Marine Corps Forensic Enterprise Strategy

20 April 2010

This page intentionally left blank

Contents

1.0. Executive Summary

> "… they [the Joint Prosecution and Exploitation Center] bring with them a whole new set of skills that we don't have, that we're able to apply directly to locating and fixing the enemy. That's the hardest part of what we're doing right now—finding them and fixing them. Once we do that they're easy to eliminate because we have overwhelming combat power and we have units that can do that, but finding them and fixing them is the challenge."
>
> Maj Gen Richard Mills, Commander
> Ground Combat Element, Multinational Force–West, Iraq

As the Marine Corps works toward the realization of the Commandant's 2025 Vision and Strategy, we fight upon battlefields that place a growing premium on agility, lethality, and precision. Although world-renowned for the application of violence on the battlefield, Marines in combat today can attest to the need for the discriminate use of carefully targeted force in order to protect our coalition and host-nation partners and defeat the adversaries who strive to dominate them. The reality of our decade-long involvement in Iraq and Afghanistan calls for a more versatile force: a force equally capable of delivering crushing blows to massed enemy targets and capable of supporting unconventional operations in a complex, dynamic, and hybrid threat environment as depicted in Figure 1.[1]

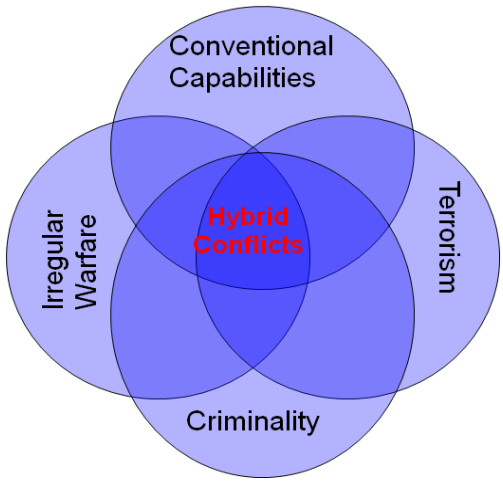

Figure 1. Hybrid threat construct.

The Marine Corps recognized the need for and benefit of adopting identity-based strategies for engaging and defeating our adversaries. An integral part of establishing identity dominance within the battlespace is the application of forensic science functions; this has unquestionably enabled Marines to identify, target, capture, and kill the enemy. The Marine Corps was the first Service to use a crime laboratory forward in pursuit of identity dominance operations. Or, more simply stated, *the Marine Corps was the first Service to fully embrace the application of integrated biometric and forensic operations because it denied the enemy anonymity and freedom of movement within the battlespace.* At present, expeditionary forensics continues to play an integral role in supporting operationally committed Marines as well as other agencies with homeland defense and intelligence missions. Specifically, expeditionary forensics directly contributes to the development of all-source intelligence, targeting, force protection, homeland defense, host-nation rule of law and capacity building, and U.S.

[1] F. G. Hoffman, "The (Re) Emergence of Hybrid Threats," presentation, Marine Corps Warfighting Laboratory, 20 May 2009

personnel recovery in the Afghanistan and Iraq theaters of operation. The use of forensics has proven particularly relevant in combating irregular, catastrophic, and disruptive challenges and their hybrids.

This document discusses how future Marine commanders can accomplish identity dominance goals with the integrated application of forensic functions. However, there is a critical need for the Marine Corps to refine and expand the scope and application of *expeditionary forensic capabilities* while defining its Service-specific requirements to the nascent Defense Forensic Enterprise (DFE) as it evolves into an enduring DoD capability. Relying solely on the evolving DFE-supported expeditionary forensic plan for future support could severely limit the Marine Corps' ability to fully support anticipated combatant command (COCOM) and joint force commander identity dominance requirements. The Marine Corps must take steps to develop and implement a Service-specific expeditionary forensic capability, resident within each Marine expeditionary force (MEF), in order to have on-demand, full-spectrum identity dominance.

The Marine Corps' expeditionary forensic capabilities must complement and integrate with other Service and agency and DFE systems while supporting the Marine Corps' unique role as the Nation's force in readiness and expeditionary force of choice. Specifically, Marine Corps expeditionary forensics must provide responsive support to naval expeditionary forces by development of truly maritime expeditionary forensic facilities, subject matter expertise integrated with forward-deployed forces, quick-response flyaway site exploitation teams, and real-time virtual access to established reach-back facilities.

Marine Corps Forensic Enterprise Strategic Statement

Leveraging joint and organic forensic exploitation capabilities, the Marine Corps will fully integrate identity dominance, and specifically expeditionary forensics, into mission planning. While synchronized with the Defense Forensic Enterprise and the Intelligence Community, Marine Corps expeditionary forensics will specifically support naval interests and will differentiate itself by being ruggedized, agile, and rapidly deployable, scalable, and designed to provide the tactical commander with near real-time forensic exploitation capabilities.

The Marine Corps' employment of a doctrine-based maritime forensic capability, if fully realized, will ensure that *naval power and influence can be applied at and from the sea, across the littorals, and ashore* by denying the enemy anonymity and freedom of movement in the global operating environment. Additionally, an integrated biometric and forensic-based identity dominance system will enable naval forces to develop a greater understanding of threats and perpetrators not yet realized.

1.0. Purpose

This document establishes a broad strategy for Marine Corps forensic capabilities across the full range of military operations. It describes the use of forensics in support of Marine Corps operating concepts and provides a framework for operators, planners, and intelligence professionals to incorporate traditional and emerging DoD forensic enablers and associated biometric applications into their respective processes. Properly articulated and executed, this strategy will guide efforts to resource the organization, drive identity dominance planning in operations, and provide indicators for training and equipping Marines so that they are fully prepared to forensically exploit material found in austere expeditionary environments or afloat. It will also assist leaders by illustrating potential gaps between current capabilities and the desired end state of attaining identity dominance over our adversaries while contributing to the national intelligence enterprise and ultimately homeland defense.

2.0. Introduction and Background

As U.S. Central Command carried out Operation Enduring Freedom in Afghanistan and Operation Iraqi Freedom (OIF) in Iraq, Marines found themselves fighting a largely anonymous enemy that chose to engage by using improvised explosive devices (IEDs). In 2004, the National Ground Intelligence Center (NGIC) pioneered the strategy of using forensic exploitation techniques to identify IED makers and their networks. NGIC incorporated forensic capabilities into the existing Combined Explosives Exploitation Cell (CEXC), which had primarily focused on technical intelligence, chemical analysis, and dissemination of IED protective measures.[2] It also created the first weapons intelligence teams to identify and collect relevant material from IED blast sites.

In December 2004, DoD law enforcement agents, from a variety of agencies, with expertise in processing crime scenes and collecting evidence, deployed to Iraq to provide training for the weapons intelligence teams and, eventually, for other units.[3] This training greatly increased the qualitative and quantitative capacity of U.S. forces to recognize, preserve, and analyze forensic materials in-theater. Often, material collected from the locations consisted of not only intelligence information (computers, documents, plans, maps, etc.) but also material with no intrinsic intelligence value, such as drinking glasses and clothes. These seemingly unimportant articles often contained a treasure trove of information such as fingerprints and biological matter suitable for DNA testing, which provided irrefutable scientific links among people, places, and events.[4] Based on its successes in Iraq, NGIC added a forensic capability to the CEXC in Afghanistan in March 2006.

---

[2] Captain Ryan Campbell, “Training the Force to Identify the Unknown Threat: NGIC’s Battlefield Forensic Training,” *Military Intelligence Professional Bulletin*, vol. 5, number 1, PB34-09-1, January-March 2009

[3] Major Tim O’Neill, David Wikoff, and Craig Coppock, “Forensic Intelligence,” *Military Intelligence Professional Bulletin*, vol. 33, number 4, PB 34-07-4, October-December 2007, pp. 46-47

[4] Campbell, 2009

In August 2006 the Joint Quick Turn Capability Baseline Assessment on DoD Biometrics "Gap 18" identified the requirement for increased capacity to conduct latent print exploitation in the theater of operation. This directly led to a Joint Requirements Oversight Council Memorandum (number 248-06), which validated the Quick Turn Capability Baseline Assessment and recommended that $301 million in funding be applied over fiscal years 2006, 2007, and 2008 to satisfy the identified capability gaps, among which was $34 million for expeditionary forensics. As a result of its pioneering work with the Naval Criminal Investigative Service (NCIS) crime lab supporting Marines in Multinational Force–West (MNF-W), the Biometrics Task Force asked the Department of the Navy to act as the office of primary responsibility for developing and enhancing this capability. The department established the Joint Expeditionary Forensic Facility (JEFF) integrated process team, which was led by Marines from Headquarters Marine Corps, Plans, Policies, and Operations Department, Security Division, Law Enforcement & Corrections Branch. The Technical Direction Agent for the team was supported by the Naval Surface Warfare Center at Dahlgren, Virginia.

Tactical success bred increased demand for in-theater forensic capabilities, and by October 2007, a Multi-National Corps–Iraq Joint Urgent Operational Needs Statement identified the requirement for four JEFFs, each with latent print, firearms, DNA, and document and media exploitation forensic capabilities for the Iraqi theater of operations.[5] Also at this time, the original developmental integrated process team for the JEFF project began transitioning responsibilities to the U.S. Army Criminal Investigation Laboratory (USACIL). In September 2008, the Army Director of Force Management approved a concept plan for 152 additional civilians to support JEFF-related manpower requirements at USACIL.

Today, although somewhat ad-hoc in organization, the JEFFs continue to provide commanders with nearly real-time forensic exploitation capabilities that significantly contribute to all-source intelligence information, force protection, and identity dominance of the battlespace.

2.1. Strategic View

> "First, we have been warning since 9/11 that al-Qa'ida, al-Qa'ida-associated groups, and al-Qa'ida inspired terrorists remain committed to striking the United States and US interests. What is different is that we have names and faces to go with that warning."
>
> —Dennis C. Blair
> Director of National Intelligence[6]

Globalization, hybrid threats, and transnational criminals and terrorists have forever altered the way the United States views threats to the homeland and how to protect it.

[5] JEFF Historical Timeline Briefing, prepared by the JEFF Program, Naval Surface Warfare Center, Dahlgren, VA, 23 Nov 2009

[6] Dennis C. Blair, Senate Select Committee on Intelligence, U.S. Intelligence Community Annual Threat Assessment 2010, 3 Feb 2010, www.dni.gov/testimonies/20100203_testimony.pdf

Consequently, a whole-of-government approach is critical to preventing future attacks in the homeland as well as protecting national interests abroad. The rapid exchange of information between U.S. government agencies and partner nations will play an increasingly important role in preventing such attacks globally. The use of forensic science to accurately identify subjects of interest and provide irrefutable links to criminal and terrorist activities will enable military, law enforcement, and intelligence professionals to develop clear and unambiguous knowledge of threats and perpetrators. Most important, this nascent capability will support tactical, operational, and strategic levels of identity dominance operations.

2.1.1. Department of Defense Forensic Enterprise

> "DoD is transcending traditional uses of forensic science by becoming surge-capable and focused on providing holistic and sustainable service to a multi-use customer, based world-wide."
>
> —Forensics for Commanders 2008

The Quadrennial Defense Review of 2010 acknowledged that preventing the rise of threats to U.S. interests requires the integrated use of diplomacy, development, and defense, along with intelligence, law enforcement, and economic tools of statecraft to help build the capacity of partners to maintain and promote stability. Stability operations, large scale counterinsurgency, and counterterrorism operations are not niche challenges or the responsibility of a single Military Department, but rather require a portfolio of capabilities as well as sufficient capacity from across America's Armed Forces and other departments and agencies.[7] One capabililty that has demonstrated great potential is DoD's maturing application of forensic science. Specifically, the application of various forensic disciplines has enabled commanders and partners to identify, target, track, and prosecute adversaries throughout the world.

Overseas contingency operations have produced emerging needs and capabilities for the application of forensics across the full range of military operations. At present, forensics plays an integral role in supporting all-source intelligence requirements, targeting, force protection, host-nation rule of law and capacity building, and U.S. personnel recovery and further enables our ability to attain identity dominance throughout the battlespace. The use of forensics has proven particularly relevant in combating irregular, catastrophic, and disruptive challenges and their hybrids.

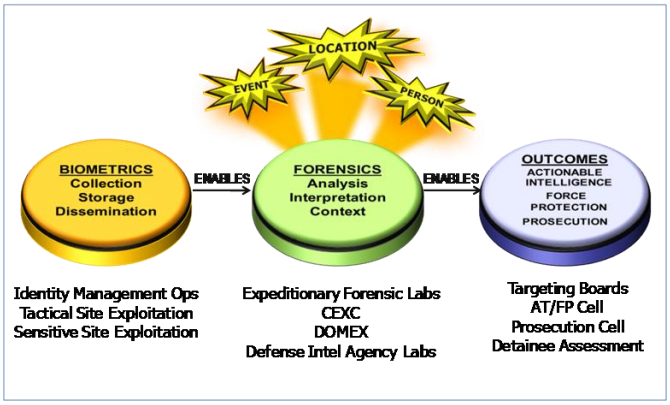

Figure 2. Forensics connects biometrics to outcomes.

The DFE consists of those DoD resources, assets, and processes

[7] Quadrennial Defense Review Report, Department of Defense, February 2010

that provide forensic science analysis linking persons, places, and things to previous events in both traditional and expeditionary environments. The DFE supports numerous customers, including joint force commanders, intelligence analysts, criminal investigators, and medical examiners. Not included in the DFE are those distinct, nontraditional missions requiring unique forensic disciplines that support technical nuclear, technical chemical and biological, and specialized intelligence disciplines.[8]

The Capstone Concept of Operations for DoD Forensics defined and established the forensic functions and operational processes that together provide specific outputs and enablers designed to support a broad range of military operations and operating environments.[9]

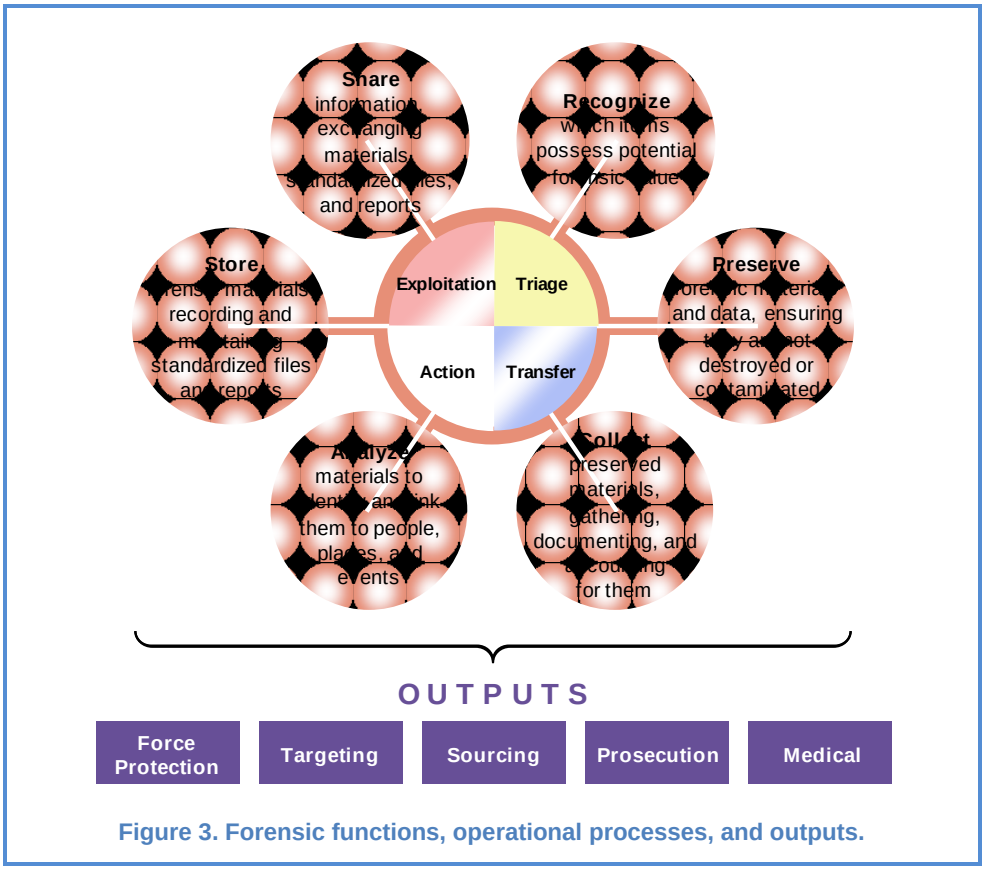

Figure 3. Forensic functions, operational processes, and outputs.

- Force protection: enables counter-IED measures, vetting of host-nation and third-country nationals through established biometric watch lists, and other measures
- Targeting: scientifically links individuals, places, things, activities, intentions, organizations, and events
- Sourcing: scientifically identifies the origin of arms, ammunition, and explosives

[8] Draft DoD Directive 5205.hhE, DoD Forensic Enterprise (DFE), December 2009

[9] Capstone Concept of Operations for Department of Defense Forensics, 8 July 2008

- Prosecution: enables the decision to hold or release; supports the development of prosecution cases to try detainees or suspected criminals in a court of law
- Medical: scientifically identifies remains and determines cause of death

The DFE comprises various facilities, personnel, and equipment from multiple Services, agencies, and organizations that have been deployed, organized, or otherwise connected to provide the joint force commander with forensic capabilities across a broad range of military operations (see figure 4).

Forensic capabilities continue to mature and converge to aid U.S. and coalition force operations by adding depth and scope to the comprehensive operational picture. Capabilities such as latent print and DNA collection, when enabled by a robust biometrics database, enable warfighters to specifically connect the dots by linking a particular person to places or events. The resulting information can provide usable intelligence to target, apprehend and detain, or prosecute criminals, terrorists, and enemy combatants.

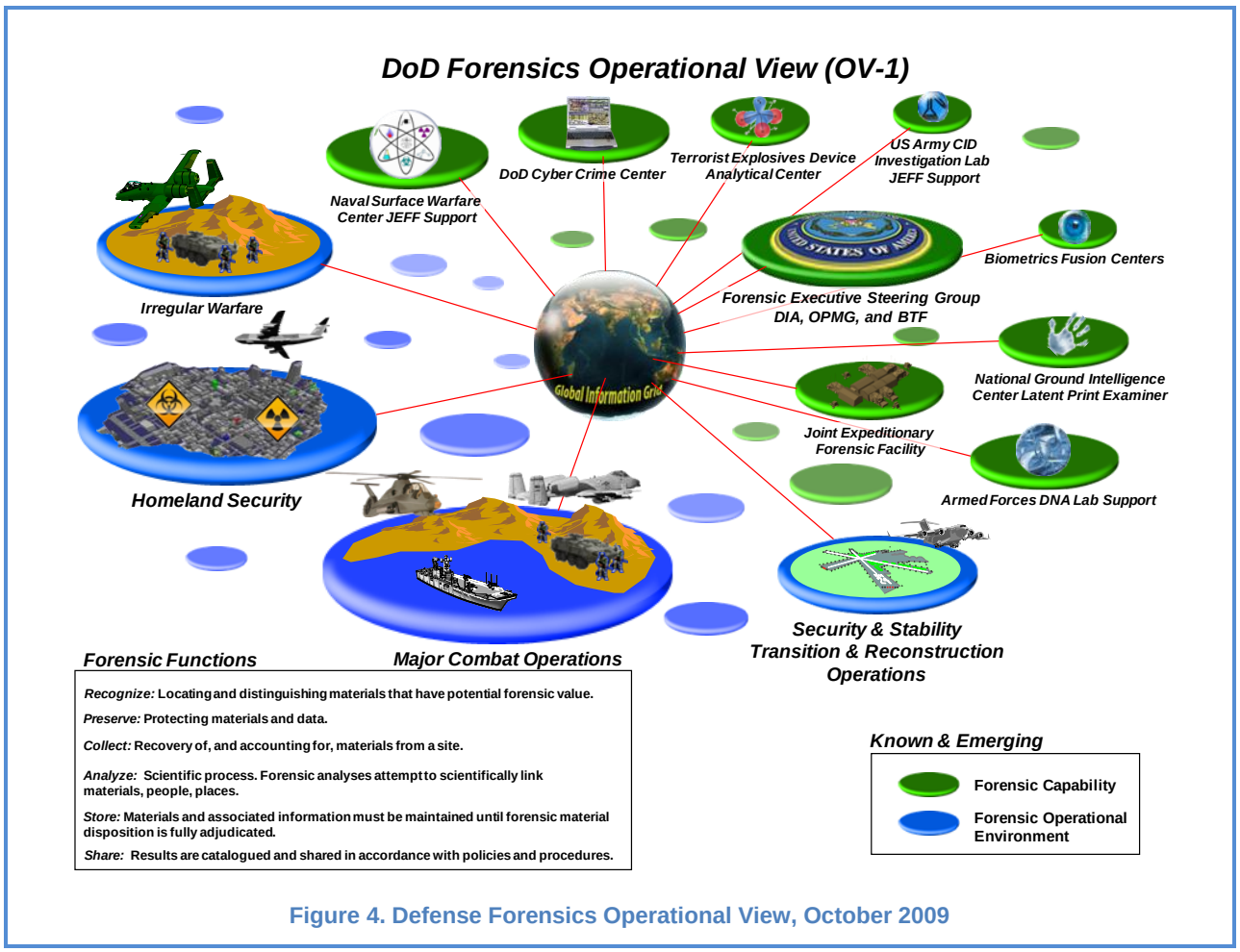

Figure 4. Defense Forensics Operational View, October 2009

2.1.2. Expeditionary Forensics

> "The challenge for the Navy and Marine Corps today is to remain capable of traditional naval missions while simultaneously enhancing our ability to conduct non-traditional missions in order to ensure that naval power and influence can be applied at and from the sea, across the littorals, and ashore, as required."[10]

The Marine Corps Vision and Strategy 2025 further outlines the broad vision for the Corps that will fulfill its duties as the nation's force in readiness in the coming decades.[11] The Marine Corps of the future will be

- Deployed forward with relevant and timely capabilities
- Educated and trained to understand and defeat adversaries in complex conflicts.

One such set of relevant and timely capabilities that will enable Marines to understand and defeat adversaries is the application of biometrics and forensics in order to attain identity dominance in the battlespace. Marines must deploy with a systems approach to identity dominance, leveraging a vast array of integrated biometric and forensic tools and processes. The Marine Corps' employment of a doctrine-based maritime forensic capability, if fully realized, will ensure that *naval power and influence can be applied at and from the sea, across the littorals, and ashore* by denying the enemy anonymity and freedom of movement in the global operating environment. Additionally, an integrated biometric and forensic-based identity dominance system will enable naval forces to develop a greater understanding of threats and perpetrators not yet realized.

2.2. Operating Environment

The Marine Corps Operating Concept for a Changing Security Environment, June 2007, describes how Marine Corps forces will contribute to the nation's defense by providing forces organized, based, trained, and equipped for forward presence, security cooperation, counterterrorism, crisis response, forcible entry, prolonged operations, and counterinsurgency using the enabling concepts of seabasing and distributed operations.[12]

The document also endorses the six-phase joint campaign construct for use in planning. Viewed through this construct, identity dominance, and specifically forensic-related

[10] Naval Operations Concept, 2006, p. 11, https://www.mccdc.usmc.mil/CIW/ER/Naval%20Operations%20Concept.pdf

[11] *Marine Corps Vision and Strategy 2025*, PCN 50100654800, http://www.quantico.usmc.mil/activities/?Section=SVG

[12] *Marine Corps Operating Concepts for a Changing Security Environment*, 2nd edition, June 2007

capabilities, can be a key enabler for many logical lines of operation across the full range of military operations.

DoD Forensic Support across the Joint Operation Six Phase Modeling Construct

Phase 0 Shape the environment	Phase 1 Deter the enemy	Phase 2 Seize the Initiative	Phase 3 Dominate the Enemy	Phase 4 Stabilize the Environment	Phase 5 Enable Civil Authority
Theater Security Engagement Host Nation Training Build Civilian Capacity	Support to Host Nation Identity Dominance Maintain Expeditionary Forensic Capability / Fly-away teams	Force Protection Identity Dominance Targeting	Force Protection Identity Dominance Targeting Detainee Interrogations	Force Protection Detainee Interrogations Transition to Rule of Law	Force Protection Host Nation Training Build civilian capacity

Figure 5. DoD forensic support across the six phases of joint operations.

3.0. The Military Problem

The Marine Corps currently lacks a coordinated and synchronized expeditionary forensic capability to support identity dominance across the full range of military operations. The current Marine Corps expeditionary forensic capabilities were developed along with the other Services, in an ad hoc, incremental approach in response to critical needs that originally emerged during OIF.

The larger DFE continues to evolve toward an enduring capability. In January 2008, the Under Secretary of Defense for Acquisition, Technology, and Logistics established the Defense Forensics Executive Steering Group to coordinate the development and management of defense forensics capabilities and to lead DoD activities to program, integrate, and synchronize forensic strategic plans, programs, policies, and capabilities and the associated combat support capability that will train, equip, deploy, and conduct forensics operations for an operational commander.[13]

While the maturation of the DFE provides significant structure and benefit to the overall application of warfighter forensics, it also poses unique challenges for Marine Corps expeditionary forensics. Marine Corps leadership must weigh the cost vs. benefit of relying solely on external, forensic capabilities provided by the DFE against the need to provide tactical Marine commanders with some level of internal forensic capability that supports broader identity dominance operations.

There is a critical need for the Marine Corps to refine and expand the scope and application of *expeditionary forensic capabilities* while defining its Service-specific requirements to the DFE as it evolves into an enduring, integral DoD capability.

[13] Under Secretary of Defense, Acquisition, Technology, and Logistics Memorandum, Defense Forensic Executive Steering Group, 14 Jan 2008

4.0. Marine Corps Forensic Enterprise Strategic Statement

Leveraging joint and organic forensic exploitation capabilities, the Marine Corps will fully integrate identity dominance, and specifically expeditionary forensics, into mission planning. While synchronized with the DFE and the Intelligence Community, Marine Corps expeditionary forensics will specifically support naval interests and will differentiate itself by being ruggedized, agile and rapidly deployable, scalable, and designed to provide the tactical commander with nearly real-time forensic exploitation capabilities.

5.0. The Marine Corps Forensics Enterprise

5.1. The "As Is" Marine Corps Forensics Enterprise

Current forensic capabilities within the Marine Corps are a collection of ad hoc training venues and task-organized units with limited doctrinal basis of sustainment. The application of forensic techniques in support of Marine Corps operations was developed in response to operational requirements identified during OIF. Forensic requirements and capabilities evolved over several years as leaders sought and applied additional forensic and multidiscipline personnel, resources, and training to the rapidly evolving and dynamic environment in the MNF-W Iraq area of operations.

A pioneer in this nascent field, the Marine Corps was the first Service to use a crime laboratory forward in pursuit of identity dominance operations. Or, more simply stated, the Marine Corps was the first Service to fully embrace the application of integrated biometric and forensic operations because it denied the enemy anonymity and freedom of movement within the battlespace. The lab was known as the "NCIS Crime Lab," and MNF-W quickly realized the benefit of using forward-deployed latent print examiners and crime scene collection techniques to establish the who, what, where, when, why, and sometimes how in the MNF-W area of operations. Leveraging this successful pilot effort, MNF-W established the Joint Prosecution and Exploitation Center (JPEC). In broad terms, this task-organized unit, under the cognizance of the MNF-W Assistant Chief of Staff/G-2, serves as an excellent example of the as-is capability that can be available to Marine commanders (see Appendix C for a more complete description of the JPEC task organization). Although closed during the Iraq transition, the JPEC was as a groundbreaking unit that provided commanders with an ability to scientifically link people, things, and places through the application of forensics and associated analyses.

The JPEC was created to coordinate and synchronize detainee intelligence and criminal prosecution efforts, but it evolved with the changing atmospherics to provide enhanced all-source intelligence information to support targeting, rule of law, and transition

operations.[14] It employed a multifaceted approach, bringing elements of law enforcement, detainee operations, and the Intelligence Community together under one roof. In its later stages, key functional areas of the JPEC included a prosecution cell, a forensic exploitation cell, a tactical site exploitation and training cell, and the ability to provide all-source intelligence and targeting support in a fluid and dynamic environment.

The JPEC was a multidiscipline organization with key elements from the USMC intelligence, Military Police, and Criminal Investigation Division (CID) communities; NCIS; USN; USAF; contracted law enforcement professionals; and linguistic and forensic specialists.

5.2. The "To Be" DoD Forensics Enterprise

> The application of a broad spectrum of science to answer questions of interest and establish factual information based on forensic material that can be used by the combatant commander. Rapid forensic exploitation will give the commander a means of gaining battlefield advantage by providing actionable intelligence to support targeting and legal prosecution.
>
> Working definition of joint forensics

A key enabler to operational success now and in the future is our ability to attain identity dominance when and where we choose to do so. Inherent in our quest for identity dominance is the application of expeditionary forensics. Forensic expertise will remain inexorably resident in various services, agencies, and communities of interest that must be leveraged, aggregated, and fused with other enablers such as biometrics, intelligence, and communication systems.

Within the Department of the Army (DA), forensics is now a program of record established under the Criminal Investigation Command's USACIL, located at Fort Gillem, Georgia. USACIL provides forensic laboratory services to DoD and other federal investigative agencies and operates a school to train forensic laboratory examiners.

The immediate intent of the program is to fully integrate forensic capabilities with intelligence and counter-IED

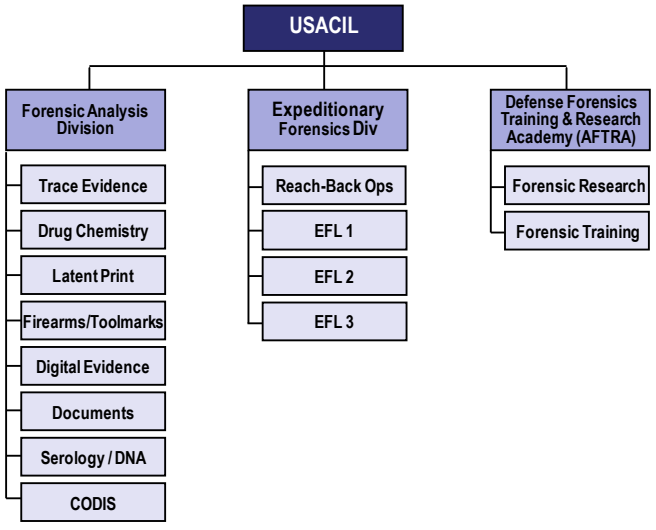

Figure 6. USACIL organization chart.

[14] Marine Corps Center for Lessons Learned Report, "Drawdown, Retrograde and Redeployment of Operation Iraqi Freedom Forces: Command Element Synchronization," 26 Jan 2010

functions and to overlay various existing and emerging capabilities to establish a cohesive approach to forensic analysis in theater.

Under the Expeditionary Forensics Division, USACIL plans to build three deployable labs and a Reach Back Operations Center located at Fort Gillem, Georgia, to provide full-spectrum forensic operational support to COCOM and joint operations anywhere in the world. As capacity builds, USACIL will take over responsibility for the currently deployed JEFF labs in the Afghanistan theater of operations.

Expeditionary forensic lab modules

As envisioned, the USACIL Expeditionary Forensic Labs will be deployable within 96 hours of tasking, operational within 48 hours of arrival in theater, and self-sustaining for 30 days with limited support. The three labs will rotate on a deployed, recovering, and ready-to-deploy operational cycle. Each lab will be staffed with up to 40 DA civilians of various forensic specialties (see figure 7). The labs will also be modular and scalable, capable of deploying as a single full-service (24/7) lab, three 12/7 labs, or four "mini" labs with limited functional capabilities.

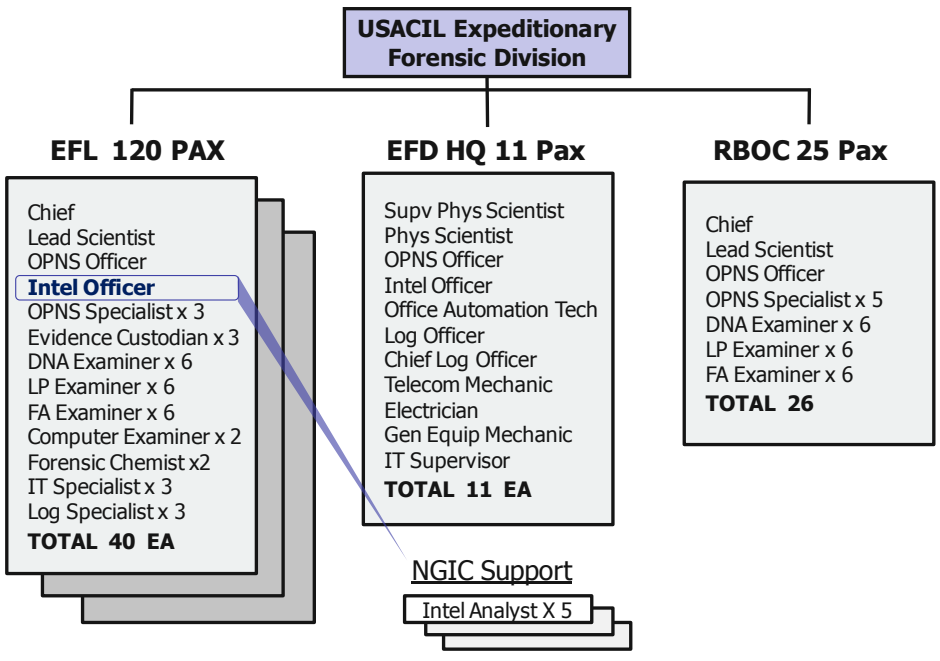

Figure 7. Expeditionary Forensic Laboratory manning.

5.3. The "To Be" Marine Corps Forensic Enterprise

The Marine Corps' expeditionary forensic capabilities must complement and integrate with other agency and DA forensic systems while supporting the Marine Corps' unique role as the Nation's force in readiness and its expeditionary force of choice. Specifically, Marine Corps expeditionary forensics must provide responsive support to naval expeditionary forces by development of truly maritime expeditionary forensic facilities, subject matter expertise integrated with forward-deployed forces, quick-response flyaway tactical site exploitation teams, and real-time virtual access to established reach-back facilities.

While the DA expeditionary forensic plan is substantial and will significantly enhance the overall DFE, it is inadequate for meeting current and emerging Marine air-ground task force (MAGTF) identity dominance operational requirements. One clear example of this is the current staffing and pending approval of an Urgent Universal Needs Statement (UNNS) outlining requirements for forensic capabilities in support of the Marine Expeditionary Brigade–Afghanistan. It is unknown how this particular UUNS will be adjudicated; however, it clearly indicates that some level of forensic support in direct and habitual relationship with Marine forces is required yet not currently available. Relying solely on the DA expeditionary forensic plan for future support could severely limit the Marine Corps' ability to fully support anticipated COCOM and joint force commander identity dominance requirements of the future. The Marine Corps must take steps to develop and implement a Service-specific expeditionary forensic capability, resident within each MEF, in order to have an on-demand and full-spectrum identity dominance capacity. Failure to do so risks the MAGTF's ability to attain deny the Enemy Anonymity, restrict freedom of movement in the battlespace and ultimately could prevent our ability to meet the challenges presented by the hybrid threat of future operating environments. In the interim and until the Marine Corps can establish an organic expeditionary forensic capability, and at the very least, Marine operating forces must play an active role in planning and articulating identity dominance (forensic) support requirements to the joint force commander. Again, failure to consider identity operations as an integral part of the planning process may result in Marine equities not being fully resourced and ultimately negatively impact the MAGTF's ability to establish identity dominance within an assigned area of operations.

The Marine Corps must concentrate its efforts on those unique requirements demanded by the maritime domain's operating concepts of distributed operations and sea basing, along with the traditional Marine Corps strength of flexibility and task-organizing to support new and evolving requirements. The Marine Corps should also concentrate on synchronizing the forensic and biometric capabilities that directly support identity dominance of the battlespace. The key distinction between conducting forensic analysis via a reach-back capability in the continental United States and in an expeditionary environment is the delivery of timely and actionable information to forward-deployed units. A relatively successful platform, the JEFFs have demonstrated the ability to provide Marine commanders with the timely processing, analyses, and exploitation of battlefield material in their area of operations.

As previously discussed, JPEC can provide a model for the task-organized future employment of Marine Corps expeditionary forensics. The JPEC successfully linked the various providers of forensic capabilities with the primary user, the Intelligence Community. This "fusion center" approach proved flexible enough to support the transitions across operational phases, from primarily kinetic targeting through the transition to the rule of law, without requiring major reorganization. Although, the JPEC provided a primarily land-based solution to forensic requirements in the Iraqi theater of operations, the to-be Marine Exploitation Cell (MEC), as conceptually introduced here, can provide the MEF with a land and sea platform with scalable, tailorable, and responsive forensic exploitation and analysis capabilities for the tactical commander.

5.4. Conceptual model of the Marine Exploitation Cell.

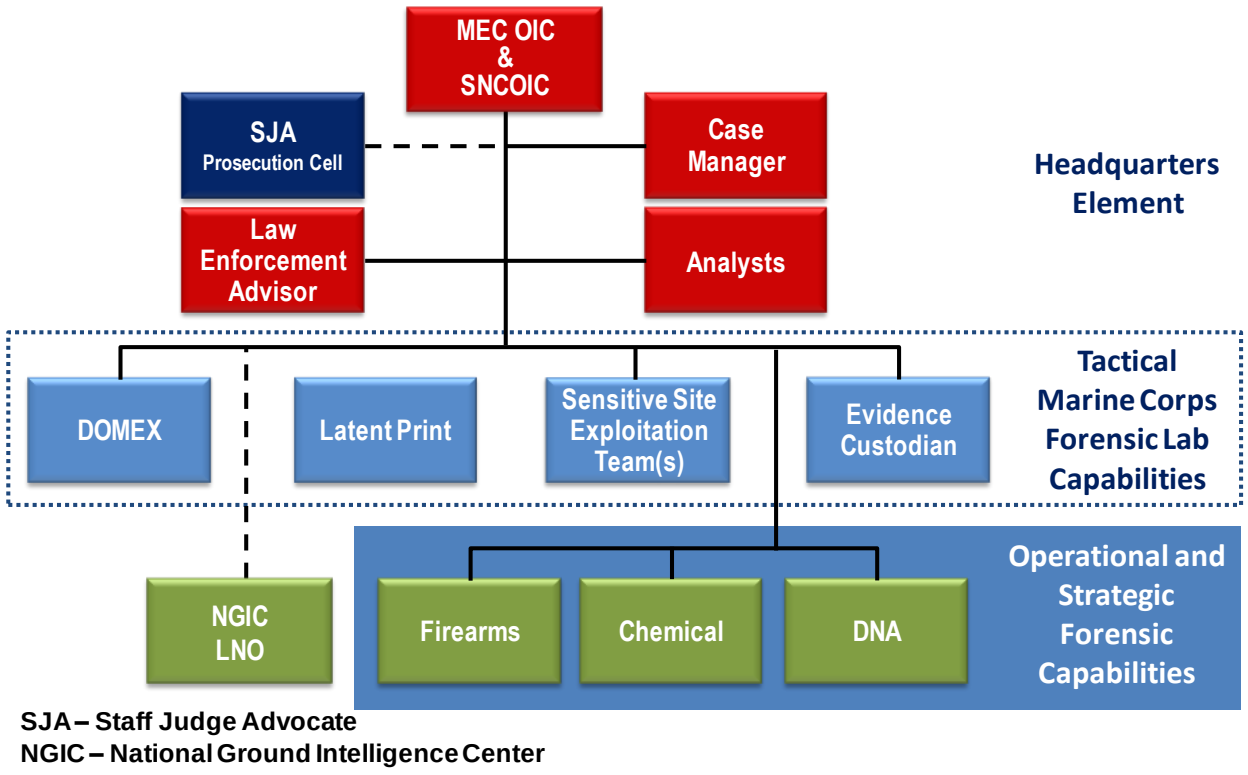

Figure 8. Task organization of the proposed Marine Exploitation Cell.

The MEC concept provides a range of capabilities to inject information to support both intelligence and operational requirements from the MEF level down to the company level intelligence cell if applicable. The MEC concept integrates civilian and military expertise for tactical site exploitation, interrogation support, targeting, and prosecution in military or civilian courts.

Task-organized under the direction of the MEF G-3, the MEC comprises four elements:

The **headquarters element** provides primary forensic capability in support of the MAGTF.

- It is primarily staffed with law enforcement and intelligence personnel organic to the MEF.
- The officer in charge and senior staff noncommissioned officer provide leadership and oversight of the MEC to promote information sharing and synchronization of forensic capabilities to support the commander's requirements. Because the forensic functions of the MEC are inherently law enforcement functions, it is recommended that the MEC officer in charge be a senior Military Police officer (military occupational specialty 5803). Additionally, because synchronization with MEF G-2 is critical for success, it is recommended that the senior staff noncommissioned officer be sourced from the 02XX community.
- If applicable, the contracted law enforcement advisor provides tactical site exploitation expertise and/or additional criminal enterprise analysis support.
- Generally staffed with 02XX or contracted support personnel, the analysis cell creates multidisciplinary products to support customers.
- Generally a senior criminal investigator, the case manager oversees criminal enterprise analysis and site exploitation functions. The case manager also serves as a forensic liaison with other forensic units.

The **Tactical Marine Corps Forensic Lab** provides rapid (24 hours or less) forensic analysis and exploitation and is the principal source of *actionable* information at the tactical level.

- In general terms, the majority of personnel required to staff and sustain this capability can be drawn from the existing Marine Corps Military Police and CID structure resident in the MEF. Military Police and CID personnel are fully capable of providing evidence custodial support as well as sensitive site exploitation train-the-trainer and flyaway crime scene investigative services in support of tactical units and/or host-nation forces.
- Serious consideration should be given to leveraging the NCIS for lab manager support. Specifically, NCIS currently employs over 50 personnel with master's degree level of forensic training, yet these professionals are not employed in any specific expeditionary forensic support role.
- Document and media exploitation and latent print forensic capabilities would likely be contracted out or coordinated via the DA expeditionary forensic facilities. Such exploitation could also likely be conducted by leveraging existing radio battalion capabilities.

Operational and strategic forensic capability supports operational and strategic intelligence requirements and those with longer processing timeframes. *It normally provides contextual vice actionable information.*

- It is provided by USACIL Expeditionary Forensic Laboratories and other DFE partners.
- Forensic disciplines include weapons source origin, firearm and toolmark, chemical, and DNA analysis.
- An NGIC liaison officer provides a link to theater and national databases.

The **prosecution cell** conducts criminal investigations and builds prosecution packages.

- Generally, this section can be staffed with a staff judge advocate, Marine Corps CID, and, if available, NCIS agents as required.
- It prepares prosecution packages suitable for trial in U.S. courts, for host-nation rule of law, and/or to internationally accepted standards.
- It assists host-nation law enforcement and the judiciary by building trust and mutual understanding of roles and responsibilities.

6.0. Challenges

6.1. Regulatory/Policy

Implementing a Marine Corps forensic capability as envisioned in this strategy will present additional challenges in the areas of intelligence oversight, appropriate classification of forensic and biometric information, accreditation requirements for forensic processes, and addressing the balance between the desire to provide identity dominance capabilities to foreign nations and protecting our methods, tactics, techniques, and procedures from red exploitation.

The Marine Corps intelligence community is keenly aware of the challenges involved with accessing and sharing intelligence across intelligence domains, let alone across and with law enforcement domains. Intelligence community stakeholders interviewed stated that overclassification of forensic analysis limited their ability to share actionable intelligence with host-nation, coalition, and even tactical elements during OIF.

Host-nation restrictions on collection of, access to, and use of biometric and forensic data may severely limit the effectiveness of forensics to provide actionable outputs for military operations. Conversely, U.S. restrictions on information sharing or technologies with host nations may limit the effectiveness of forensics in theater security engagement strategies. Furthermore, international and host-nation regulations and policies that limit the time detainees may be held without cause dictates the requirement for increasingly responsive, timely, and accurate forensic analytical capabilities. Excluding forcible-entry environments, MAGTF planners, through appropriate channels, must advocate favorable conditions for the employment of identity dominance tools with host nations.

6.2. Operations

> *We had the MNF-W ORSA study the latency of processing fingerprints from IED components at CEXC as compared to what we could do here at the JPEC. On average, it took the CEXC 64 days to provide information back to us while it took the JPEC under 24 hours.*
>
> *—Former MNF-W JPEC Director*

The Marine Corps' unique role as the Nation's force in readiness highlights the need for a truly expeditionary forensic capability that is agile, scalable, and highly responsive to the needs of tactical commanders for both sea-based operations (visit, board, search, and seizure) and sustained operations ashore.

Based on the lessons learned during OIF and Operation Enduring Freedom, the original concept of expeditionary lab capabilities lagged identified requirements by several months and morphed into larger, more robust fixed facilities rather than the more responsive mobile ones in line with (original) Marine Corps operating concepts.[15] Although not necessarily the vision of the DFE for the future, this demonstrated tendency towards larger fixed facilities and centralized control of forensic applications in theater is counter to the MAGTF principles of providing rapid, self-sustained, and immediate support to the tactical commander. As previously identified, it also demonstrates the need for the Marine Corps to develop and clearly articulate its requirements through both the COCOM Joint Urgent Operational Needs Statement process used to request forensic capabilities in theater and through the Urgent Universal Needs Statement process used to request Service-specific capabilities.

6.3. Information Management

Current tactical communications infrastructures challenge rapid information exchange between forward forces and analytic nodes. Although systems are constantly being improved, there remain severe challenges in communicating information quickly enough to support identity dominance requirements and provide actionable intelligence.

Currently there is no central repository for forensics and biometrics information accessible by both law enforcement and intelligence personnel. The established databases do not talk to each other, and the information system architecture is based on a "pull" concept versus a "push" to appropriate personnel. This results in law enforcement and intelligence personnel spending a large portion of their time searching through a multitude of databases to find relevant information. Further exacerbating the problem is the lack of protocols for sharing biometric and forensic information with the host nation.

Consequently, this is why there is a premium placed on an organization's ability to deftly manage, search, and input and extract data from multiple sources. The conceptual MEC serves this connect-the-dots function with respect to biometrics and forensics and provides a critical linkage between disparate databases and systems.

[15] Interview with JEFF Program Manager, Dahlgren, VA, 23 Nov 2009

6.4. Force Management

The employment of an enduring forensically supported identity dominance capability will challenge existing the Marine Corps' organizational employment constructs and force structure. Although the envisioned Marine Corps forensic enterprise comprises occupational specialties and functional capabilities from many highly specialized disciplines, the preponderance of the required skill sets necessary for an MEC reside within the Military Police and intelligence communities. Because stakeholders overwhelmingly indicated that "this is a G-3 function," HQMC, Plans, Policies & Operations Department, Security Division, Security Branch, is the recommended office of primary responsibility to lead the advocacy for enhanced MAGTF identity operations and to integrate these capabilities into an overarching identity dominance framework. Operational units must identify and provide additional training to key high-demand, low-density military occupational specialties in order to perform critical identity dominance and forensic tasks that rest at the nexus of intelligence, law enforcement, biometrics, and forensics. Key high-demand, low-density occupational specialties that should consider additional training and skill identifiers to enable the broader application of identity dominance and forensic tasks include the Military Police, CID, and intelligence communities. Additionally, leaders must consider identity dominance an integral part of operational planning, thus ensuring the proper employment of these skilled personnel throughout all phases of operations.

Increasingly, battlefield forensics plays an integral role in not just military operations but homeland security as well. As the Marine Corps develops and refines its own forensically supported identity dominance capability, consideration must be given to establishing a permanent subject matter expert structure necessary to develop and sustain Marine Corps expeditionary forensic operations afloat or ashore. Significant operational enhancements can be attained with select and modest increases in forensic subject matter expert structure at MEF, Marine Corps forces, and headquarters levels.

7.0. DOTMLPF Implications

7.1. Doctrine

The Marine Corps should incorporate forensics concepts and related capabilities into applicable doctrine—that is, counterinsurgency, humanitarian assistance, and irregular warfare publications. In particular, Marine Corps Warfighting Publication 3-33.5, *Counterinsurgency*, should be updated with

- One or more forensic vignettes to reinforce the success of forensic functions in OIF
- The addition of forensics and collection of biometrics to discussions on logical lines of operation, intelligence, and population control
- The addition of forensic and related capabilities to Appendix A, *A Guide for Action*, or as a standalone annex

In addition, it is recommended that forensic *training, tactics, and procedures* be incorporated into applicable Marine Corps Reference Publications or Marine Corps Interim Publications, such as the proposed *Combat Policing.*

7.2. Organization

The employment of the JPEC model in OIF established forensics and criminal investigative techniques as a model to support future Marine counterinsurgency operations; however, the structure, organization, and sourcing of the enduring capabilities are not self-evident. When asked who should own forensics, stakeholders agreed that although the intelligence community has a great interest in the products and outcomes of forensic activities, the Military Police community already has many of the requisite skills and is the logical choice as the office of primary responsibility for executing forensically enhanced identity operations. Further, this community has a vested interest in using forensics in both its operating force and supporting establishment missions. Forensics is also traditionally viewed as a law enforcement function with relatively recent adaptations that support the broader Marine Corps intelligence enterprise. Finally, the Military Police are also highly skilled in evidence preservation and chain-of-custody procedures that enable forensic processing in support of rule of law and prosecutorial efforts.

Several ongoing initiatives provide opportunities to leverage and synchronize mutually supporting and associated efforts. The law enforcement advisors program and the recent transition of significant Military Police and CID structure to the MEFs provide operating forces with additional resources that have many of the requisite skill sets to establish and maintain a baseline expeditionary forensic capability. Additionally, the Company Level Intel Cell and Combat Hunter initiatives may also be leveraged to ensure that intelligence derived through the MEC both supports and is supported by tactical units.

7.3. Training

The Marine Corps requires a comprehensive review of training courses required to support identity operations and the forensic enterprise. Other than the traditional criminal and medical communities' institutional forensic requirements, training is developed and delivered ad hoc with limited awareness at the operating force level. Currently, the only formal requirement for training Marine Corps personnel in expeditionary forensic functions derives from the CENTCOM Commander's training requirements for all forces deploying in support of Operations Iraqi and Enduring Freedom to counter the IED threat.[16]

The Marine Corps should develop a three-tiered training strategy for forensics, consisting of tactical site exploitation courses for operating forces, advanced sensitive site exploitation training for the Military Police (and CID) and intelligence communities, and specialized training for forensic lab personnel and supervisors. This training

[16] CENTCOM Commander's Memorandum, *Counter-IED Training and Capability Guidance*, 20 Mar 2008

program must have strong advocacy, primarily through the Military Police community, to propagate across the military occupational specialty spectrum, create Marine subject matter expert instructors, and track trained personnel to sustain the program.

Operating forces require a train-the-trainer program to maintain baseline capabilities in tactical site exploitation techniques and the use of collection tools in tactical units to enable the forensic enterprise. Stakeholders expressed the need for a training program that focuses on all phases of the joint planning model, not just the kinetic phases. A training program for forensics and related identity dominance operations that is exportable to friendly nations may provide them with evidence collection, forensic analysis, and identity management capabilities sufficient to defeat insurgency before U.S. involvement is required.

Finally, operational planners and leaders at all levels must be given identity operations training that stresses a systems methodology for addressing critical enablers, tasks, and outcomes of attaining or failing to attain identity dominance in the battlespace. Generally, and as stated previously, this revolves around the nexus of intelligence, law enforcement, biometric, and forensic operations.

During the most recent official Training and Readiness Manual review, the Military Police community specifically incorporated “expeditionary forensic operations” into its Training and Readiness Manual. It is expected that the Military Police community will work in concert with Training and Education Command to develop an effective course curriculum for formal training.

7.4. Material

Joint Expeditionary Lab

Establishing organic Marine Corps forensic capabilities that support the tactical commander requires agile, ruggedized, and scalable expeditionary forensic laboratory facilities that are compatible and fully integrated with joint, other Service, and interagency laboratories, yet also tailored to the unique operating requirements of the maritime domain. The JEFF originally designed and deployed to Iraq provides a good starting point and successful model for scalable and deployable labs. Additional considerations for maritime applications include the ability to support Marine expeditionary units and ruggedized construction similar to that used by Naval Air Systems Command for deployment of sensitive avionics equipment, as forensic testing and analysis equipment requires similar packaging, handling, and overall safeguards. Stakeholders in the operating forces repeatedly stressed that quick response times to inquiries are their paramount concern, and they suggested a scalable forensic lab with forensic disciplines (capabilities) sequenced according to how quickly the discipline can become operational

as well as how quickly the discipline can return actionable information.[17] For this reason, a Marine Corps material solution that includes latent print examination and document and media exploitation capabilities for each MEF (refer to figure 8, the conceptual MEC diagram) is most desirable. Other forensic disciplines that require longer processing time are not particularly well suited for MAGTF operations and can be provided through the DFE and/or other reach-back support.

Additionally, a centralized, standardized, universal database that is accessible, searchable, and sharable across all stakeholders must be considered. Information system capabilities must be compatible with, or integrated into, the Distributed Common Ground System–Marine Corps to ensure that forensic analysis outcomes are available to all echelons.

7.5. Leadership and Education

Commanders at all levels must recognize the application of forensics and associated activities as a mission enabler across the full range of military operations and as a *fundamental* mission enabler for hybrid threat and counterinsurgency operations. Leader education should include the concepts of identity dominance lines of operation enabled by forensics and biometrics. MAGTF staffs must be familiar with the timelines, priorities, and requirements associated with the exploitation process at the tactical, operational, and strategic levels in order to help commanders set favorable conditions.

As defined by the weapons technical intelligence community, the level of exploitation and analysis required is based on time, place, and supported customer—not value.[18] Tactical exploitation occurs nearest to the time and place of the event. Actions at this level involve local military or law enforcement forces and provide immediate impact in the area of operations. At the operational level, exploitation activities are in direct support of local and in-country forces, but they may occur outside the immediate area of operations. Strategic-level exploitation may occur anywhere in the world and focuses on long-term effects and intelligence requirements.

Commanders must require that staffs answer critical questions of the level of exploitation required at each level, the outputs and products required for each customer, and the necessary authorities and resources to achieve these outcomes. As stated previously, the Military Police community is the logical staff element for primary responsibility to prepare this staff estimate.

7.6. Personnel

Personnel requirements for establishing expeditionary forensics must be identified and analyzed against the existing force structure to determine the proper mix of military,

[17] Interview with I Marine Expeditionary Force HQ forensic enterprise stakeholders, Camp Pendleton, CA, 15 Dec 2009.

[18] Weapons Technical Intelligence Handbook, Version 1.0, Defense Intelligence Agency, p. 191, September 2009

civilian, and contracted personnel, as well as their number, skill sets, and owning organizations.

At present, Military Police and CID personnel at the MEF can provide the core of a train-the-trainer forensically supported identity dominance baseline, providing support and subject matter expertise to deployed and deploying forces. Additionally, the NCIS has, on staff, approximately 50 personnel with training and certification in forensic disciplines at the master's degree level. Consideration should be given to developing a sustained agreement for NCIS to support the MEFs with forensic experts who provide additional reach-back and augmentation for a task-organized unit (MEC) during extended operations.

7.7. Facilities

To build an enduring expeditionary forensic capability, training and education facilities that are accessible and responsive to the needs of both maritime and land-oriented identity dominance operations must be available. Currently Marines receive enhanced pre-deployment biometric training via the MAGTF Integrated System Training Centers. While this innovative approach is effective for immediate needs, consideration must be given to development of or utilization of additional facilities that can provide comprehensive forensic and biometric training in support of broader identity operations. As the DFE continues to mature, the Marine Corps may be able to leverage the existing facilities of other organizations, such as USACIL, to train specialized low-density, high-demand MAGTF forensic personnel. Current training facilities initially sponsored by the Joint IED Defeat Organization to develop and maintain the required level of proficiency in sensitive site exploitation and tactical site exploitation appear adequate.

Appendix A. References

1. Capstone Concept of Operations for Department of Defense Forensics, 8 July 2008
2. Captain Ryan Campbell, "Training the Force to Identify the Unknown Threat: NGIC's Battlefield Forensic Training," *Military Intelligence Professional Bulletin*, vol. 35, number 1, PB34-09-1, January-March 2009
3. CENTCOM Commander's Memorandum, *Counter-IED Training and Capability Guidance*, 20 Mar 2008
4. Concept of Operations for Police Intelligence Operations, 4 March 2009
5. Director of Defense Research and Engineering Memorandum, Forensics Executive Steering Group Charter, Apr 8, 2008
6. DoD Identity Management Strategic Plan, April 2009
7. Erik Berg, "CEXC Biometrics: Identifying the Bombmaker Networks," *Military Intelligence Professional Bulletin*, vol. 35, number 1, PB34-09-1, January-March 2009
8. John D. Woodward Jr., "Using Biometrics to Achieve Identity Dominance in the Global War on Terrorism," *Military Review*, September-October 2005, pp. 30-34
9. Keith Warman, *Identity Dominance: A Way to Map the Population and Deny the Enemy Anonymity*, Center for Army Lessons Learned
10. Major Tim O'Neill, David Wikoff, and Craig Coppock, "Forensic Intelligence," *Military Intelligence Professional Bulletin*, vol. 33, number 4, PB 34-07-4 October-December 2007, pp. 46-47
11. Marine Corps Center for Lessons Learned Report, *Drawdown, Retrograde and Redeployment of Operation Iraqi Freedom Forces: Command Element Synchronization*, 26 Jan 2010
12. Marine Corps Center for Lessons Learned Report, *Joint Prosecution and Exploitation Center (JPEC) Operations and Use of Forensics in Iraq* (revision 1), 4 February 2009
13. Marine Corps Doctrinal Publication 1-0, *Marine Corps Operations*, September 2001
14. Marine Corps Doctrinal Publication 1-2, *Campaigning*, August 1997
15. Marine Corps Doctrinal Publication 2, *Intelligence*, June 1997
16. Marine Corps Operating Concepts for a Changing Security Environment, 2nd edition, June 2007
17. *Marine Corps Vision and Strategy 2025*, PCN 50100654800, available at http://www.quantico.usmc.mil/activities/?Section=SVG
18. Marine Corps Warfighting Publication 2-1, *Intelligence Operations*, September 2003.
19. Marine Corps Warfighting Publication 2-3, *MAGTF Intelligence Production and Analysis*, September 2001
20. Quadrennial Defense Review Report, Department of Defense, February 2009
21. Robert M. Gates, "A Balanced Strategy—Reprogramming the Pentagon for a New Age," *Foreign Affairs*, January/February 2009
22. *Weapons Technical Intelligence Handbook*, Version 1.0, Defense Intelligence Agency, September 2009

Appendix B. DoD Forensic Functions and Operational Process

The Capstone Concept of Operations for DoD Forensics, published in July 2008, establishes the six forensic functions—*recognize*, *preserve*, *collect*, *analyze*, *store*, and *share*—and four activities that make up the operational processes: *triage*, *transfer*, *exploitation*, and *action.*

DoD Forensic Functions

Figure 9. DoD forensic functions.

Recognize: This involves locating and distinguishing materials that have potential forensic value. It may entail special methods and advanced training to detect items.

Preserve: This involves protecting materials and data from the moment those items are recognized as holding potential forensic value. Materials must be protected and preserved by available, reasonable measures (marking, packaging, and tracking) to prevent contamination, loss, or alteration.

Collect: This describes recovery of and accounting for materials from a site. The site is documented and contextual information is recorded, within the parameters allowed by the situation. This often includes limited processing of specific items or areas in an effort to detect additional forensically relevant information. Presumptive testing of materials may also be involved.

Analyze: Forensic analysis may occur beginning with the recognition of materials and contextual information at the site through in-depth examination at mobile or institutional labs. Presumptive testing of materials may be involved. A variety of factors (the submitting unit's request, expected use of the results, time priorities, available lab resources, etc.) dictate the type of analyses and examinations that a lab will perform.

Store: Materials and associated information must be maintained until an issue is fully adjudicated or resolved. Policies and procedures should dictate proper disposition. Balancing information assurance with necessary retrieval capabilities is critical when storing data.

Share: Once forensic analyses are completed, results are catalogued and shared in accordance with policies and procedures. Interoperability is key to developing databases and retrieving information. Sharing information with the relevant stakeholders, including the submitting unit, is vital.

DoD Forensics Operational Process

Four activities—*triage*, *transfer*, *exploitation*, and *action*—make up the operational process used to enable forensic capabilities:

Triage: Forensic materials may be prioritized or *triaged* multiple times during the operational process. This begins at the site by deciding which materials might hold forensic and/or exploitation value. Triage continues each time an individual handles, transports, or examines the materials. The appropriate facility for scientific analysis must be identified—and whether the materials can indeed be analyzed. Triage also involves prioritizing which lab section(s) should receive which materials, as well as how long the materials should be stored. Even the reporting and sharing of information is prioritized.

Transfer: Transfer consists of physically transporting materials or transmitting digital information. Once collected, forensic materials and information are usually transferred to an appropriate location that allows for a more complete scientific analysis.

Exploitation: Exploitation is taking full advantage of any information for tactical, operational, or strategic purposes. After the information, personnel, and materials collected are forensically analyzed, the resulting information is fed into the intelligence cycle—in a word, *exploited*—to produce an advantage for follow-on actions. Exploitation uses the results of forensic analysis as an enabler in military operations to produce an action.

Action: Exploiting the results of forensic analysis may lead to actions such as additional intelligence taskings, battlefield targeting, apprehension and prosecution of suspects, or helping medical personnel resolve their issues. Once the appropriate action has been taken to exploit the results of the scientific analyses, the operational process has been completed.

Appendix C. The Joint Prosecution and Exploitation Center

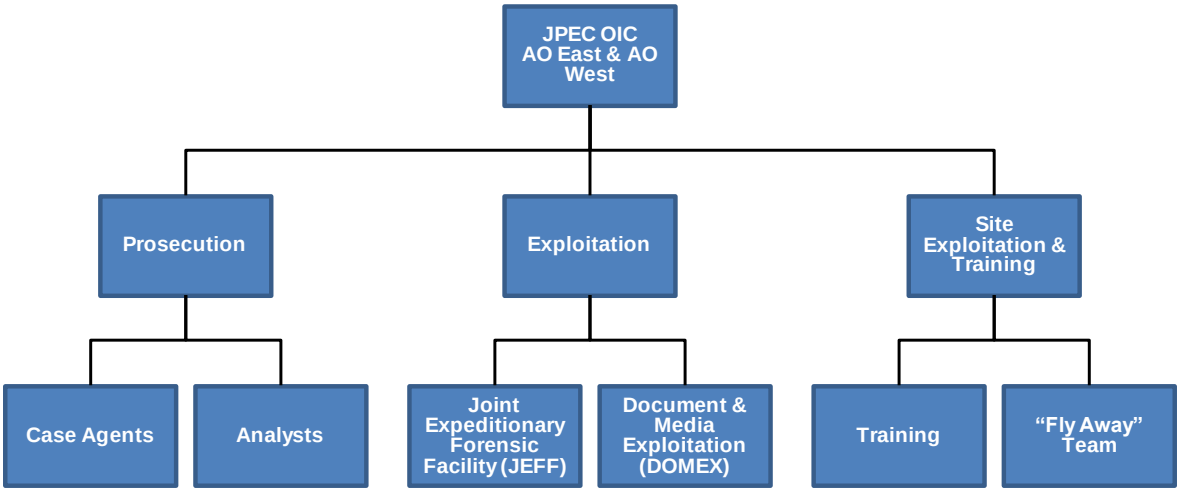

Figure 10. JPEC structure supporting regimental combat teams.[19]

Headquarters Element

The headquarters element of the JPEC was co-located with the MNF-W G-2 to oversee the two site JPECs in direct support of regimental combat teams. The JPEC held coordination meetings several times per week at the MEF through tactical levels with the human intelligence exploitation team, the staff judge advocate, detention facilities staff, and others to promote information sharing and the synchronization of information and forensic data.

The Prosecution Cell

The prosecution cell consisted of Marine criminal investigators, NCIS agents, and intelligence analysts whose primary focus was detainee operations and target package development. Working in concert with their corresponding regimental combat team and across MEF staff sections (counter-IED, rule of law, detainee operations, the G-3 Iraqi Security Force cell, and various G-2 elements including the tactical fusion center), the prosecution cell produced detainee assessments that aided in the criminal prosecution of detainees.

The Exploitation Cell

The exploitation cell contained forensic capabilities to provide analysis to the prosecution cell, intelligence functions, and others in the area of operations. The JEFF provides a "lab in a box" capability with all necessary equipment, resources, and personnel to execute forensic processing and analysis at the forward location. Supported almost entirely by contract forensic specialists, its specific capabilities

[19] Marine Corps Center for Lessons Learned Report, *Joint Prosecution and Exploitation Center (JPEC) Operations and Use of Forensics in Iraq* (revision 1), 4 Feb 2009

included latent prints, DNA, firearms and toolmark analysis, chemical analysis, and document and media exploitation.

Site Exploitation and Training Cell

The site exploitation and training cell conducted site exploitation flyaway missions (an on-call crime scene investigation capability that can be employed wherever needed in the area of operations) and site exploitation training for coalition and host-nation forces. Key evidence retrieved from site exploitation is processed and analyzed at the JPEC JEFF to build additional target packages or later used in trial proceedings against detainees.

Appendix D. Abbreviations and Glossary

Abbreviation	Definition
AO	area of operations
AT/FP	antiterrorism and force protection
BTF	Biometrics Task Force
CEXC	Combined Explosives Exploitation Cell
CENTCOM	Central Command
CID	Criminal Investigation Division
COCOM	combatant command
CODIS	Combined DNA Index System
DFE	Defense Forensic Enterprise
DIA	Defense Intelligence Agency
DNA	deoxyribonucleic acid
DoD	Department of Defense
DOMEX	document and media exploitation
DOTMLPF	doctrine, organization, training, materiel, leadership and education, personnel, and facilities
EFD	Expeditionary Forensics Division
EFL	Expeditionary Forensic Laboratory
FA	firearms
IED	improvised explosive device
IT	information technology
JEFF	Joint Expeditionary Forensic Facility
JPEC	Joint Prosecution and Exploitation Cell
LNO	liaison officer
LP	latent print
MEC	Marine Exploitation Cell
MEF	Marine expeditionary force
MAGTF	Marine air-ground task force
MNF-W	Multinational Force–West
NCIS	Naval Criminal Investigative Service
NGIC	National Ground Intelligence Center
OIC	officer in charge
OIF	Operation Iraqi Freedom
OPMG	Office of the Provost Marshal General

Abbreviation	Definition
ORSA	Operations Research and Systems Analyst
QDR	Quadrennial Defense Review
RBOC	Reach Back Operations Center
SNOIC	Senior Noncommissioned Officer In Charge
USACIL	U.S. Army Criminal Investigation Laboratory
USAF	U.S. Air Force
USMC	U.S. Marine Corps
USN	U.S. Navy

Glossary

Term	Definition
adversary	Enemy combatants, detainees, criminals, hostile foreign intelligence officers, persons of interest, or a party acknowledged as potentially hostile to a friendly party, and against which the use of force may be envisaged.
analysis	1. *Forensic* (forensic function): the scientific examination of physical material and/or data. 2. *Intelligence*: The conversion of processed information into intelligence through the integration, evaluation, and interpretation of all source data and the preparation of intelligence products in support of known or anticipated user requirements.
biometric	A measurable physical characteristic or personal behavior trait used to recognize the identity or verify the claimed identity of an individual (JP 2-0).
biometrics	The process of recognizing an individual based on measurable anatomical, physiological, and behavioral characteristics (JP 2-0).
collect	(Forensic function): recover and account for materials from a site. This may include limited processing of specific items or areas in an effort to detect additional forensically relevant information.

Term	Definition
combatant command	Nontransferable command authority exercised only by commanders of unified or specified combatant commands, unless otherwise directed by the President or the Secretary of Defense. Combatant command cannot be delegated and is the authority of a combatant commander to perform those functions of command over assigned forces: organizing and employing commands and forces, assigning tasks, designating objectives, giving authoritative direction over military operations, joint training, and logistics. It provides full authority to organize and employ commands and forces as the combatant commander considers necessary to accomplish assigned missions. Operational control is inherent in combatant command. Also called COCOM, combatant command should be exercised through the commanders of subordinate organizations.
concept of operations	A verbal or graphic statement, in broad outline, of a commander's assumptions or intent in regard to an operation or series of operations. The concept of operations is frequently embodied in campaign plans and operation plans—in the latter case, particularly when the plans cover a series of connected operations to be carried out either simultaneously or in succession. It is included primarily for additional clarity of purpose.
database	Information that is structured and indexed for user access and review. A collection of one or more computer files. For forensic systems, these files could consist of case information, biometric data, sensor readings, templates, match results, related end-user information, etc.
detainee	A person in custody of the DoD as a result of military operations, including enemy combatants, enemy prisoners of war, and civilian internees, or any person captured or otherwise detained by an armed force.
detainee operations	Taking into custody, maintaining, protecting, and accounting for all categories of detainees who are a threat to U.S. forces, the local population, or other security interests and complying with the law of armed conflict (often referred to as the law of war) as well as implementing U.S. policy. The key sources of U.S. policy for detainee operations include the overarching U.S. Law of War Policy and the multi-Service Detainee Regulation.
Defense Forensic Enterprise	The DoD resources, assets, and processes required to provide forensic capabilities in support of DoD operations.
exploitation	Taking full advantage of any information that has come to hand for tactical, operational, or strategic purposes (JP 1-02; NATO, AAP-6).

Term	Definition
force protection	Preventive measures taken to mitigate hostile actions against DoD personnel (including family members), resources, facilities, and critical information. Force protection does not include actions to defeat the enemy or protect against accidents, weather, or disease. Also called FP.
forensics	The application of multidisciplinary scientific processes to establish facts.
homeland security	A concerted national effort to prevent terrorist attacks within the United States, reduce vulnerability to terrorism, and minimize the damage and recover from attacks that do occur.
host nation	A nation or province that in civil and military matters during peacetime, emergencies, crisis, or conflict renders assistance to allied forces and organizations located on, operating in, or in transit through its territory. Arrangements concluded between the appropriate authorities of host nations and the "sending nations" and/or NATO form the basis of such assistance.
identification	The process of determining the friendly or hostile character of an unknown contact. In combat operations, discrimination between recognizable objects as being friendly or enemy. Also the name that belongs to an object as a member of a class.
identity dominance	Using biometrics and identity management to gain tactical and strategic advantages over the enemy.
information assurance	Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation, including restoration of information systems by incorporating protection, detection, and reaction capabilities.
intelligence exploitation	The process of converting collected information into forms suitable to the production of intelligence.
interagency	Made up of, involving, or representing two or more government agencies.
interoperability	The conditions achieved among communications-electronic equipment systems or items of such equipment when information or services can be exchanged directly and satisfactorily between them and their users. Software applications are considered systems in evaluating interoperability, and their interfaces include carriers and other applications with which they must function for mission accomplishment.
joint	Connotes activities, operations, organizations, etc., in which elements of two or more military departments participate.

Term	Definition
joint force	A force comprising significant elements, assigned or attached, of two or more Military Departments operating under a single joint force commander.
preserve	(Forensic function): protect materials and data, from the moment those items are recognized as holding potential forensic value.
recognize	(Forensic function): locate and distinguish materials that have potential forensic value. Recognition may entail special methods and advanced training to detect items.
reference (function)	The process of querying various repositories of associated information on individuals (intelligence, medical, human resources, financial, security, education, law enforcement, etc.) for analysis purposes.
share	(Forensic function): the cataloguing and distribution of results of forensic analyses in accordance with policies and procedures.
store	(Forensic function): maintain forensic materials and associated information until forensic material disposition is fully adjudicated or resolved. Policies and procedures should dictate proper disposition.
synchronization	(DoD) 1. The arrangement of military actions in time, space, and purpose to produce maximum relative combat power at a decisive place and time. 2. In the intelligence context, application of intelligence sources and methods in concert with the operation plan to ensure that intelligence requirements are answered in time to influence the decisions they support.
technical intelligence	Intelligence derived from the collection, processing, analysis, and exploitation of data and information pertaining to foreign equipment and materiel for the purposes of preventing technological surprise, assessing foreign scientific and technical capabilities, and developing countermeasures designed to neutralize an adversary's technological advantages (JP 2-0).
traditional forensics capabilities	Criminal investigations, including identifications, medical examiner functions, document examination, ballistics, forensic expert testimony, repositories, and research and development.
transfer	Physically transport materials or transmit digital information. Once collected, forensic materials and information are usually transferred to an appropriate location that allows for a more complete scientific analysis.

Term	Definition
triage	(Forensic process): prioritization of forensic materials. This begins at the site by deciding which materials might hold forensic and/or exploitation value. Triage includes making decisions on the appropriate receiving facility, whether and how the materials can indeed be analyzed, the timeline for analysis, how long the materials should be stored, and when and with whom results should be shared.
weapons technical intelligence	Intelligence derived from the technical and forensic exploitation of captured or found explosive devices, associated components, and weapons (DoDD 5101.14).