Moving away from a Name Based Paradigm

USMC BIOMETRICS
Agenda

• Identity management across the range of military operation
• Using identity management tools
  – Biometrics as a single tool of many to establish identity
  – Forensics
• How we operate
• Training implications
• Results we are seeing
• Biometrics & Forensics Training
• Sensitive Site Exploitation Training
Bottom Line Up Front

• Identity Management is not new
  – Using a name is effective, but a biometric is more effective
  – Biometrics is a tool
  – Forensics is a tool

• Solutions are less than perfect, but will improve

• We are at the beginning of the hard work, not the end
What We Do

• Locate, close with, and destroy the enemy
• Repel the enemy’s advance with fire and close combat
• America’s force in readiness
  – Disaster relief
  – Humanitarian Assistance

Who is the Enemy? Who is not?
What is Identity management?

• Distinguishing an individual (or group)
  from a crowd
• Individualizing people
  – Many ways of doing it
  – “Denying the enemy anonymity”

Where is the enemy?
Is he even there?
Identity Management

- What we do has not changed in a millennium:
  - We are still figuring out who is the enemy
  - "Halt who goes there?"
  - Positive ID
  - IFF transponders
  - Order of battle
  - Electronic Order of battle
  - Biometric Order of battle

- Then we destroy them

- How we do it is changing

2000 Years
Military Identification

Past

• Large formations
• Uniforms
• Equipment
  – BRDM vs BMP

Now

• No formations
• No Uniforms
• Indistinguishable Equipment
• Lots of Individuals
Establishing Identity

Identity

- People
  - Know
  - Operation
- Activity
  - Other
  - Technology
- Other
  - Finger prints
  - Blood vessels
- Iris
  - Are
  - Respiration
- DNA
  - Face
  - Gait
- Credit Card
- Phone
- Computer
- ID
  - Own
- Relationships
- Other
- Vehicle
- Property
- Other
  - Activity
  - Spending Habits
- Painting
- Other
  - Eating
  - Do
  - Read Books
- Crime
- Movement
- Drive

UNCLASSIFIED
Identity Management Uses

- Detainee Management
- Access control
- Population Screening
  - Entry Control Points
  - Gated Communities
  - Election Workers
  - Third Country Nationals
  - Locally Employed Persons
  - Resource distribution.

- Law Enforcement
- Targeting Packages
- Business functions / delivery of services
  - Medical
  - Pay
  - Feeding
Identity Management Tools

• Data bases
  – Collect, index, collate, cross reference information

• New tools
  – Biometrics
  – Forensics
Old Paradigm

- Name based
  - Language
  - Alphabet
  - Cultural- Multiples names
- Activity based
  - Associations
  - Occupation
  - After hours
- Knowledge based
  - Phone numbers
  - Email they know
  - Education

- Geneva Convention
  - Name, Rank, Serial number
- Red, Blue, civilians
New Paradigm

- How do you verify a name?
  - How do you ensure they are not a civilian?
  - What if they are lying?
  - Honest mistakes?

- Need something that does not change and is difficult to hide!

- When you encounter a combatant now what?
  - No unit to tie them to?
  - No uniform or equipment to associate them with?
  - Enemy hides among the population
    - Red, Blue, GRAY

- Deny them anonymity
What is Biometrics?

Biometrics (National Science and Technology Council Definition): Biometrics is a general term used alternatively to describe a characteristic or a process. [Biometrics Glossary]

- As a characteristic: A measurable biological (anatomical and physiological) and behavioral characteristic that can be used for automated recognition.
- As a process: Automated methods of recognizing an individual based on measurable biological (anatomical and physiological) and behavioral characteristics. The National Institute of Standards and Technology (NIST) performs research in measurement, evaluation and standards for fingerprint matching and interchange, criminal justice information systems, face recognition and multi-modal biometrics.
Why Biometrics

• Deny the enemy anonymity
  – Inhibits anti-coalition forces and criminal elements movement
  – Deters & complicates anti-coalition & criminal element access to US facilities.

• Aids identification of targets

• Reduced incidents of inadvertently releasing dangerous detainees through administrative error or the detainee's use of deception.
What is Forensics?

• Uses science to establish fact

• Is a collection platform for biometrics
  – No different than BAT or BISA
  – Collects non-biometrics also
Why Forensics?

- Links events, people, and things
- Enables you to use biometrics effectively

Current Uses

- Grunts exploiting sites
- Document Exploitation
- Forensics Databases
How we do and will operate

• Present: MEF, MEB, MEU
  – Using and developing biometric enabled Intel at the Bn level

• Future: Distributed Company and Platoon Operations doing thing battalions do now
  – Biometric support
    • New uses for biometrics
    • New modalities
  – What have we not thought of?
What we do?

Then

- Nominate a target using data
  - Targets were things and units
- Assess effectiveness of servicing target
- Write down name, rank, serial number
- Grab things of intel value
  - Docs
  - Radios
  - Code books
  - Weapons
Training Implications

• Biometrics
  – Employment?
  – Equipment operations?

• Forensics
  – Protecting forensic material during site exploitation?
  – Lifting fingerprints, Extracting DNA, comparing tool marks?

• If yes, were you told you would do it
  – In a combat zone
  – Sleeping in the combat zone side by side with the Marines
  – In a lab that is not certified
How we are getting there

• Training is at the option of the commander
  – Biometric Equipment Operator Level
  – Biometric networking and trouble shooting
  – Biometrics Operations Course
  – Forensics is included in site exploitation courses

• Verified at Mojave Viper
Results
In late 2007, The Joint Prosecution and Exploitation Center (JPEC) investigated a Jaysh Al Mujahidin (JM) cell which was conducting kidnappings, murders and IED/SAF attacks in the Ramadi area. The investigation began with the capture of Qudair Walid Farhan who was the JM propagandist. During the capture, Farhan’s computer was seized and later exploited by the Document and Media Exploitation (DOMEX) section assigned to JPEC. This further led to the discovery of multiple videos of the JM cell conducting IED/SAF attacks on Coalition Forces (CF). The faces of the insurgents were electronically obscured to hide their identities; however, DOMEX removed the obscuration which allowed JPEC investigators to identify 10 additional insurgents; two of which were Iraqi Police Officers. Target packages were then developed and the JM cell was captured by operating forces. JPEC then developed prosecution packages in preparation for trial at the Central Criminal Court of Iraq (CCCI). All (11) JM insurgents were convicted of terrorist acts at the Central Criminal Court of Iraq with (6) receiving the death penalty.
CONVICTIONS

Khudayir Walid Farhan

Nazar Muhammad Khalaf

Ahmad Khalil Fayyad

Muhammad Rauf Al-Rawi

Basim Muhammad Suidan

Shakir Mahmud Salih

Yasir Hamzah Khaddam

‘Abdallah Sami Salih

FILMED VIDEOS

Abbas Khudayir Abbas

Muhammad Fahad Jasim

UNCLASSIFIED
USMC Biometric and Forensics Training and Education
Thoughts on Training

• Sending untrained men to war is sending them to their death.
  • Sun Tzu

• The country that draw too great a distinction between it’s warriors and it scholars, will have it’s thinking done by cowards and it fighting done by idiots.
  • Thucydides

• What is untrained?
• How does biometrics fit into the picture?
Holistic Approach

• CAVEATS - 24 hours in a day
• Multiple needs – Marksmanship – First aid – Counter IED training – Equipment Maintenance – Unit movement – Language training – Communication – Call for fire – Crew Served Weapons training
Training Implications

• Did anyone in the room learn at your MOS school:
  – Biometrics
    • Employment?
    • Equipment operations?
  – Forensics
    • Protecting forensic material during site exploitation?
    • Lifting fingerprints, Extracting DNA, comparing tool marks?
  – If yes, were you told you would do it
    • In a combat zone
    • Sleeping in the combat zone side by side with the Marines
    • In a lab that is not certified
First Biometrics Operators Course

- A520 Camera
- CF-73/74 Toughbook
- 10 Print Reader
- Fingerprint Reader
- Iris Reader
- 500GB Hard Drive
“Sgt Bruns here it is, figure out how it works, and figure it out how we can use it.”
How we are getting there

• Training is at the option of the commander
  – Basic Operator Course
  – Advanced Operator Course
  – Biometrics Manager Course
  – Leaders Training Course
  – Forensics is included in site exploitation courses

• Train as we fight at Mojave Viper
Are they getting the right training?
How we are getting there (Cont)

• In country
  – FSE help to maintain and constantly keep current
  – Refresher training on site exploitation training
  – Left seat/ right seat ride

• Feed Back
  – Town hall
  – Marine Corps Center for Lessons Learned
Resources

- Biometric systems at Mojave Viper
- Training Support Package
- Best Practice Guide
- Field Reference Cards
- Training Kits
Anyone can use them!!!

- Training Support Package is $210.00 per copy, stock number 008-001-00190-8 (only one per instructor needed)
- Best Practice Guide is $38.00 per copy, stock number 008-001-00188-6 (ideally one per student needed)
- Field Reference Cards are $19.00 for 5 copies, stock number 008-001-00189-4 (ideally one per student needed)
- Training Kits (not available through GPO) cost $450 each to procure items and assemble.
Supporting Instructors

• Training Command (TECOM)
• Marine Corps System Training Center
• Marine Corps Systems Command
• Forensics work with other sources
  – NGIC
  – FBI
  – LA County Sherriff
  – Friend of a Friend of a Friend
Some other training

<table>
<thead>
<tr>
<th>Current Name</th>
<th>Length of Instruction</th>
<th>Training Organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Level 1: Evidence Collection and Exploitation</td>
<td>4 hrs.</td>
<td>USA Military Police School (USAMPS)</td>
</tr>
<tr>
<td>Level 2: Evidence Collection and Exploitation</td>
<td>5 Days/ 40 hrs.</td>
<td>USA Military Police School (USAMPS)</td>
</tr>
<tr>
<td>Level 3: Evidence Collection and Exploitation</td>
<td>6 hrs.</td>
<td>USA Military Police School (USAMPS)</td>
</tr>
<tr>
<td>Combat Search Operations</td>
<td>5 Days</td>
<td>US Army Engineer School US Army Counter Explosive Hazards Center</td>
</tr>
<tr>
<td>Advanced Search Operations</td>
<td>3 Weeks</td>
<td>US Army Engineer School US Army Counter Explosive Hazards Center</td>
</tr>
<tr>
<td>Unk</td>
<td>Unk</td>
<td>US Army: Asymmetric Warfare Group (AWG)</td>
</tr>
<tr>
<td>Tactical SE (Battlefield Forensics)</td>
<td>4 Days/ 40 hrs.</td>
<td>National Ground Intelligence Center (NGIC)</td>
</tr>
<tr>
<td>Evidence and Forensic-related Biometric Collection Course MTT</td>
<td>4 Days/ 40 hrs.</td>
<td>National Ground Intelligence Center (NGIC)</td>
</tr>
<tr>
<td>DOMEX</td>
<td>5 Days</td>
<td>Numerous</td>
</tr>
<tr>
<td>ISR Forensics Tool</td>
<td>3 Days</td>
<td>The New Systems Training &amp; Integration Office (NSTIO) &amp; the Military Intelligence (MI) School</td>
</tr>
</tbody>
</table>
Sensitive Site
Exploitation Training
What is Sensitive Site Exploitation (SSE)

The systematic search of a secure location that enables the collection of evidence and information that can be used in the prosecution and conviction of military detainees.
Why SSE

• Exploitation of physical evidence from combat scenes has become a warfighting requirement in GWOT in order to help identify, detain and prosecute insurgents/criminals.

• Marines conducting combat missions may come across items of evidentiary value that may be crucial in identifying personnel and/or proving crimes.

• Current pre-deployment SSE/forensics training is ad hoc and is accomplished via a number of different venues without an established program.
  – Standardization and level of training for deployed units is varied/unknown.
SSE Operational Impact – Today

- Aids in identification of insurgents or criminals in on or off-base activities
- Evidence prevents the releasing dangerous insurgents or criminals
- Increased successful prosecutions
- Links insurgent groups and aids in development of targeting packages
SSE Training Plan

– Local unit training:
  • Develop basic understanding of TTPs and concepts.
  • Learn from experience.
  • Familiarization with Training Support Packages.
  • Incorporate SSE training into various aspects of pre-deployment training.
    –Raids
    –Vehicle Searches
    –Checkpoint Screenings
    –DOMEX (Documents/Media)
What has been accomplished

• Funded by TSWG via Training Technology Development Subgroup to develop a Training Support Package (TSP) for SSE being completed by NTPI.

• Gathered input directly from the JPEC IZ, NGIC, the interagency, and OPMG.

• Final product consists of TSP, Trainer materials, video, student materials, field flip cards, and training kit.

• Training materials have been developed and filming has wrapped up on the training video. Currently in editing.

• Identified target audience – Marines preparing to deploy who will be performing an SSE mission.
Next Steps

• Standardized SSE training package for deploying units with an SSE mission - Initial completed, available through GPO, more and updated versions in late 2008

• Incorporate SSE into pre-deployment unit training (PTP).

• Establish distribution of the TSP and Command buy-in.

Way Ahead: TECOM Sanction SSE training as an Irregular Warfare Training Requirement and mandate biometrics-forensics/SSE training in the PTP.
Questions?

POC: Maj William Coffey
USMC Biometrics
William.w.coffey@usmc.mil