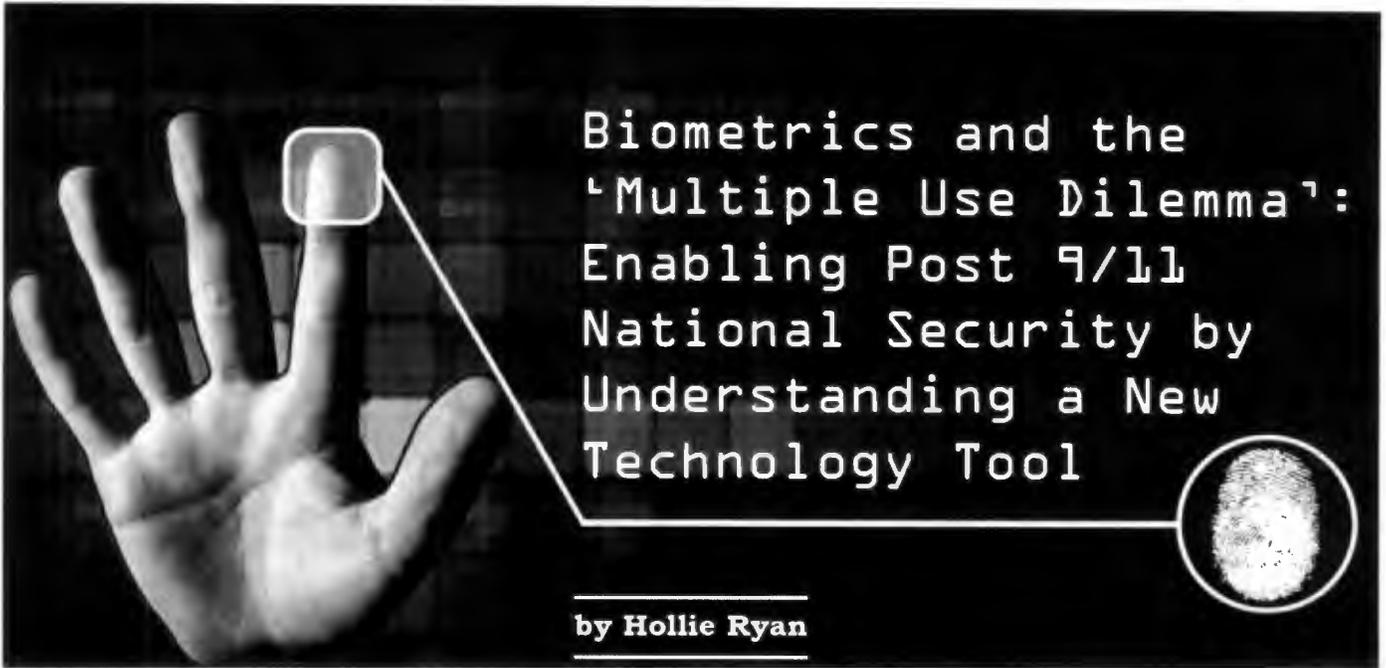


(b) (7)(E)



(b) (7)(E)





Biometrics and the 'Multiple Use Dilemma': Enabling Post 9/11 National Security by Understanding a New Technology Tool

by **Hollie Ryan**

Introduction

As it often happens with breakthrough concepts, biometric technology development has been rapidly outpacing conceptual understanding and informed policy development, both of which help to ensure the proper application of novel solutions that, in this case, stand to revolutionize how we approach crime and conflict. Additionally, popular media, with programs like *Alias* and movies like *Minority Report*, have skewed the reality of scientific limitations and bureaucratic processes that most often encumber rather than enhance the efficiency of fielding such new and improved technological capabilities. Advances in biometric human identification technology nevertheless offer enormous potential for forensics and for meeting evolving national security objectives.

Technologies to collect and process biometric data have grown exponentially in the last few decades, and the competitive demand to develop biometrically enabled tools that are smaller and faster continues to be at the forefront of federal science and technology procurement efforts. The downside is that false impressions and competing technologies hinder the effective development of operational tools that utilize biometrics because those in the position to make policy and planning decisions, or who rely on those decisions for technology development (i.e., vendors), too often confuse process and application. This article presents an approach to understanding

the relationship between biometrics and forensics by distinguishing the various applications, functions and missions of both among the defense, law enforcement (LE) and intelligence communities (ICs). It is hoped that a clearer understanding of the possibilities and limitations of each, and of the respective needs and restrictions across federal agencies and between government and industry, will serve to advance and focus current efforts to make the most of these vital national security capabilities.

So what are, or what is, Biometrics?

A biometric is a measurable physical or biological characteristic, such as a fingerprint or iris pattern, a personal behavioral trait such as handwriting style, or on a much smaller scale, DNA sequence or blood type. As a discipline, biometrics (or biometry) is an established scientific field of studying methods for uniquely recognizing humans based on these intrinsic traits.'

The front end of biometrics in operations typically comprises manual or automated processes of collection, processing, and storage. In the current context, effective biometric recognition relies on rapidly evolving automated database and collection device systems that offer the promise of enabling security personnel to compare digitally translated templates to quickly identify questioned individuals if their profiles exist in the queried database. The Federal Bureau of Investigation (FBI) has made consider-

able use of such systems to store and search digital biometric profiles, most notably by way of the Integrated Automated Fingerprint Identification System (IAFIS). The *IAFIS maintains the largest biometric database in the world, containing fingerprints and corresponding criminal history information voluntarily submitted by state, local, and federal LE agencies*. A national fingerprint and criminal history system maintained by the FBI, the Criminal Justice Information Services (CJIS) Division, the IAFIS provides automated fingerprint and latent search capabilities, electronic image storage, and electronic exchange of fingerprints and continuous responses. By comparison, *the Combined DNA Index System (CODIS) is used to store and search DNA profiles obtained from a number of indices, specifically: convicted offender, forensic, arrestees, missing persons, unidentified human remains, and biological relatives of missing persons*. CODIS operates at national, state, and local levels, where the National DNA Index System enables laboratories to exchange and compare DNA profiles across the country, including those from all 50 states, the U.S. Army, and the FBI.²

The Department of Homeland Security (DHS) maintains an Automated Biometric Identification System known as IDENT, consisting of biometric data and information on known criminals and suspected terrorists from profiles contained in IAFIS on non-U.S. citizen persons of interest to LE.

Similar to the DHS IDENT, the Department of Defense (DOD) maintains its own Automated Biometric Identification System (ABIS.) ABIS is the DOD's central repository for all biometrics collected by DOD personnel from non-U.S. citizen persons of interest. While numerous other federal, state and local government agencies also have biometric databases, the above constitute the largest national biometric databases in the U.S.

Biometric Applications

As the field of biometrics continues to evolve, so does the precise manner of classifying biometrics systems. Used in conjunction with automated databases, biometric applications that center on the broader functions of access control and identity management allow expanded capabilities in forensics and military Counterintelligence to authenticate, identify, or facilitate attribution of a human

subject. While the concept of access control is self-explanatory, identity management can be defined as “the registration, storage, protection, issuance, and assurance of a user’s personal identifier(s) and privileges(s) in an electronic environment in a secure, efficient, and cost-effective manner.”³ Applications may use automated or manual processes, independently or as part of an overall information gathering scheme.

A biometric device can be applied in virtually any application scenario in which one might otherwise use non-biometric identification, such as keys, identification cards, security cards, personal identification numbers (PINs), or passwords to gain access to a physical facility, a virtual domain (information system), or a process, or to determine eligibility for a privilege.⁴ In the contexts of LE and national defense, relevant sub-categories encompass physical and logical access control and security, and identification–applications that help the above communities in determining who someone is, who someone should be, or who someone might be. Many departments and agencies at all levels of government, as well as private companies, use a combination of biometrics based systems with various modalities, primarily fingerprint, face and iris, for automated recognition and verification.

Biometric applications can function in either of two ways—verification or identification. Verification is the process of comparing a presented biometric template to a stored biometric reference(s) associated with a specific purpose. Verification application processes can be generally described as one-to-one (1:1) matching, where it must be determined that the user is in fact the person they claim to be.⁵ During verification, a user will typically present their “claim” of identity in the form of a name, unique identification number, token or ID card. Then, the user must authenticate against the claim of identity by presenting their biometric sample and having the resulting template matched against the reference(s) associated with that user’s enrollment record. Verification is commonly used in access control applications where an individual has already been granted privileges or access rights and the system needs to verify that the person seeking access under the given identity is, in fact, that individual.⁶

The DOD uses biometric verification to control access to U.S. military facilities in Iraq. Specifically, the Biometric Identification System for Access (BISA) is a verification system that results in the issue of a “smart card” type of identification token. Its target population is non-U.S. personnel seeking employment at, or access to, U.S. and Coalition bases. The ID card used for BISA contains key biometrics of the person to whom the card was issued, allowing for fast matching between the biometric stored on the badge and the biometric provided by the badge holder, each of which is read by a single integrated device, which compares the two (1:1) each time a badge-holder attempts to gain access to a base.⁷

In identification applications, the system attempts to determine if a person is known to the system (with or without a claimed identity) by comparing the presented biometric sample and resultant template with all known references (the entire enrolled population) in the database. The process associated with biometric identification involves one-to-many (1:n) matching. Identification applications are typically used for LE investigations or, as a screening process to ensure that the person applying for a benefit is not already enrolled in the system and receiving the entitlement under another name or identity.⁸ Identification is often performed during or immediately following initial enrollment of the person’s biometric.⁹ Part of the federal criminal records check process, for example, involves an applicant’s or suspect’s ten-print to ten-print search verification through IAFIS, which compares the complete set of fingerprints against the database of ten-prints.

DHS, with eligibility input from the Department of State (DoS), established the identification program called the United States Visitor and Immigrant Status Indicator Technology Program, better known as US-VISIT. It is one component of a system of security measures that begins overseas and continues through a visitor’s arrival in and departure from the U.S. In many cases, US-VISIT begins at U.S. consular offices issuing visas overseas, where officials collect a person’s biometrics (digital fingerprints and photographs) and check them against IDENT (“one-to-many”). When the visitor arrives at the U.S. port of entry, their fingerprints are taken and used to verify (“one-to-one”) that the person entering the country is the same person who received the visa.¹⁰

While such federal systems have achieved notable success, the creation of more sophisticated systems like the FBI Next Generation Identification system may help to do more than simply verify an identity through direct searching and matching. Projects, including the establishment of a national Biometrics Center of Excellence, are underway to expand and increase the efficacy of automated biometric identification systems to include other intrinsic and extrinsic biometrics such as palm prints, scars, marks, tattoos, and iris and facial imaging.¹¹ In biometric identification systems, however, obtaining a “hit” in a database is far from identification in the worlds of forensic science and military CI.

Attribution

*Biometric systems can also be used to record and associate facts about an individual, helping to establish connections between people and places, events, or other people.*¹² The development of tools designed to compare and analyze biometrics serve to strengthen both capability areas. Biometric algorithms can be designed to relate facts and characteristics to build a profile of someone who is otherwise anonymous. An example would be obtaining a “one-to-many” match of the biometric profile from an unknown individual collected during a crime scene investigation or during tactical or sensitive site exploitation, with an enrolled profile (e.g., a known detainee or convicted felon, or other unknown biometric profile associated with a prior event).

Biometric systems like IAFIS assist LE in making the critical connection between a crime and a suspect. An evidence print to ten-print search can be run when crime scene technicians recover a fingerprint from a crime scene and investigators have not identified a suspect or find that a suspect’s fingerprints do not match the evidence print. If the search does not yield a hit, then the system retains the evidence print as an unsolved file. When new ten-prints are entered into the system, they are searched against unsolved files. This “ten-print to latent print search” may reveal the involvement of a suspect with a previously unresolved crime.¹³ The FBI also uses the CODIS Program as a similar resource to generate forensic leads when investigators recover DNA from a crime scene.¹⁴ A match between DNA profiles from the Forensic and Offender indi-

ces provides investigators with a suspect's identity, while a match between DNA profiles in the Forensic Index can link crime scenes.¹⁵

The DOD's Biometrics Automated Toolset (BAT) is an identification and enrollment system that has allowed military operators to collect biometrics from persons of interest and search that data against a repository of known and suspected terrorist data, as well as profiles from "unknown" individuals. The collection process is essentially the same as for BISA, but BAT is used to create and maintain profile records in ABIS.¹⁶ BAT equipment consists of a laptop computer with identity management software and the various peripheral devices used mainly by military personnel and serviced by contractors to collect specific biometric modalities: fingerprints, iris images, and facial photographs. Quick reaction forces equipped with BAT kits may process a scene after an improvised explosive device (IED) has been detonated, to include collection of biometrics from people in the vicinity who may have been involved. BAT is also used to process prisoners brought into various detention centers.¹⁷ All biometrics collected by BAT and BISA operators are routed by various means to the ABIS for initial enrollment or verification. Data from each system has been used successfully to identify persons known to have hostile intentions toward the U.S. and coalition forces, enabling their apprehension and detention.

While these biometric systems can provide crucial clues to LE, they are not substitutes for the human analytical component of investigation required to draw valid conclusions about motive, history, and the relatedness of tangible and intangible evidence particular to an incident. It takes the revolving and combined efforts of LE and forensic science to enable and enhance the ability to establish "truth" in terms of the law. Similarly, it takes the combined efforts of intelligence and military operations that use biometrics to achieve identity superiority on the battlefield.

Biometrics in LE

Anthony Fortune, a consultant with the Office of the Secretary of Defense (Policy), recently told an audience, "When I was a civilian police officer, we didn't call it biometrics—we called it evidence."¹⁸ Lieutenant Colonel John Manson made one distinction by stating, "Biometrics can tell us who some-

one is; forensics can tell us what they did."¹⁹ These are telling statements about how biometrics and forensics often become confused.

Alphonse Bertillon solved the problem of identifying criminals during growing urbanization in the late 1800s by establishing a method of identification called anthropometry, which is based upon the measurement of various distinguishable aspects of the human body including such things as arm length and head circumference. While many others eventually developed more specific methods of measuring human characteristics, Bertillon essentially discovered the first application of biometrics in LE.²⁰

Forensic science, or simply forensics, is any field of science "dedicated to the methodical gathering and analysis of evidence to establish facts that can be presented in a legal proceeding."²¹

Forensics, like biometrics, is multidisciplinary and uses knowledge and methodologies from many scientific disciplines including biology, anthropology, chemistry, engineering, genetics, and even computer science that support both criminal and non-criminal investigations. The greatest difference between forensics and biometrics then is that while *forensics by definition examines the entire spectrum of scientific fields and methods and applies them to the law, biometrics focuses solely on those fields related to human identification—merely one aspect of forensics.* While LTC Manson correctly implied that forensics is a more involved process, perhaps a more precise statement would be that *forensics can tell us if the individual in question did what we have reason to believe he did.*

The biometric technologies and methods used in forensics for human identification are increasingly being applied in other areas of national security, most notably defense, and have corresponded with efforts in finding new and non-lethal ways of fighting the non-conventional War on Terrorism. Human identification may serve as an end in itself or be part of a larger process, involving stakeholders whose operational requirements often overlap (see Table 1.) The various policies, operating procedures, management, and administrative work concerned with the institutional application of biometrics, however, are most effective when the primary biometric application is clear.

Federal Department	Responsible Areas			
	LE	Intelligence	Access Control	Immigration & Border Management
Justice	*	*		
Defense	*	*	*	
Homeland Security	*	*		*
State		*		*

Table 1. Areas of responsibility for biometric use among federal national security agencies.²²

Identity Management on the Battlefield

The control and management of information is critical for success on the battlefield. The DOD's overarching goal of using biometrics as a key enabling capability for identity management²³ logically leads to combat identification as the pivotal purpose of biometrics in military operations, which the DOD defines as:

“. . . the process of attaining an accurate characterization of detected objects in the battle space to the extent that a high confidence, timely application of tactical options, and weapons resources can occur. Depending on the situation and the tactical decisions that must be made, this characterization will be at least, but may not be limited to, “friend,” “enemy,” or “neutral.” Combat identification functions encompass cooperative and non-cooperative identification capabilities.”²⁴

Overcoming the challenge of characterizing and classifying potential threats through combat ID, particularly when little is known about the subject (such as a person of interest), relies upon a consideration of all associated facts and on recognized shapes, markings, signatures, signals and other factors through the conduct of military operations, not simply biometric confirmation.²⁵ The cooperation of combat forces with the IC is thus vital in understanding the relationship between these factors.

As indicated earlier, the use of biometrics in combat operations may drive intelligence functions, or biometrics-based CI that makes maximum use of covert collection or future stand-off recognition systems,²⁶ which may drive combat operations. Intelligence supports and enables effective combat operations, involving similar processes to LE investigation of information gathering and analysis to draw critical connections and conclusions about those associations. Along with combat iden-

tification, one of the strategic objectives of intelligence is to “defeat terrorists at home and abroad by disarming their operational capabilities and seizing the initiative from them.”²⁷ In meeting that objective, biometrics provides the opportunity to deny the enemy anonymity and is a necessary function of battlefield identity management.²⁸

The combined capabilities of the IC and operational use of biometric identification systems has resulted in considerable success identifying, tracking and targeting persons of interest in the War on Terrorism. The cooperation between intelligence and combat forces is the driving force behind operational effectiveness, just as the interplay between LE and forensics drives successful legal investigation. In either scenario, however, *automated tools such as biometric databases may help to develop leads, but without the benefit of analysis, have limited meaning.*

Consolidating Biometrics and Forensics in the War on Terrorism

Attribution in anti-terrorism operations relies predominantly on making the link between persons of interest and information obtained during tactical and sensitive site exploitation. However, there are two major obstacles to this:

- ◆ Inconsistency at all levels in communicating whether the goal of site exploitation is for intelligence/targeting or for criminal prosecution.
- ◆ Lack of the initial establishment of Joint Forces Command doctrine to include the business of forensics.

No concerted authoritative doctrine or training vehicle currently exists to fully prepare military leaders and Soldiers, marines, sailors and airmen to manage forensic versus CI focused site exploitation.

The military application of forensic science has expanded beyond its traditional internal focus on criminal, judicial, and medical investigative matters. Part of current collection efforts in OCONUS operations include focused counter-IED (CIED) teams, forward-based CIED forensic laboratories, building tactical laboratory capabilities for non-CIED support, and expanding forward-deployed DNA labs. Capabilities in these efforts include the biometric modalities—latent fingerprint and DNA examination—as well as trace evidence and firearms

examination. Forensics has the ability to support military operations by attributing enemy activity to state or non-state actors using nationally and internationally accepted legal standards. Combat forces may utilize forensic methodologies to defeat adversaries, deterring them from gaining military advantages, and providing proof of adversary operations capable of withstanding legal scrutiny. Armed with attributable data supported by biometrics, military forces can begin to influence the enemy's decision making process by affecting the enemy's operational environment.²⁹

CI versus Prosecution

The "beyond a reasonable doubt" standard of proof to which forensic scientists are held along with strict standards for scientific and technical evidence,³⁰ requires that conclusions offered by forensic scientists be supported by more than what is available through automated biometric systems.³¹ The LE community requires strict chain of custody protocols in the collection of evidence (in this case, associated biometric and non-biometric data) and allows substantially more time on scene than is permitted combat forces. These operating procedures may consequentially restrict crucial access to biometric data and are unrealistic in combat operations. The "burden of proof" for military commanders is substantially lower than that for LE for a number of reasons, not the least of which is the requirement for rapid decision making and response on site. Further, the austere conditions of combat do not guarantee that biometric samples are either collected or maintained in a manner that is acceptable to the legal system. As one Army officer opined in April 2005, "We have to document and catalog evidence to make a case against people that we capture...The process is painstaking and often frustrating to soldiers who have, up until recently, been trained for maneuver warfare."³² The military may only require a minimum level of acceptability in order to carry out its mission. Despite that, in some cases the results of a mission may also have LE implications.

In its strategic efforts to make biometrics fully operational in support of DOD objectives and to enable DOD-wide identity superiority, biometrics doctrine development has been toward a distinct military capability, and primarily considered as a targeting tool with LE implications, where the LE community

was recognized as being the technical experts.³³ Perhaps it would be prudent to consider Captain Brian Gellman's approach to evidence versus intelligence collection in **fighting an unseen enemy**:

"Evidence collection is more important than body count in counterinsurgency. We cannot kill insurgents when they do not fight back; they know their chance of winning a court case is much greater than the chance of winning a firefight. Instead of relying on other government agencies or untrained combat arms soldiers, each unit needs an organic CSI team that can conduct on-site evidence collection techniques to increase the successful prosecution of captured insurgents."³⁴

Imposing forensic standards on the use of biometrics in military operations may prove to be a major limiting factor in broadening biometric applications in meeting overarching national security objectives, but ignoring their importance may prove just as detrimental.

The Challenge

The same functions that allow the DOD to be self-sufficient and self-sustaining, namely internal LE and intelligence capabilities, make operational decision making and policy development challenging when it comes to managing biometrics. Recently, the Government Accountability Office released a report acknowledging the complicating factor of managing biometrics in a unique organization like the DOD. The report highlighted:

"Biometrics activities are dispersed throughout DOD at many organizational levels...and DOD has not established implementing guidance clarifying decision making procedures to minimize duplications of effort and ensure interoperability across these levels... [W]ith many different organizations using biometrics for their own requirements and missions, coordination has been difficult to achieve across DOD."³⁵

Both the competing and overlapping needs and objectives of the various DOD organizations makes streamlining an approach to biometrics difficult, not only within DOD, but among the various members of the user community who want to take advantage of the capabilities that biometrics offers. The National Science and Technology Council Subcommittee on Biometrics and Identity Management (IdM) has adequately summarized

the need to lift limitations imposed by the independent development and application of biometric technologies.

“At the Federal level, needs and uses vary significantly, and a one-size-fits-all technical IdM architecture cannot satisfy all agency constraints and requirements. However, there are clear commonalities that would benefit from a coordinated Federal effort, enhance agencies’ abilities to meet mission needs, ensure privacy protection, and enable individuals to exercise their identities securely.”³⁶

The FBI CJIS is endeavoring to establish interoperability between the IAFIS and other biometric systems, with primary emphasis currently on DHS’s IDENT, DoS, and the DOD’s ABIS.³⁷ Additionally, the FBI and DOD have been engaged in a mutually beneficial information sharing relationship since 2003-2004. Since then, the FBI has allowed DOD to install and maintain its central database at the CJIS facility in West Virginia. This arrangement has allowed it to take advantage of existing FBI expertise, shared security and logistics. Last spring, senior FBI and DOD officials agreed that the collocation and convergence of the DOD biometric facility with CJIS would be mutually advantageous. In particular, maturation of the Next Generation ABIS ensures that the DOD will be poised to share this innovation more readily with FBI as the Next Generation IAFIS and CODIS programs concurrently grow.³⁸

The Biometrics Task Force (BTF), who has been given the daunting responsibility of tackling this multi-layered obstacle, has a mission to lead “DoD activities to program, integrate, and synchronize biometrics technologies and capabilities to support the National Security Strategy.”³⁹ Bill Vickers, Special Advisor to the Director at the BTF, stressed that, “Given the crucial role biometrics is playing in the War on Terrorism, DOD must plan to provide secure facilities and a reliable platform for the central databases providing interaction with other biometric databases and responses to the field.”⁴⁰ A consistent theme regarding many aspects of U.S. national security, greater cooperation in strategic planning, as well as implementation between primary stakeholders, must take place if the U.S. is to have a united front against its enemies, foreign or domestic.

Conclusion

The U.S. has the opportunity to take maximum advantage of biometric technologies and their potential to effectively meet our national security objectives by developing a better understanding of its various functions, and distinguishing between the needs and requirements of the user community, particularly LE forensics. The challenge remains in determining how best to achieve operational efficiency by using one tool to accomplish many ends. Whether the DHS requires biometric technology for airport screening, the DOD for access control at a temporary checkpoint in a theater of operations, or the FBI to monitor the transfer of DNA data processed from a crime scene, the key to understanding biometrics across a growing community of users lies in setting clear goals and expectations for its application in each user community.

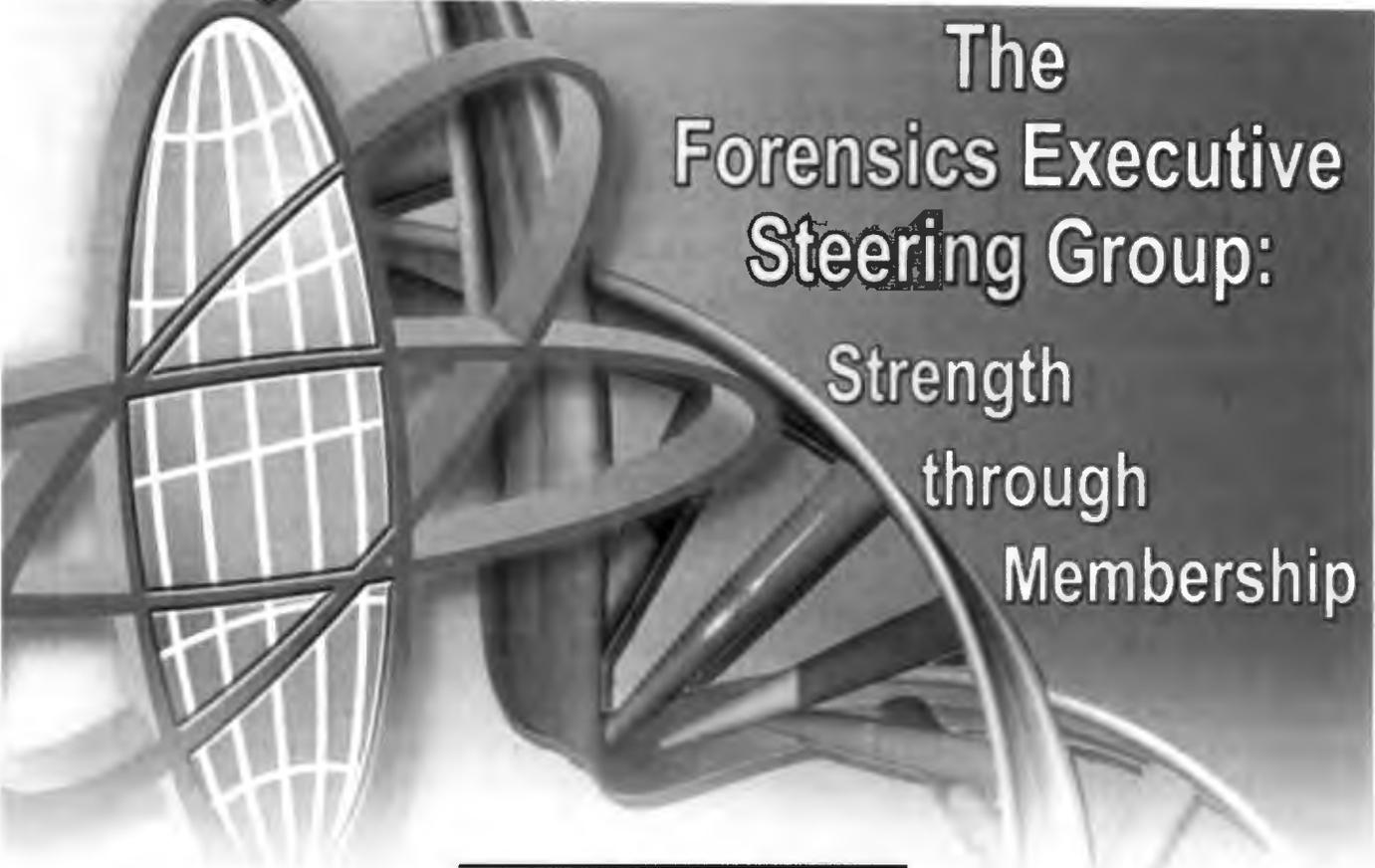
Concerns about chain of custody, the protection of sensitive information associated with a biometric profile, and the need for access to those profiles to enable rapid decision making must guide rather than stifle the effective management of biometrics and the important processes they stimulate. The unprecedented opportunity to make the most of this increasingly important non-lethal application of science and technology to fight crime and defeat our foreign adversaries depends on it. ❀

Endnotes

1. “Biometric Technology Services” at http://www.defenselink.mil/DBT/products/2008_BEA_ETP/bea/iwp/definitions2_technicalservice_621936.htm, accessed 30 October 2008.
2. James Jasinski in Philip Jones, “Using Biometric Technology to Advance Law Enforcement,” *Forensic Magazine* at http://www.forensicmag.com/Article_Print.asp?pid=104, accessed 30 October 2008.
3. International Biometric Group, “Best Practices for Privacy-Sympathetic Biometric Deployment,” IBG Bio-Privacy Initiative at www.biometricgroup.com.
4. James Jasinski in Philip Jones, “Using Biometric Technology to Advance Law Enforcement.”
5. U.S. Department of the Army, “Biometric Identification System for Access (BISA),” PEO Enterprise Information Systems, September 2008.
6. Marc Watkins, “Biometrics,” University of Ottawa, Canadian Internet Policy and Public Interest Clinic (CIPPIC) at http://www.cippic.ca/index.php?page=biometrics/#faq_for-what-purposes, accessed 31 October 2008.
7. Peter Langworthy, *Biometric Identification System for Access (BISA)*, Northrop Grumman Corporation, 12 October 2006.

8. U.S. Federal Bureau of Investigation, *"Integrated Automated Identification System."* Criminal Justice Information Services, at <http://www.fbi.gov/hq/cjisd/iafis.htm>, accessed 29 October 2008.
9. International Biometric Group, *"Best Practices for Privacy-Sympathetic Biometric Deployment,"* IBG Bio-Privacy Initiative at www.biometricgroup.com.
10. FBI Science & Technology Branch, *"FBI Biometric Center of Excellence,"* Presentation at the International Association for Identification 94th Annual Education Conference, Louisville Kentucky, August 2008), Slide 4.
11. Ibid.
12. Marc Watkins.
13. James Jasinski.
14. Ibid.
15. James Jasinski.
16. The Privacy Act establishes strict regulations that govern what and how personally identifying information can be collected by the U.S. Government on its citizens.
17. U.S. Department of the Army, *"Biometrics Automated Toolset (BAT),"* PEO Enterprise Information Systems, DOD Biometrics Project Management Office (Flyer, September 2008).
18. Anthony Fortune, *"Department of Defense Session: Policy Discussion,"* Office of the Secretary of Defense (Policy), Presentation at the Biometrics Consortium Conference 2008, Tampa, Florida.
19. Lieutenant Colonel John Manson, U. S. Marine Corps, Presentation at the Biometrics Consortium Conference 2008, Tampa, Florida.
20. Simon Cole, *Suspect Identities: A History of Fingerprinting and Criminal Identification,* (Cambridge Massachusetts: Harvard University Press, 2001), various paging.
21. Elizabeth Morgan, *"Definition of Forensic Science,"* at <http://ezinearticles.com/?Definition-of-Forensic-Science&d=410618>, accessed 22 October 2008.
22. NSTC Subcommittee, *Biometrics in Government Post-9/11: Advancing Science, Enhancing Operations,* (Washington D.C.: GPO, August 2008), various paging.
23. Shawn Elliott, *"DOD Biometrics Identity Management (BIdM),"* Futures Branch, Presentation, BTF Advance Planning Brief to Industry, 28 February 2008.
24. Countering Air and Missile Threats, JP 3-01, 5 February 2007.
25. *Biometrics Overview* by Tom Dee, Office of the Secretary of Defense, Presentation to the Information Technology Association of America (ITAA), 22 April 2008.
26. Lisa Swan, *Future Biometric Technology Capabilities,* presentation by the DOD BTF, 23 September 2008.
27. Office of the Director of National Intelligence, *The National Intelligence Strategy of the United States of America: Transformation through Integration and Innovation,* October 2005, 1.
28. Elliott, slide 4.
29. *Joint Forcible Entry Joint Integrating Concept,* Version .92A3, (Washington D.C.: GPO, September 2004), various paging.
30. In *Daubert vs. Merrell Dow Pharmaceuticals,* 509 U.S. 579 (1993), the Supreme Court established a legal precedent regarding the admissibility of expert witnesses' testimony during federal legal proceedings by holding that federal trial judges are the "gatekeepers" of scientific evidence. Under the Daubert standard, trial judges must evaluate proffered expert witnesses to determine whether their testimony is both "relevant" and "reliable", a two-pronged test of admissibility.
31. Richard W. Vorder Bruegge, *"Biometrics and Forensics: Similarities and Differences,"* Presentation to the Biometric Consortium Conference 2004, Arlington Virginia, available at http://www.biometrics.org/bc2004/Bios/vorderbruegge_bio_OK.pdf.
32. Major K., *CSI Baghdad,* online blog, 11 April 2005 at http://strengthandhonor.typepad.com/captaink/2005/04/csi_baghdad.html.
33. Vickers, *"DOD Biometrics Briefing,"* Presentation at the FBI Criminal Justice Information Services Division Advisory Policy Board BTF, 5 December 2007.
34. Captain Brian Gellman, "Improving Relevance of Tactical Intelligence in the COE," *Military Intelligence Professional Bulletin* 33, 2 (April-June 2007). Available at <http://www.universityofmilitaryintelligence.us/mipb/article.asp?articleID=570&issueID=45> (accessed 1 November 2008).
35. U.S. Government Accountability Office, *"Defense Management: DOD Needs to Establish Clear Goals and Objectives, Guidance, and a Designated Budget to Manage its Biometrics Activities,"* Report to Congressional Requesters, GAO-08-1065, September 2008, 13.
36. *"NSTC Subcommittee on Biometrics and Identity Management Room"* at <http://www.biometrics.gov/nstc/Default.aspx>, accessed 30 October 2008.
37. Thomas E. Bush, *"State of CJIS: Connecting the World with Bigger-Better-Faster Criminal Justice Information Services,"* Presentation at the Biometrics Consortium Conference 2008, Tampa Florida.
38. Vickers.
39. Department of the Army, "Biometrics Task Force: Mission," <http://www.biometrics.dod.mil/About/MissionVisionGoals.aspx> (accessed 30 October 2008).
40. Vickers.

Hollie Ryan currently works as a strategic planner for Ideal Innovations, Inc., Programs and Operations Division, with whom she was previously tasked as a policy analyst for the BTF. Ms. Ryan holds an M.A. in War Studies from the Royal Military College of Canada, a Bachelor of Social Science in Political Science, and is currently working on a Master's degree in Chemistry with a focus on forensics. She is also a retired Army Captain, having completed tours of duty between 1994 and 2006 in Bosnia, the Republic of Georgia and Western Europe. Readers may contact Ms. Ryan via email at hollie.a.ryan@us.army.mil.



The Forensics Executive Steering Group: Strength through Membership

by Captain Shawn McMahon

Introduction

The application of science and technology to achieve military objectives dates as far back as the history of human conflict. Since the age of Archimedes and the ancient Greeks, and even before, mankind has sought to employ science and technology to gain an advantage over its enemies. Oftentimes, the combatant that can effectively manage and focus the power of science and technology at the decisive moment emerges as the victor. Today, the organization responsible for coordinating forensic efforts within the Department of Defense (DOD) is facing such a management challenge.

The Forensics Executive Steering Group (FESG) is the organization assigned the task of coordinating all DOD expeditionary efforts and establishing forensics as an enduring, global, and deployable capability.¹ These tasks, while straightforward, are made more complex by several factors. First, throughout DOD and beyond, there are differing views as to just what 'forensics' is. Across law enforcement, medical, and

intelligence communities the definition of forensics can vary widely. Secondly, there are organizations within DOD with overlapping responsibilities across the broad range of disciplines and modalities within forensic science. Lastly, the sheer number of organizations that produce, consume, or train forensic analysis makes coordination difficult.

The FESG has made progress despite these challenges, but there is much more to be done. New forensic requirements continue to emerge, and the foundation for an enduring forensics capability has yet to be agreed upon. By examining the conditions which spawned the creation of the FESG, the evolution of its creation, and the overarching challenges it faces, it is possible to identify the core challenges which the FESG must overcome to achieve success. Because the DOD forensic community lacks a completed capabilities based assessment (CBA), which would inform changes to doctrine and organization, and a DOD Directive, which would assign responsibility for coordinating

forensics within DOD, the FESG must rely upon the experience and expertise residing within its membership to guide the FESG towards achieving its objectives. In other words, the success of the FESG hinges upon the participation and cooperation of the entire forensics community.

Origins of the DOD Forensics Governance Structure

Operations Iraqi Freedom/Enduring Freedom (OIF/OEF) generated a large mobilization of technology and ideas in support of mission accomplishment. The enemy's ability to employ anonymity within the population presented a unique challenge to the military, a challenge which was ideally suited to be met through the application of forensic science. As the enemy applied new techniques, tactics, and weapons, technological solutions were rushed to the battlefield in support of the warfighter. The immediate success enjoyed by the several forensic solutions that were implemented in OIF and OEF gave rise to an even greater demand for forensic capability and illustrated the need for the capability to be established as one that would be available into the indefinite future.

Forensics was applied through multiple efforts and programs to support intelligence operations and targeting, law enforcement, and medical support missions. The forensic exploitation of weapons and materials for intelligence purposes expanded greatly in response to the improvised explosive device (IED) and sniper threats in Iraq. Beginning with the efforts of a handful of latent print examiners to identify IED cell members and snipers, other forensic capabilities were incrementally deployed on the initiative of many individual organizations and communities.² Forensic laboratories with firearms signature, tool-mark, and DNA analysis capabilities were soon deployed to Iraq, while digital forensics examiners exploited captured computers and cell-phones for intelligence value. As the multi-discipline forensic laboratories were established in Iraq, they were leveraged not only against enemy targeting, but against the coalition mission of establishing the rule of law in Iraq. With little capability of its own to exploit potential evidence for prosecuting criminals, the Iraqi government relied upon the deployed DOD forensic labs to supply evidence and testimony in the prosecution of criminals within the Iraqi judicial system.

The growing number of forensic laboratories in Iraq spawned the need for the training of coalition ground forces in the identification, collection, and handling of materials for forensic exploitation. With no established forensics collection training plan, deploying units turned to multiple sources for help. In recognition of the immediate training requirement, organizations conducting forensic analysis responded by establishing mobile training teams to provide the necessary training. The dramatic impact of forensics to the success of these diverse missions led to an increase in the demand for forensic capabilities. The demand for forensic training and analytical assets was beginning to exceed the supply. If the demand for forensic capabilities equated to its value, the value of forensic science to the warfighter had become unquestionable.³

By 2007, the success of the multiple individual forensic efforts, and the potential shortfall in resources, brought attention to the lack of an authority responsible for coordinating the ongoing efforts and ensuring that forensics was a capability that continued to be available in the long term. In a July 2007 memorandum Mr. John Young, then Director of Defense Research and Engineering (DDR&E), recommended that the Joint Requirements Oversight Council initiate a CBA to assess forensics as an enduring capability and to support a strategy to identify and manage the desired capabilities, develop supporting science and technology investments, information management requirements, and supporting manpower and technical skill levels. Once initiated, the CBA would become an 18 month effort that would provide for the establishment of forensics as an enduring capability.⁴

In recognition of the more immediate need to coordinate ongoing efforts, Mr. Young, in cooperation with the Army Provost Marshal General (PMG), also convened a three day Defense Forensics Workshop to address the coordination and resourcing of expeditionary forensic capabilities. Among the workshop's 55 findings and recommendations was the overarching recommendation to establish a joint management structure to oversee and guide the development of a defense forensics capability. The recommendations developed by the workshop attendees provided the groundwork for the establishment of the FESG. In a January 2008 memorandum,

the Under Secretary of Defense for Acquisition, Technology, and Logistics formally established the FESG to coordinate the development and management of defense forensics capabilities. The FESG Charter was signed in April 2008 and established the scope, objectives, membership and responsibilities of the FESG.

The concurrent establishment of the FESG with the initiation of the Forensics CBA serves as a reminder of the separate solutions that have been implemented to resolve the two sides of the same capability gap. While the CBA is expected to provide solutions across the doctrine, organization, training, materiel, leadership, personnel and facilities (DOTMLPF) spectrum to establish an enduring forensics capability, the FESG was established as an interim solution to rectify the immediate management gap. The FESG need only exist until a forensics Executive Agent and Principal Staff Assistant are designated, and the CBA has informed the creation of an enduring capability. This fact presents the FESG with its most fundamental challenge: How can an interim organization maintain its relevance and authority? The answer lies in the organization and membership of the FESG.

FESG Structure and Organization

The structure and organization of the FESG was developed in recognition of the several organizations which have a significant investment in the future of forensics as an enduring capability. The leadership of the FESG is composed of the principals of three DOD organizations: the Defense Intelligence

Agency's Directorate for Measurement and Signals Intelligence and Technical Collection (DIA-DT); the Biometrics Task Force (BTF); and the Army's senior law enforcement officer, the PMG. The three chairs are responsible for providing oversight and undertaking resolution of issues across DOD forensics initiatives and programs. The chairs are supported in this effort by the Chairman of the DOD Forensic Science Committee, who is responsible for advising the FESG on matters pertaining to the technical aspect of forensics (see Figure 1).

While the FESG co-chairs provide the necessary guidance and direction to the FESG, the continuing progress of the FESG will occur as a result of the work of its membership. One strength of the FESG is that it exists as the single forum and structure for the DOD forensic community to communicate its requirements and coordinate its efforts with other organizations. Originally chartered to include only the Services, combatant commanders, and a handful of other DOD activities as its members, the FESG membership has grown to over 30 Service, staff, and joint organizations. These organizations have come to realize that it is in their best interests to be involved as the FESG has begun to address resourcing immediate expeditionary forensic requirements and is taking the steps to establish the foundation for an enduring forensic capability. The FESG membership is comprised of all DOD forensic stakeholders, or organizations that have an interest, due to either direct or indirect participation in one or all of the forensic functions. It includes organizations across operational, medical, intelligence, and law enforcement fields; across the Services, the Joint Staff, combatant commands, and other DOD activities. (See the partial list of FESG members and their contributions to the forensics community at the end of this article.)

The body of the FESG structure is divided among three working groups which are structured along three distinct topics related to forensics governance:

- ◆ Transformation and policy.
- ◆ Capabilities and requirements.
- ◆ Training and certification.

Each FESG member has a voice in the recommendations forwarded to the co-chairs from each working group. More

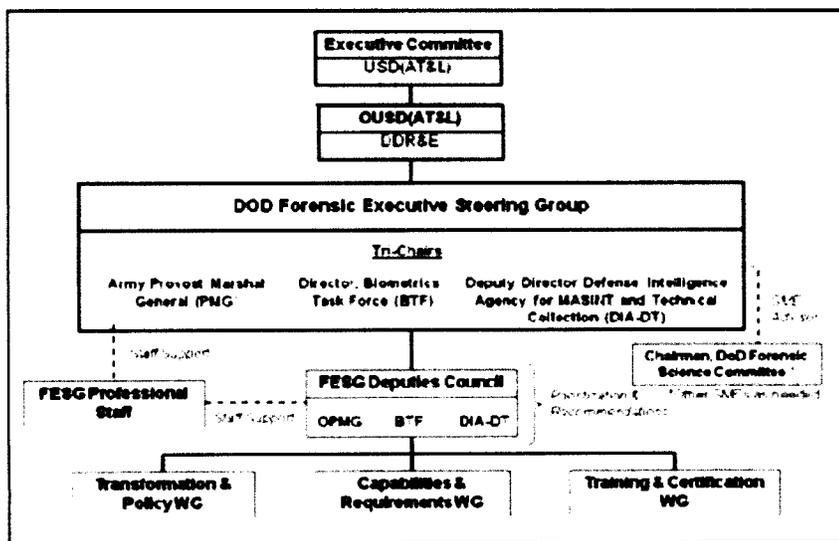


Figure 1. FESG Structure.

importantly, the solutions and recommendations developed in each working group are the result of the direct participation of the FESG membership. The full participation in ongoing, and future FESG working group efforts are critical because the FESG relies upon the expertise that resides in the decentralized forensic environment to develop realistic and prudent solutions to immediate capability needs.

The Capability and Requirements Working Group's (CRWG) newly developed requirements process is a prime example of how membership participation in a working group task can directly impact DOD forensic governance decisions. As proposed, the process allows for the CRWG to examine all emerging capability requirements, and using the expertise resident in the CRWG membership, provide resourcing recommendations that will best satisfy those emerging requirements. The recommendation will then go forward with the weight of the entire forensic community behind it.

The FESG members, through the working groups have also taken the first steps toward establishing the foundation for an enduring forensics capability. The development of the Capstone Concept of Operations (CONOPS) for DOD Forensics was made possible through the participation of the FESG membership. The CONOPS provides the basis for the assessment and analysis of capability gaps and redundancies done using the CBA process. The Training and Certification Working Group's examination of Battlefield Collection Training and forensic examiner and technician training standards will also directly feed the CBA demand for information and analysis. It is critical to the timeliness of the CBA that all the efforts of the FESG membership continue to directly feed into the CBA process. It is through this relationship with the CBA that the FESG members will have a direct impact on the establishment of an enduring forensic capability.

Conclusion

Interim or not, the FESG is moving forward with decisions which impact both the forensic community and the warfighter. As the DOD biometrics capability has grown more robust, forensic collection and analysis capabilities have become a vitally important link between an anonymous enemy and the evidence which links him to a specific event or

place. As the enemy transitions from an infrastructure-based hierarchy to one based on a social network of individuals, it is essential that the DOD develop and maintain the means to detect and identify the unique signature of individuals. Tasked with the responsibility to both maintain the expeditionary forensic capability and to establish an enduring capability, the FESG will rely upon its membership to provide the solutions which will accomplish those tasks. The FESG will succeed or fail based on the dedication of its membership to the accomplishment of those tasks.

Membership of the FESG

This partial membership listing is not intended to be all inclusive roster of the FESG, but rather a sample which illustrates the diverse organizations which have come together to support both an expeditionary and enduring forensic capability within DOD. This list is not intended to provide a description of the full scope of the organizations activities. For more information on any of the organizations listed here, refer to the sources listed in each organization's description.

U.S. Air Force Office of Special Investigations (AFOSI). AFOSI provides professional investigative service to commanders of all Air Force activities. Its mission is to identify, exploit, and neutralize criminal, terrorist and intelligence threats to the U.S. Air Force, DOD, and the U.S. The agency reports to the Inspector General (IG), Office of the Secretary of the Air Force. AFOSI is headquartered at Andrews Air Force Base, Maryland and has units in 221 places globally, both on Air Force bases and in strategically important locations around the globe.
<http://www.osi.andrews.af.mil/>.

Armed Forces DNA Identification Laboratory (AFDIL). AFDIL provides human remains identification, forensic DNA analytical services, bio-informatic analysis and management services, mass fatality specimen collection and management services, human reference specimen collection, cataloging, archival, and retrieval repository services. It supports the Armed Forces Medical Examiner System (AFMES) and Armed Forces Institute of Pathology (AFIP) through consultation, education and research. AFDIL is located in Rockville, Maryland. <http://www.afip.org/consultation/AFMES/AFDIL/index.html>.

Biometrics Task Force (BTF). The BTF leads DOD activities to program, integrate, and synchronize bi-

ometric technologies and capabilities and to operate and maintain DOD's authoritative biometric database to support the National Security Strategy. The BTF acts as the DOD proponent for biometrics, leading the development and implementation of biometric technologies for combatant commands, Services, and agencies, delivers capabilities in order to contribute to the enhancement of the biometric community, and empowers the warfighter by improving operational effectiveness on the battlefield.

<http://www.biometrics.dod.mil/>.

DOD Cyber Crime Center (DC3). DC3 sets standards for digital evidence processing, analysis, and diagnostics for any DOD investigation that requires computer forensic support to detect, enhance, or recover digital media, including audio and video. The center assists in criminal, counterintelligence (CI), counterterrorism, and fraud investigations of the Defense Criminal Investigative Organizations (DCIOs) and DOD CI activities. It also supports safety investigations and IG and commander-directed inquiries. DC3 aids in meeting intelligence community (IC) document exploitation objectives from a criminal law enforcement forensics and CI perspective. DC3 provides computer investigation training to forensic examiners, investigators, system administrators, and any other DOD members who must ensure Defense information systems are secure from unauthorized use, criminal and fraudulent activities, and foreign intelligence service exploitation. DC3 is located in Linthicum, Maryland. <http://www.dc3.mil/home.php>.

Defense Cyber Crime Institute (DCCI). DCCI provides legally and scientifically accepted standards, techniques, methodologies, research, and tools on digital forensics to meet the current and future needs of the DOD CI and law enforcement communities. <http://www.dc3.mil/home.php>.

Defense Cyber Crime Investigation Training Academy (DCITA). DCITA develops and delivers computer investigation training courses for DOD organizations, DCIOs, military CI agencies, and law enforcement organizations. The Academy is the only government organization solely dedicated to computer investigations training, development, and delivery. Students are trained in the latest digital forensic techniques using state-of-the-art equipment, classrooms, and technologies. <http://www.dc3.mil/home.php>.

Defense Computer Forensics Laboratory (DCFL). The DCFL mission is to provide timely and innovative digital evidence processing, analysis, and diagnostics for any DOD investigation that requires computer forensic support to detect, enhance, or recover digital media, to include audio and video. This includes on-site assistance including search and seizure and expert testimony. The DCFL supports criminal, CI, counterterrorism, and fraud investigations of DCIOs and DOD CI activities; but also safety investigations, IG directed inquiries and commander inquiries. DC3 also sets DOD guidelines for digital forensic analysis. <http://www.dc3.mil/home.php>.

Defense Intelligence Agency (DIA). DIA plays a central role in gathering, processing, and producing intelligence used to inform policymakers and warfighters alike. DIA has been a major part of the unification of effort among the IC as a whole. It is increasing its investment in the development of Human Intelligence and technical collection capabilities to further improve its surveillance and warning capabilities. <http://www.dia.mil/>.

Joint IED Defeat Organization (JIEDDO). JIEDDO leads, advocates, and coordinates all DOD actions in support of combatant commanders and their respective Joint Task Forces' efforts to defeat IEDs as weapons of strategic influence. JIEDDO works aggressively to find, develop, test and rapidly deliver emerging counter-IED (C-IED) capabilities to the warfighter. Split along three lines of operation (Attack the Network, Defeat the Device and Train the Force), JIEDDO's initiatives to help maximize warfighter capabilities include technical and forensic exploitation of devices, explosives detection and IED-specific pre-deployment training for Soldiers, Sailors, Airmen and Marines. JIEDDO tailors these initiatives to the urgent needs of combatant commanders, bringing them to the field quickly using its rapid acquisition capabilities. <https://www.jieddo.dod.mil/>.

Joint POW/MIA Accounting Command-Central Identification Laboratory (JPAC-CIL). The mission of JPAC-CIL is to achieve the fullest possible accounting of U.S. service personnel missing from past conflicts through the direct recovery and laboratory analyses of human remains. Located in Hawaii, it is the largest Forensic Anthropology laboratory in the world. <http://www.jpac.pacom.mil/>.

National Ground Intelligence Center (NGIC). NGIC produces and disseminates all-source integrated intelligence on foreign ground forces and related military technologies to ensure that U.S. forces have a decisive edge in current and future military operations. It is DOD's primary producer of ground forces intelligence. NGIC produces scientific and technical intelligence and military capabilities analysis on foreign ground forces required by warfighting commanders, the force modernization and research & development communities, DOD, and national policymakers. NGIC is leading the way in the U.S. Army Intelligence and Security Command's C-IED targeting program by providing technical intelligence and all source fusion capabilities to assist Multi National Forces-Iraq in identifying bomb-making networks in Iraq. NGIC is located in Charlottesville, Virginia. <http://www.inscom.army.mil/MS/DefaultNGIC.aspx?text=off&size=.8em>

National Media Exploitation Center (NMEC). NMEC is a Director of National Intelligence Center composed of DIA, CIA, FBI, NSA, and DC3 as partner organizations. NMEC is responsible for integrating Intelligence Community DOMEX policies, standards, and procedures with tactical and operational level DOD procedures and ensures responsive DOMEX support to meet the needs of intelligence, defense, homeland security, law enforcement, and other U.S. Government consumers.

Naval Criminal Investigative Service (NCIS). NCIS is the primary law enforcement and CI arm of the U.S. Department of the Navy. It works closely with other local, state, federal, and foreign agencies to counter and investigate the most serious crimes: terrorism, espionage, computer intrusion, homicide, rape, child abuse, arson, procurement fraud, and more. Examiners in NCIS' forensic laboratories play an important part in supporting agency investigations by examining evidence and providing testimony in court. The examiners apply their expertise in analyzing arson accelerants, trace evidence, latent fingerprints, questioned documents, and drug chemistry and related chemicals. <http://www.ncis.navy.mil/ncis/index.asp>

Provost Marshal General (PMG). The PMG leads and directs policy for Army law enforcement, police intelligence, physical security, corrections and internment, criminal investigations, and military police support throughout the full range of

military operations. The PMG supports the Army for management and execution of the Army Force Protection mission including antiterrorism operations and intelligence functions and serves as the commanding general of U.S. Army Criminal Investigation Command. <https://www.us.army.mil/suite/page/409448>

U.S. Army Criminal Investigation Laboratory (USACIL). USACIL provides worldwide forensic laboratory service, training, and R&D to all DOD investigative agencies in trace evidence, DNA/Serology, latent prints, firearms and toolmarks, digital evidence, drug chemistry, and forensic documents. It provides the widest range of services of all the DOD accredited forensic laboratories. USACIL also operates an Army school to train forensic laboratory examiners and manages the U.S. Army CID Command criminalistics and visual information programs. Of the federal laboratories accredited by the American Society of Crime Laboratory Directors-Laboratory Accreditation Board, only the Federal Bureau of Investigation Laboratory offers as many supporting forensic disciplines as USACIL. USACIL, located at Fort Gillem, Georgia, provides forensic laboratory services to DOD investigative agencies and other federal law enforcement agencies. <http://www.cid.army.mil/usacil.html>. ❖

Endnotes

1. FESG Charter, April 2008.
2. John J. Young, Jr., Defense Forensics Workshop Invitation, July 25, 2007.
3. For more detail on the early forensics efforts in Iraq, read the article by Tom Cantwell and Sean Falconi in this issue.
4. John J. Young, Jr., Defense Forensics Workshop Invitation, July 25, 2007.

Captain Shawn McMahon is currently assigned to the Office of the PMG serving on the Professional Staff of the FESG. He holds an MA in Strategic Intelligence from the National Defense Intelligence College and is a graduate of the MI Captains Career Course.

USACIL RBOC:

Providing Support to the Warfighter and Expeditionary Forensics



by William G. Doyne

Introduction

Given the demonstrated successes of Weapons Technical Intelligence, Biometrics and the forensic functions performed at the Combined Explosive Exploitation Cell (CEXC) Labs, it is clear that forensics not only has a role on the current battlefield but also is a force multiplier. The need for a non-improvised explosive device (IED) (material which is not associated directly with the device exploitation) forensic capability to augment the CEXC labs IED oriented forensics has generated a requirement for expeditionary forensics.

Forensics is the application of multi-disciplinary scientific processes to establish facts. Expeditionary forensics is currently provided by the Joint Expeditionary Forensic Facilities (JEFFs) and can be used to:

- ◆ Establish facts that can be used by commanders to shape force protection measures.
- ◆ Drive intelligence analysis and subsequent targeting for combat operations.
- ◆ Prosecute detainees in a court of law.
- ◆ Determine sources of insurgent arms, ammunition, and explosives.

Expeditionary Forensics and Intelligence Operations combine to degrade the enemy's ability to capitalize on anonymity. (U//NF)

The result is often usable intelligence as well as the moral and legal justification needed to target, apprehend, and prosecute terrorists or enemy combatants.

The downside of this success is that it has generated an increase in the amount of potential forensic material collected, resulting in an increased workload at both the CEXC and JEFF labs, the Terrorist Explosive Device Analytical Center (lab providing CONUS support to the CEXC labs), and the Biometric Fusion Center (BFC). As Site Exploitation and Forensic Collection training programs and accompanying tactics, techniques, and procedures are developed and promulgated, there will be more units collecting material further exacerbating the severity of the situation.

Reach Back Operations Center

It is largely unrecognized that the Department of Defense (DOD) possesses one of the most powerful forensics toolsets in the U.S. because the forensics capability is dispersed throughout DOD and is uncoordinated. Forensics has historically been used mainly to support criminal investigations and human remains identifica-

tion for judicial and medical reasons. In order to leverage these capabilities in the LP, DNA, and firearms/tool marks (FA/TM) areas to support the warfighter in-theater, the U.S. Army Criminal Investigation Laboratory (USACIL) has established the Reach Back Operations Center (RBOC).

The RBOC mission is to provide support to the warfighter and to expand JEFF forensic capabilities by leveraging DOD's institutional forensic laboratories, accessing national and international forensic databases, and utilizing CONUS expertise without increasing the in-theater footprint or sustainment costs. RBOC will support the warfighter by:

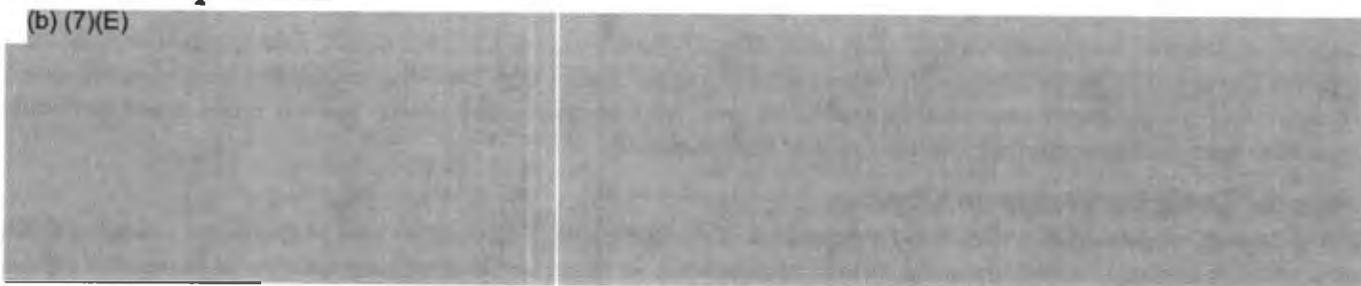
- ◆ Providing assistance to DOD and Allied force commanders when triaging specific forensic LP, DNA and FA/TM potentialities.
- ◆ Serving as the authoritative resource for advice on the development, purchase, and deployment of technical and scientific LP, DNA, and FA/TM equipment or techniques in forensics.
- ◆ Providing forensic analysis interpretation of exploited materials to supported commanders, investigators, and intelligence agents when needed at all stages of examinations.
- ◆ Conducting and/or coordinating appropriate forensic research, developing new forensic applications, testing, and evaluating emerging technologies.

RBOC will support the JEFFs, as well as CEXC labs and others upon request, by:

- ◆ Providing LP and FA/TM identification verification.
- ◆ Assisting in monitoring complex LP case interpretation in collaboration with deployed lab personnel.
- ◆ Conducting Integrated Automated Fingerprint Identification/Automated Biometric Identification System (IAFIS/ABIS) database searches and providing reports.
- ◆ Receiving material from JEFFs and assisting in the processing of highly difficult, sensitive, and technical cases.
- ◆ Conducting Questioned to Known comparisons of latent impressions
- ◆ Providing footwear and tire track analysis, examinations, comparisons, and verifications.
- ◆ Providing technical advice on DNA data basing capabilities and search results.
- ◆ Providing guidance on DNA technical review.
- ◆ Providing DNA data interpretation and technical review.
- ◆ Providing performance checks on new DNA equipment.
- ◆ (b) (7)(E)
- ◆ (b) (7)(E)
- ◆ Assisting in working all firearm case-related evidence including comparison examinations and conclusions.
- ◆ Assisting in working TM cases including comparison examinations and conclusions.
- ◆ Providing distance determination evaluation and bullet trajectory analysis.
- ◆ Providing and supporting Integrated Ballistic Identification Systems operations.

RBOC Composition

(b) (7)(E)



All personnel will be members of the DOD.

(b) (7)(E)

The RBOC is a win-win proposition for all individuals and organizations concerned. Initially concern was expressed that this was an effort to take from another "rice bowl", fix a system that isn't broken, or just become a "bump" in the road. Currently most forensic faculties are working at or near maximum capacity and have some degree of a case backlog. As indicated earlier, forensic processing and analysis capability is directly proportional to the collection capability. Since forensic examiners, particularly the certified variety, are a limited asset there is a significant lag time where the time the need for additional capacity (i.e., more examiners) is identified and when it becomes available. This is true whether the more expensive route of contractors is taken or the cheaper but longer route of training DOD personnel is selected. Therefore, it makes a great deal of sense to maximize current capabilities with the minimum resources.

RBOC's Benefits to Expeditionary Forensics

It is important to recognize that in expeditionary forensics, there are certain tasks that can be completed in-theater or in the rear and some tasks that can only be accomplished in-theater. For example, transporting material out of theater for LP processing can be done; however, it is generally not practical because of the transportation time involved. So it makes sense that LP processing should be done in-theater. LPs present or developed on forensic material are normally captured digitally and transmitted to either the BFC for search in the ABIS or the Federal Bureau of Investigation's Criminal Justice Information Services for search in IAFIS.

The time required for these actions is time taken away from processing material which is best done in-theater.

(b) (7)(E)

This method is invisible to the in-theater examiner and assists the BFC by reducing its workload.

U.S. Army Criminal Investigation Laboratory (USACIL)



USACIL Reach Back Operations Center

Chief Lead Forensic Scientist Operations Officer

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

RBOC DNA examiners can assist with data interpretation, particularly with DNA mixture interpretation (profiles with multiple contributors) and technical reviews. In those circumstances where material can be sent to CONUS for processing, (i.e., large back log, low priority, not time sensitive) with appropriate coordination with the RBOC chief, USACIL RBOC examiners can receive, process, and render reports to support in-theater labs.

RBOC on AKO and AKO-S

USACIL RBOC has established a page on both AKO and AKO-S so that users can submit RFI/RFA and upload images (both LP and FA/TM) for search or verification. You can request access to the RBOC page by emailing the following information to bill.doyne@us.army.mil or kevin.kahley@us.army.mil:

RBOC Community Membership Request

Name: _____

Date: _____

Organization/Position: _____

NIPR Email Address: _____

SIPR Email Address: _____

DSN Phone Number: _____

Commercial Phone Number: _____

VOIP Number: _____

FAX Number: _____

Secure Telephone: _____

Reason for Submitting Request: _____

Conclusion

As DOD builds on the hard work and vision of those individuals who saw the potential of forensics on the current battlefield to transition to a cost-effective enduring forensic capability, the introduction of the USACIL RBOC will serve as the genesis for that effort. As the JEFF Concept Plan works its way through the system to become a program of record, the RBOC will provide the tools necessary for commanders and current expeditionary forensic facilities to maximize capability and capacity at minimum cost. 

William Doyne is currently employed as a DA Civilian at the USACIL and serving as the chief of the RBOC. Prior to becoming the RBOC chief, he was assigned as an LP examiner in the LP Branch. Mr Doyne is certified as an IAI Latent Fingerprint Examiner and Footwear Examiner. He has a BS in engineering from the U.S. Military Academy, an MA in Chemistry from Villanova University, and a Public Education Certification from Wilson College. Mr. Doyne is a retired U.S. Army Colonel with over 30 years service as an Infantry officer.

TRADOC Capability Manager—Biometrics and Forensics (TCM-BF)

Fort Huachuca, Arizona



TCM-BF serves as the Army use advocate to Program Manager (PM) DOD Biometrics and designated Forensics PMs, and coordinates closely with other service and branch proponent user representatives to enable, facilitate, and champion the development of biometrics and forensics across the Doctrine, Organization, Training, Materiel, Leadership, Personnel and Facilities (DOTMLPF) spectrum with Army, Joint, interagency, allies, Coalition, and National organizations.

TRADOC Capability Manager-Biometrics and Forensics Office and the Department of Defense (DOD) define forensics as *“the application of multi-disciplinary scientific processes to establish facts.”*

Traditionally, the DOD has employed forensics to establish facts for use in: investigations, a court of law, Uniform Code of Military Justice proceedings, or to determine the identification of human remains as well as cause and manner of death.

The War on Terrorism has produced emerging needs and capabilities for forensics across the range of military operations.

Forensics has an integral role in intelligence functions, operational activities, force protection, host nation legal support, personnel recovery, and identity superiority functions.

Recently, operations in Afghanistan and Iraq Theatres have validated the importance of forensics in providing intelligence and battlefield awareness for military decision-making and operations at all levels.

TCM-BF Contacts

Director

COL Mark R. Wallace
(520) 533-4432 / DSN 821
NIPR: mark.wallace@us.army.mil
SIPR: mark.wallace@us.army.smil.mil

Deputy Director

Kathy Debolt
(520) 533-4657 / DSN 821
NIPR: kathy.debolt@us.army.mil
SIPR: kathy.debolt@us.army.smil.mil

Forensics Division Lead

LTC Malcolm McMullen
VOIP (520) 515-1797
NIPR: malcolm.mcmullen@us.army.mil
SIPR: malcolm.mcmullen@us.army.smil.mil

Operations Officer

MAJ Clea McCaa
(520) 533-0304 / DSN 821
NIPR: clea.mccaa@us.army.mil
SIPR: clea.mccaa@us.army.smil.mil

Senior Enlisted Advisor

MSG Nestor Rodriguez
(520) 533-0303 / DSN 821
NIPR: nestor.rodriquezjr@us.army.mil
SIPR: nestor.rodriquezjr@us.army.smil.mil

TCM BF Web Portal:

<https://67.128.198.116/sites/TPO-BF/default.aspx>

A

AAIDB	Anti-Armor Incident Database
AATF	Anti-Armor Task Force
ABIS	Automated Biometric Identification System
ACE	Analysis Control Element
ADCON	administrative control
AFDIL	Armed Forces DNA Identification Laboratory
AFI	automated fingerprint identification
AFMES	Armed Forces Medical Examiner System
AFOSI	U.S. Air Force Office of Special Investigations
AFRSSIR	Armed Forces Repository of Specimen Samples for the Identification of Remains
AIMS	Automated Identity Management System
ALARACT	all Army activities
AMSAA	Army Materiel Systems Analysis Agency
AO	area of operation
AOR	area of responsibility
ARL	Army Research Laboratory
AT&L	Acquisition, Technology, and Logistics
ATF	Bureau of Alcohol, Tobacco, Firearms and Explosives

B

BAT	Biometric Automated Toolset
BCT	brigade combat team
BESB	ABIS Biometric Examination Services Branch
BEWL	Biometric-Enabled Watch List
BIAR	Biometrics Intelligence Analysis Report
BISA	Biometric Identification System for Access
BOD	DOD Biometric Operations Directorate
BTF	Biometrics Task Force
BUSK	Bradley Urban Survivability Kit

C

CALL	Center for Lessons Learned
CBA	capabilities based assessment
CCCI	Central Criminal Court of Iraq
CED	Iraqi Criminal Evidence Division
CENTCOM	U.S. Central Command
CEXC	Combined Explosives Exploitation Cell
CEXC-A	Combined Explosives Exploitation Cell-Afghanistan
CEXC-I	Combined Explosives Exploitation Cell-Iraq
CID	U.S. Army Criminal Investigation Command
CIDNE	Combined Information Data Network Exchange
CIED	counter improvised explosive device
CIL	JPAC Central Identification Laboratory
CITP	Counter-IED Targeting Program
CJCSI	Chairman of the Joint Chiefs of Staff Instruction
CJIS	Criminal Justice Information Services
CNR	Center for National Response
COCOM	combatant command
CODIS	Combined DNA Index System
CONOP	concept of operation
CONUS	continental United States
CPA	Coalition Provisional Authority

CRWG Capabilities and Requirements Working Group
 CTC combat training center
 CTC U.S. Military Academy Counter Terrorism Center

D

DC3 DOD Cyber Crime Center
 DCCI Defense Cyber Crime Institute
 DCFL Defense Computer Forensics Lab
 DCGS-A Distributed Common Ground System-Army
 DCITA Defense Cyber Crime Investigation Training Academy
 DDR&E Director of Defense Research and Engineering
 DFES Defense Forensics Enterprise System
 DFL Defense Forensic Laboratories
 DFN Defense Forensic Network
 DFTRA Defense Forensics Training & Research Academy
 DHS U.S. Department of Homeland Security
 DIA Defense Intelligence Agency
 DNA deoxyribonucleic acid
 DOD Department of Defense
 DOMEX document and media exploitation
 DOTMLPF doctrine, organization, training, material, leadership, personnel, and facilities
 DT Directorate for MASINT and Technical Collection (DIA)

E

EA executive agent
 EBTS Electronic Biometric Transmission Specification
 EFL expeditionary forensic laboratories
 EFP explosively formed projectile
 EJK-TF Extra-Judicial Killing Task Force
 EOD explosive ordnance disposal, explosive ordnance detachment
 ES2 Every Soldier is a Sensor

F

FA firearm
 FBI Federal Bureau of Investigation
 FEB Forensic Exploitation Battalion
 FEI For everyone's information
 FESG Forensics Executive Steering Group
 FOB forward operating base
 FOC full operational capability
 FORINT Forensics Intelligence
 FP Forensic Photographer
 FRT Firearms Reference Table

G

G2 Army or Marine Corps component intelligence staff officer
 G3 Army or Marine Corps component operations staff officer
 GRC general rifling characteristics

H

HARMONY National DOMEX database
 HBCT heavy brigade combat team

HIIDE Handheld Interagency Identity Detection Equipment
HJC Higher Judicial Council (Iraq)
HMMWV high-mobility multipurpose wheeled vehicle
HUMINT Human Intelligence
HVAC high-voltage air conditioning

I

IAFIS Integrated Automated Fingerprint Identification System
IAI International Association for Identification
IBIS Integrated Ballistic Identification Systems (ATF)
IC Intelligence Community
ICO Iraqi correctional officers
IDENT DHS Automated Biometric Identification System
IdM Identity Management
IED improvised explosive device
IIR intelligence information report
IO information operations
IOC initial operational capability
IPB Intelligence Preparation of the Battlespace, Intelligence Preparation of the Battlespace
ISAF International Security Assistance Force
ITF Investigative Task Force
ITO Iraqi Theatre of Operations
IZ Iraq
IZ International Zone

J

J2 Intelligence Staff Officer; Joint command
JATAC Joint Asymmetric Threat Awareness Counter
JCIDS Joint Capabilities Integration Development System
JDEC Joint Document Exploitation Center
JEFF Joint Expeditionary Force Forensics, Joint Expeditionary Forensic Facility
JFC Joint force commander
JIEDDO Joint IED Defeat Organization
JITEC Joint Interagency Training and Education Center
JPAC Joint POW/MIA Accounting Command
JPEC Joint Prosecution and Exploitation Cell
JROC Joint Requirements Oversight Council
JTAPIC Joint Trauma Analysis and Prevention of Injury in Combat

L

LE law enforcement
LEP Law Enforcement Professional
LIMS Laboratory Information Management Systems
LP latent print
LPE latent print examination

M

MASINT Measurement and Signature Intelligence
MEDEX media exploitation
METT-T mission, enemy, terrain, troops available, and time available
MiTT military transition team
MNC-I Multi-National Corps–Iraq
MND Multi-National Division

MND-North Multi-National Division–North (Iraq)
 MNF-W Multi National Force–West (Iraq)
 MOS military occupational specialties
 MRAP mine resistant ambush protected
 mtDNA mitochondrial DNA
 MTT mobile training team

N

NAVEODTECHDIV Naval Explosive Ordnance Disposal Technology Division
 NCIS Naval Criminal Investigative Service
 NCTC National Counter Terrorism Center
 NGA Next Generation ABIS
 NGA National Geospatial-Intelligence Agency
 NGI Next Generation Identification
 NGIC National Ground Intelligence Center
 NMEC National Media Exploitation Center
 NSTC National Science & Technology Council
 NTC National Training Center

O

O/C observer/controller
 OCONUS outside continental United States
 OEF Operation Enduring Freedom
 OIF Operation Iraqi Freedom

P

PIER 2.3 Portable Iris Enrollment and Recognition System
 PIR priority intelligence requirement
 PJCC Provincial Joint Coordination Center
 PM program manager
 PMG Provost Marshal General
 PPE personal protective equipment
 ppi pixels per inch
 PSA principal staff assistant
 PTSD Post Traumatic Stress Disorder

R

RBOC Reach Back Operations Center
 RFA requests for action
 RFI request for information
 ROMO range of military operations

S

S&T science and technology
 S2 intelligence staff officer; brigade, battalion, and Armored Cavalry
 S3 operations staff officer
 SIGACT significant activity
 SIPRNET Secret Internet Protocol Router Network
 SME subject matter expert
 SOCOM U.S. Special Operations Command
 SOP standard operating procedures
 SSE sensitive site exploitation
 SUV sport utility vehicles

T

TCM-BF	TRADOC Capability Manager-Biometrics and Forensics
TCWG	Training and Certification Working Group
TECHINT	Technical Intelligence
TEDAC	Terrorist Explosive Device Analytical Center
TIF	theatre internment facilities
TM	toolmark
TNT	Tactical Network Topology
TRADOC	U.S. Army Training and Doctrine Command
TSC	terrorist screening center
TSE	tactical site exploitation
TTP	tactic, technique, and procedure
TUSK	Abrams Tank Urban Survivability Kit

U

ULF	unsolved latent file
ULM	unsolved latent match
ULW	universal latent workstation
USACIL	U.S. Army Criminal Investigation Laboratory
USAIC&FH	U.S. Army Intelligence Center and Fort Huachuca
USD	Under Secretary of Defense
US-VISIT	U.S. Visitor and Immigrant Status Indicator Technology Program

V

V5	Military Police Investigator (ASI identifier)
VBIED	vehicle-borne IED

W

WIT	weapons intelligence team
WL	watchlist

Y

Y-STR	Y-chromosome—Short Tandem Repeat (STR)
-------	--





CONTACT AND ARTICLE Submission Information



This is your magazine. We need your support by writing and submitting articles for publication.

When writing an article, select a topic relevant to the Military Intelligence (MI) and Intelligence Communities (IC).

Articles about current operations and exercises; TTPs; and equipment and training are always welcome as are lessons learned; historical perspectives; problems and solutions; and short "quick tips" on better employment or equipment and personnel. Our goals are to spark discussion and add to the professional knowledge of the MI Corps and the IC at large. Propose changes, describe a new theory, or dispute an existing one. Explain how your unit has broken new ground, give helpful advice on a specific topic, or discuss how new technology will change the way we operate.

When submitting articles to MIPB, please take the following into consideration:

- ◆ Feature articles, in most cases, should be under 3,000 words, double-spaced with normal margins without embedded graphics. Maximum length is 5,000 words.
- ◆ Be concise and maintain the active voice as much as possible.
- ◆ We cannot guarantee we will publish all submitted articles and it may take up to a year to publish some articles.
- ◆ Although **MIPB** targets themes, you do not need to "write" to a theme.
- ◆ Please note that submissions become property of **MIPB** and may be released to other government agencies or nonprofit organizations for re-publication upon request.

What we need from you:

- ◆ **A release signed by your unit or organization's information and operations security officer/SSO stating that your article and any accompanying graphics and photos are unclassified, nonsensitive, and releasable in the public domain OR that the article and any accompanying graphics and photos are unclassified/FOUO (IAW AR 380-5 DA Information Security Program).** A sample security release format can be accessed at our website at <https://icon.army.mil>.

- ◆ A cover letter (either hard copy or electronic) with your work or home email addresses, telephone number, and a comment stating your desire to have your article published.
- ◆ Your article in Word. Do not use special document templates.
- ◆ A Public Affairs or any other release your installation or unit/agency may require. Please include that release(s) with your submission.
- ◆ Any pictures, graphics, crests, or logos which are relevant to your topic. We need complete captions (the Who, What, Where, When, Why, and How), photographer credits, and the author's name on photos. **Do not embed graphics or photos within the article. Send them as separate files such as .tif or .jpg and note where they should appear in the article. PowerPoint (not in .tif or .jpg format) is acceptable for graphs, etc. Photos should be at 300 dpi.**
- ◆ The full name of each author in the byline and a short biography for each. The biography should include the author's current duty assignment, related assignments, relevant civilian education and degrees, and any other special qualifications. Please indicate whether we can print your contact information, email address, and phone numbers with the biography.

We will edit the articles and put them in a style and format appropriate for **MIPB**. From time to time, we will contact you during the editing process to help us ensure a quality product. Please inform us of any changes in contact information.

Submit articles, graphics, or questions to the Editor at MIPB@conus.army.mil. Our fax number is 520.533.9971. Submit articles by mail on disk to:

MIPB
ATTN ATZS-CDI-DM (Smith)
U.S. Army Intelligence Center and Fort Huachuca
Box 2001, Bldg. 51005
Fort Huachuca, AZ 85613-7002

Contact phone numbers: Commercial 520.538.0956
DSN 879.0956.

FOR OFFICIAL USE ONLY



Check Out MIPB Online @



https://icon.army.mil/apps/mipb_mag/

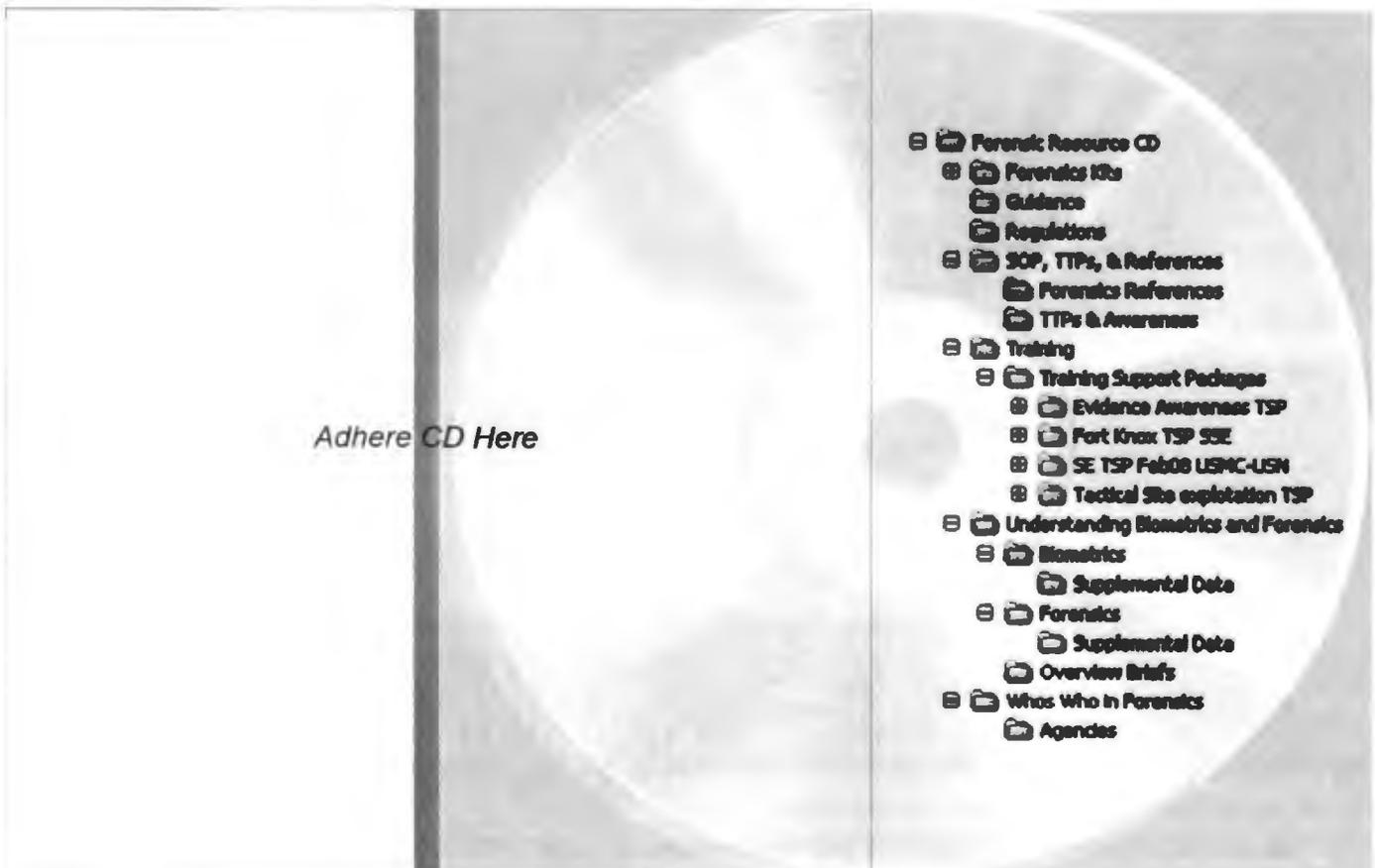


FOR OFFICIAL USE ONLY

Forensic Resource CD

- ◆ **The purpose of the Forensic Resource CD is to provide useful, relevant, and enabling information.**
- ◆ **The CD offers several resources, covering all applications to give the the Warfighter a holistic view of the forensic community, provide points of contact for training and resources, and other guidance related to DOD Forensics.**

- ◆ **Forensic Kits**
 - Available mission equipment and essential items.
- ◆ **Guidance**
 - Army and Theater specific guidance in managing site exploitation and task organization.
- ◆ **Regulation**
 - Know the supporting parameters.
- ◆ **SOPs, TTPs, and References**
 - See how units execute their Forensic missions.
 - Considerations for tactical site exploitation missions, lessons learned.
 - Observations on Forensic measures and effectiveness.
- ◆ **Training**
 - Training support packages, view available training.
- ◆ **Understanding Biometrics & Forensics**
 - How Forensics supports irregular warfare, the responsibilities, and effects.
- ◆ **Who's Who in Forensics**
 - Diagram of the community, understand the process, and know members in the Forensic community.



FOR OFFICIAL USE ONLY

FOR OFFICIAL USE ONLY

**ATTN: MIPB (ATZS-CDI-DM) 12
BOX 2001
BLDG 51005
FORT HUACHUCA AZ 85613-7002**



FOR OFFICIAL USE ONLY

**Headquarters, Department of the Army.
This publication is approved for public release.
Distribution unlimited.**

PIN: 085424-000