Concept of Operations (CONOPS) for Police Intelligence Operations (PIO)

4 March 2009

U.S. Army Military Police School

Mission

The U.S. Army Military Police School trains Soldiers and develops agile and adaptive leaders who are well grounded in Army values, war fighting tasks, MP technical skills, and doctrine; prepares Soldiers to be capable of executing the five MP functions in support of Military Police, Army, and Joint Force Commanders while conducting full spectrum operations in the operating environment; plans and focuses on the future by developing and refining doctrine, organization, training, materiel, leader development, personnel, facilities, and nonlethal capabilities that will enable and facilitate the relevance and mission success of the Military Police Corps Regiment, our Soldiers and our formations.

Project Leader

Rich Vanderlinden

ANSER (Analytic Services Inc.)
2900 South Quincy Street, Suite 800
Arlington, Virginia 22206

703-416-3276

richard.vanderlinden@anser.org

Concept of Operations (CONOPS)

for

Police Intelligence Operations (PIO)

4 March 2009

Acknowledgements

Brigadier General David D. Phillips (Commandant of the U.S Army Military Police School and Chief of the Military Police Corps Regiment) and Brigadier General Rodney L. Johnson (The Provost Marshal General of the Army) were the driving force and sponsors behind the development of the Concept of Operations (CONOPS) for Police Intelligence Operations (PIO). The enthusiasm and expert consultation provided by Major Art Horton as the USAMPS Project Leader is gratefully acknowledged. The cooperation of all those organizations that attended and participated in the PIO Tiger Team and the contributions of their representatives are greatly appreciated. The partnership and technical expertise of the ANSER CONOPS writing team was fundamental to the overall success.

USAMPS Project Leader

Major Art Horton (USAMPS PII)

Working Group Facilitators

- Mr. Scott Leonard (USAMPS PII)
- Maj Dave Dozier (USAMPS PII)
- MAJ Vic Baez-An (USAMPS PII)
- CW4 Shaun Collins (USAMPS DOT)

Tiger Team Members

- Mr. Brian Love (USAMPS PII)
- SFC John Waters (USAMPS PII)
- CW3 Paul Arthur (USAMPS PIO)
- Mr. Ron Mullihan (USAMPS DOT ITDD)
- Mr. Bob Catron (USAMPS PIO)
- MAJ Micheal Migliara (MANSCEN CDID RDD)
- Mr. Mike Meyer (MANSCEN CDID CDD)
- LTC Al Bazzinotti (MDOT MP Doctrine)
- Mr. Doug Loggins (MDOT MP Doctrine)
- Mr. George Anderson (MANSCEN TCM-MS)
- Mr. Mark Henley (USAMPS DOT CTDD)
- Mr. Mike Dasso (USAMPS LEP)
- Mr. Chris Holland (USAMPS LEP)
- LTC Noel Smart (OPMG Initiatives)
- MAJ Mike Jensik (OPMG Initiatitives)
- Mr. Eric Barras (OPMG Initiatives)
- Mr. Eric Nikolai (Advancia)
- Mr. Steve Huston (Advancia)
- LTC Dennis Zink (92d MP BN)
- MAJ Caroline Horton (92d MP BN)
- 1LT Benton Parsons (92d MP BN)
- LTC Carl Packer (TRADOC CPMD)
- MAJ Kurt Ritterpusch (TRADOC CPMD)
- LTC Gary Whitaker (USARPAC OPD)

- LTC Glen Giddings (USACIDC LEP Program Manager)
- Mr. Tom Kennedy (USACIDC LEP)
- MAJ Dave Thompson (716th MP BN)
- MAJ James Walker (385th MP BN)
- Mr. John Towery (I Corps DES)
- Mr. Kenneth Cates (AAWO)
- LTC Addison Turnquist (AAWO)
- SGM Jay Thorpe (AWG)
- SGT Micheal Hicks (16th MP BDE (ABN))
- Mr. Mark Nash (ARNORTH PMO)
- Mr. Guy Surian (USACIDC)
- CW4 Al Hogan (CITF)
- CW3 Thomas Roelke (CITF)
- CW3 Jennie Callahan (CITF)

ANSER CONOPS Writing Team

- Mr. Rich Vanderlinden (Project Leader, Analytic Services Inc.)
- Mr. Scott Todd (Senior Subject Matter Expert, The Praevius Group, Inc.)
- Mr. Jim Powlen (Senior Subject Matter Expert, Logos Technologies Inc.)
- Mr. Sam Meale (Subject Matter Expert, MPRI)

Table of Contents

List of Figures

Executive Summary

This concept of operations (CONOPS) establishes a broad approach to provide Police Intelligence Operations (PIO) capabilities and supporting requirements for the United States Army across the spectrum of operations.

PIO is the military police (MP) integrating function. PIO integrates, connects, and shares information and intelligence collected during the conduct of the other four MP functions (Law & Order, Internment/Resettlement, Maneuver and Mobility Support, and Area Security). It supports the operations process through the inclusion of police engagement, police information collection, criminal intelligence, and police investigations to enhance situational understanding, battlefield visualization, and protection, to focus policing operations and support social order (Rule of Law).

This CONOPS seeks to improve coordination and integration across the Army, thereby enhancing operations in both garrison and expeditionary environments. The keys to PIO success for commanders include:

- Integrating PIO into the operations, intelligence and targeting processes.
- Increasing and leveraging criminal intelligence (CRIMINT) analytic and investigative capabilities.
- Linking police, forensic and biometric information with supporting technology to produce intelligence.
- Improving doctrine, training and leader development.

1. Introduction

1.1 Purpose

This CONOPS establishes a broad approach to define the process and effect of PIO capabilities across full spectrum operations (offense, defense, stability, civil support). It describes the use of police information collection, police engagement, criminal intelligence, and criminal investigations in support of maneuver commanders as well as installation commanders in CONUS and OCONUS. In addition, it provides a framework for operators, planners, and intelligence professionals to incorporate traditional and emerging military police capabilities into their respective processes. The end state is to develop doctrine and seek resources to organize, train and equip the Army to meet evolving PIO requirements and capabilities. Finally, this CONOPS provides the basis for a rigorous assessment and analysis of capability gaps and redundancies.

1.2 Scope

PIO has traditionally supported law enforcement, criminal investigative, detention and judicial functions. In recent years, emerging requirements from the Global War on Terror (GWOT), as well as combat operations in the United States Central Command (USCENTCOM) theater of operation, have focused MP and U.S. Army Criminal Investigation Command (USACIDC) functions and applications in support of the Joint, Interagency and Multinational (JIM) communities. This CONOPS provides the background and operational context needed to examine, validate and apply Army concepts for employing “police” (MP and CID) capabilities.

2. Background

PIO is a military police function that supports, enhances, and contributes to an Army force commander's situational understanding, battlefield visualization, and protection by portraying relevant criminal threat and friendly information, which may affect both current and future operations. PIO is supported by forensic, biometric, information sharing and database management tools that capitalize on military police capabilities to analyze police information to develop criminal intelligence. PIO serves as a primary function in order to support intelligence-driven activities.

Vignette: Department of Defense (DoD) Criminal Investigation Task Force (CITF) special agents and analysts working with a task force were preparing criminal cases against detainees. The cases supported the task force's focus on identifying those responsible for the Mosul Dining Facility bombing and eliminating the Al Qaida in Iraq (AQI) cell in Mosul. Analysts began to prepare link analysis diagrams of the cell and its connections. Meanwhile, CITF special agents received a request from another unit to help them prepare a criminal case against a foreign fighter detained in Fallujah. While interviewing the foreign fighter, CITF special agents determined he was a Mosul cell member, who was sent to Fallujah. The foreign fighter was wounded in the fighting and abandoned by his companions. He was angry with his companions for leaving him and agreed to provide information about the Fallujah cell. With the foreign fighter's help, the task force was able to identify the entire cell structure, safe houses, cache locations, and other information about the Mosul cell, to include its Emir and the chief bomb maker. As a result, the task force began detaining members of the cell. The foreign fighter was presented to an investigative judge for the Central Criminal Courts of Iraq, and he provided complete information on the cell and its activities. Using link analysis diagrams, CITF special agents were able to obtain confessions from other cell members, who were also presented to the investigative judge. As a result of the operation, the Emir of the cell, along with several other members, was killed during raids. The remaining members, including the master bomb maker for AQI, were detained and presented to the investigative judge. CITF agents were able to identify insurgent videos of bombing operations that were tied to the bomb maker and the cell. This evidence was presented to the investigative judge who charged the men, who were later convicted.

The CITF is a unique organization within the history of DoD. It was established by Executive Order in November 2001 to combine military law enforcement and intelligence to investigate and support prosecution of war crimes and acts of terrorism in the GWOT. Many lessons were learned during its evolution in combining these two skills sets. Eventually they adapted the A3 paradigm in which Agents, Intelligence Analysts, and Attorneys work in a team to develop and finalize investigations to support prosecution in a variety of venues from military commissions to host nation courts. This paradigm has proved very successful and should serve as a model for the development of PIO in order to avoid repeating the problems CITF encountered during its early evolution.

3. Joint Operating Concepts

A Joint Operating Concept (JOC) describes how joint force capabilities are expected to conduct operations within a military campaign. Army PIO concepts have potential for joint force application. JOCs that require PIO capabilities include, but are not limited to:

3.1 Irregular Warfare (IW) JOC

PIO supports the IW JOC through police information collection, police engagement, criminal intelligence, and criminal investigations conducted against insurgent, terrorist, and criminal networks, linking personnel, equipment, locations, and events. Using criminal intelligence analytical and investigative skills, Army forces may be able to identify threats while simultaneously protecting our assets and friendly civilian populations.

3.2 Major Combat Operations (MCO) JOC

PIO supports the MCO goal of a joint force that acts to achieve decisive outcomes; employs a knowledge enhanced, effects-based approach; gains and maintains operational access; and engages and generates pressure on the adversary. The resulting effect will be joint force action and protection of personnel (combatants and non-combatants), facilities, and equipment throughout full spectrum operations. Army PIO enables inherent operational and tactical flexibility to defeat highly adaptive adversaries by providing the joint force commander with another source of actionable intelligence that is integrated into the common operational picture to enhance situational understanding and decision-making, thereby facilitating decisive action.

3.3 Security and Stability Transition and Reconstruction Operations (SSTRO) JOC

PIO supports the SSTRO goal of effective counterinsurgency operations (COIN), unconventional warfare, and counterterrorism activities, as well as limited conventional operations, in order to impose a level of security that host nation authorities can enforce and maintain in establishing and sustaining an effective government and the Rule of Law (RoL).

Vignette: During the early transition to COIN and Stability Operations during Operation Iraqi Freedom (OIF), site exploitation received priority in attempting to curtail insurgent operations. During the exploitation of a weapons cache, IED weapons material was discovered and seized. The forensic processing of the material revealed latent fingerprints on several detonators that bore identification numbers originating from stock material shipped from a neighboring country. Because of biometric information already on file, a suspect was identified as a possible conspirator in an improvised explosive device (IED) bomb making cell. This consolidated information was provided to military commanders, host nation law enforcement, military intelligence (MI), police agencies, and provost marshals (PM). As a result, a warrant was issued; the suspect was identified, arrested and interviewed by host nation police. The suspect was later prosecuted within the host nation judicial system based upon information derived from US military police information and biometric data.

3.4 Deterrence Operations JOC

The Joint Force Commander, supported by the national intelligence community, must identify and profile adversary decision-makers to identify adversary value structures, as well as the decision-making structures and processes in which adversary decision-makers interact. The ultimate goal of this information collection and analysis is to develop actor-specific analyses of adversary decision-making that describe an adversary's values, culture, decision calculus, risk propensity, and capacity for situational awareness to the maximum extent possible. Interagency cooperation will be key to achieving success in these efforts. Army PIO can support interagency cooperation through a collaborative environment that incorporates intelligence community, diplomatic, law enforcement, armed service, and multinational inputs to achieve true global situational awareness for strategic deterrence.

3.5 Homeland Defense (HD) JOC

PIO supports the homeland defense goals of detecting, deterring, preventing and defeating threats and attacks. PIO supports the range of homeland defense operations and civil support protection capabilities. A CONUS based PIO network that is integrated with local, county, tribal, state and federal, law enforcement entities will ensure a federated approach to enable a unified effort for defense support to civil authorities (DSCA) as well as support (within legal constraints) development and exchange of data assisting in the production of watch lists that deny adversaries access to the homeland, fixed installations/facilities, or expeditionary forces in-transit.

4. Military Problem

The Army lacks sufficient, integrated and coordinated police information collection, police investigative, and crime analytical capabilities to enable PIO across the spectrum of Army operations. Current Army capabilities were designed to meet yesterday's traditional and echeloned adversaries. These capabilities are not sufficient for today's decentralized adversary networks that leverage insurgency, terrorism, organized crime, and irregular warfare. The complexity of the future operational environment, and the prevalence of adversaries leveraging organized crime and criminal activities to support their objectives, drives an increased need for a criminal intelligence analysis and investigative capability at lower organizational levels. Policing, criminal investigative and criminal analytical capability gaps span the entire doctrine, organization, training, materiel, leader development, personnel and facilities (DOTMLPF) domains.

The Army's application of evolving PIO and capabilities (to collect and analyze information for the purpose of producing actionable intelligence to target adversaries) has tremendous potential for criminal enterprise analysis to facilitate methods of identifying, monitoring, penetrating, interdicting and suppressing international, criminal and terrorist network enterprises. Despite the long standing value of Army MP and CID, neither the long-term capabilities nor the responsibility to source these capabilities, have been completely identified or validated. This has resulted in an ad hoc and sometimes disjointed approach to police and police intelligence operations. GWOT, combined with combat operations within the USCENTCOM area of responsibility, has produced a host of emerging requirements that should be addressed through evolving police and police intelligence capabilities.

The Law Enforcement Professional Program (LEPP), [currently being implemented in Operation Enduring Freedom (OEF) and Operation Iraqi Freedom (OIF)] combined with the employment of biometrics and forensic capabilities on the battlefield, has validated the importance of police intelligence-driven operations to support the military decision making and targeting processes across all levels of warfare. The LEPP capability, in particular, was developed by the Joint Improvised Explosive Device-Defeat Organization (JIEDDO) in collaboration with the Army Asymmetric Warfare Office (AAWO) to provide experienced former law enforcement (LE) personnel with criminal enterprise analytical and investigative skills for embedding into corps, division, brigade, regimental and battalion headquarters. Starting in September 2006, JIEDDO conducted a LEPP proof-of-concept by providing former LE professionals to enhance expertise and methodology to understand, identify, target, penetrate, interdict, and suppress criminal networks. Based on the successful LEPP operational assessment, JIEDDO transitioned the program to the Office of the Provost Marshal General in August 2007. In 2008, the Training and Doctrine Command's Capabilities Development for Rapid Transition (CDRT) validated LEPP. USACIDC now manages the program and has the responsibility to resource and develop the enduring capability.

Vignette: A seasoned law enforcement professional's direct participation in site exploitation resulted in the seizure of weapons caches and homemade explosives (HME) source discoveries. One specific case resulted in the successful identification and recovery of a cache of 168 explosively formed penetrators (EFP) from a mosque in Baqubah.

Enhanced criminal intelligence capabilities can enable near real-time actionable intelligence for tactical commanders and contribute strategic products relevant to the JIM community. For example, the use of criminal intelligence analysis is critical within the Improvised Explosive Device-Defeat (IED-D) "Attack the Network" line of operation. PIO represents a unique capability that readily transitions from major combat operations to stability operations and the implementation of the RoL.

Vignette: During stability operations, information obtained during an arrest interview and previous information collected during combat operations yielded an analytical product that produced credible information implicating a new suspect's involvement in an IED cell. As a result of this information, an arrest warrant was obtained and the suspect was later detained at a border crossing of the adjacent country. Subsequent biometric and police database information confirmed the suspect's identity, and an arrest warrant was issued. The suspect was detained by US military forces and jointly interviewed by HN and US law enforcement. He admitted to being the Emir of this IED cell and stated he purchased detonators from military sources within neighboring countries, as well as received financial support from locals in those countries. This information was provided to US and multi-national force intelligence agencies and host nation prosecutors. As a result, the suspect was prosecuted and imprisoned. Intelligence agencies utilized this information as means to target state supported terrorist cells that operated outside the boundaries of the host nation.

There is a critical need to refine and expand the Army scope, capabilities and application of PIO while simultaneously capitalizing on existing capabilities such as those inherent in the CITF and LEPP. This effort requires the Army to aggressively pursue and plan for robust, fully integrated and well resourced police intelligence capabilities and applications throughout full spectrum operations.

5. Vision

PIO is the "integrating" military police function that provides police information and critical criminal intelligence analysis to support criminal investigations, maneuver commanders prosecuting full spectrum operations, and installation commanders (both in CONUS and OCONUS) conducting protection and law enforcement operations. PIO has an integral role in the intelligence and protection warfighting functions (and applicability in others) as well as the Army's operations, targeting and composite risk management (CRM) processes.

PIO, and the criminal information developed from these operations, is generated by MP Soldiers and CID agents on the ground, CID agents and examiners in deployable and CONUS-based forensic labs, and MP Soldiers conducting counterinsurgency operations in detention facilities, all linked by biometric identification instruments and a common intelligence system. A criminal intelligence analyst uses this information to produce criminal intelligence products (identifying patterns, series, trends, associations, etc.) that are used to guide targeting, decision making and investigative efforts.

Police Intelligence Operations is the integrating function across the other four MP battlefield functions (Law & Order, Internment/Resettlement, Maneuver & Mobility Support, and Area Security). The result is effective information collection, analysis, and management to support the common operational picture, operational planning, development of actionable intelligence, and the ability to interdict criminal networks. These capabilities also support other U.S. governmental agencies, multi-national forces, allies, and host nations (JIM partners) to establish civil authority and RoL.

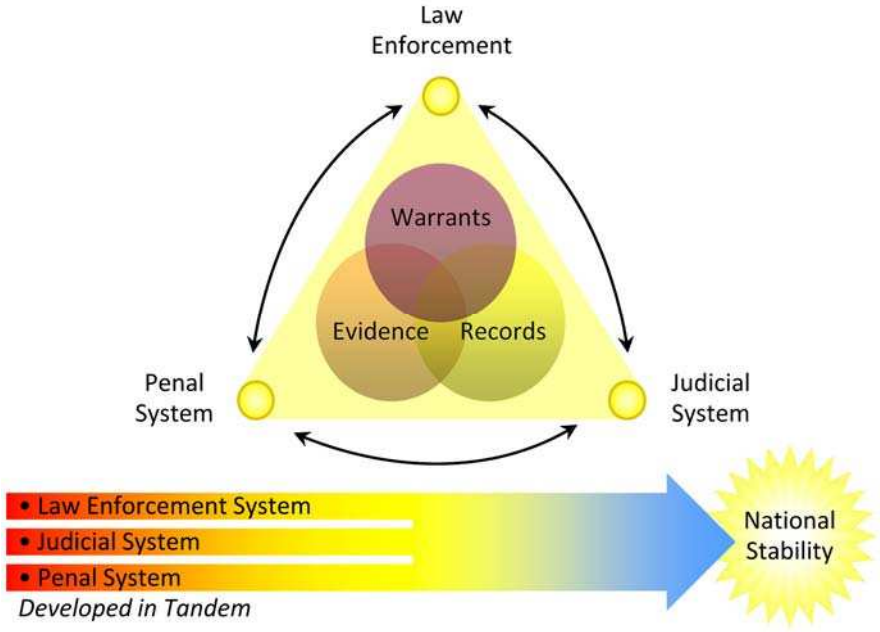


Figure 1 – Civil Authority Triad

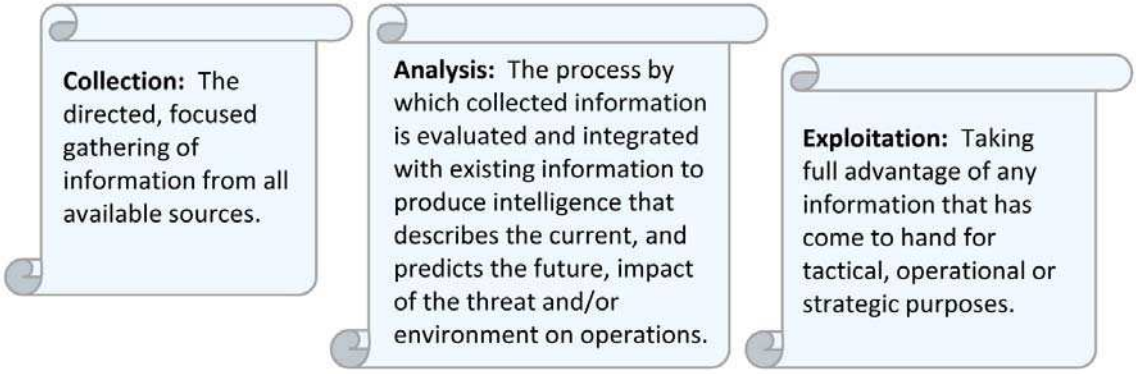
6. Police Intelligence Operations

PIO is the military police integrating function that supports the operations and intelligence processes through the inclusion of police engagement, police information collection, and police investigations to enhance situational understanding, battlefield visualization and protection, to focus policing operations and support social order (Rule of Law).

PIO must support the full spectrum of ever-changing, emerging Army expeditionary and garrison operations to meet traditional, irregular, disruptive, and catastrophic challenges, adversaries and threats. PIO capabilities effectively integrated into Army operations are highly effective in assisting commanders and leaders in shifting their focus from traditional threats to non-state and transnational actors, insurgents, terrorists and criminals.

The Army must keep pace with these challenges, allocate sufficient resources, and assign permanent responsibility for sourcing. Efforts to integrate PIO must begin by effectively integrating the PIO functions throughout approved and accepted Army processes.

6.1 Principles of Police Intelligence Operations



6.2 PIO Integration into the Operations Process

It is imperative that police intelligence be firmly woven into the operations process (Figure 2) for both CONUS and OCONUS garrison and expeditionary operations. While each operation and environment differs in design and circumstances, all operations follow the planning, preparation, execution and assessment cycle inherent in the operations process. Army expeditionary forces should include PIO considerations in all appropriate warfighting functions.

Figure 2 – Operations Process

The mission analysis phase of the military decision making process (MDMP) is the initial step to integrate PIO considerations into the planning effort for the police domain. Analysis of the policing environment is facilitated by a doctrinal tool (FM 3-19.50) using the acronym "POLICE" to analyze the police environment.

- **P**olice and Prisons: What are the capabilities and conditions (organization, training, equipment, communications, logistics, and facilities)?
- **O**rganized Crime: What organized criminal networks exist, and what is their influence and impact on the security environment?
- **L**egal System: What is the level of due process within the society and what are the procedures to support prosecutorial functions? Are all components of the legal system (police, prosecution, judiciary, penal) fully integrated and functional?
- **I**nvestigations and Interviews: What are the investigative capabilities within the police organizations?
- **C**rime Conducive Conditions: What is the assessment of criminal activities for the region and factors influencing the conditions?
- **E**nforcement Gaps and Enforcement Mechanisms: What mechanisms that help to enforce norms, rules, and laws are present (and not present) within the society?

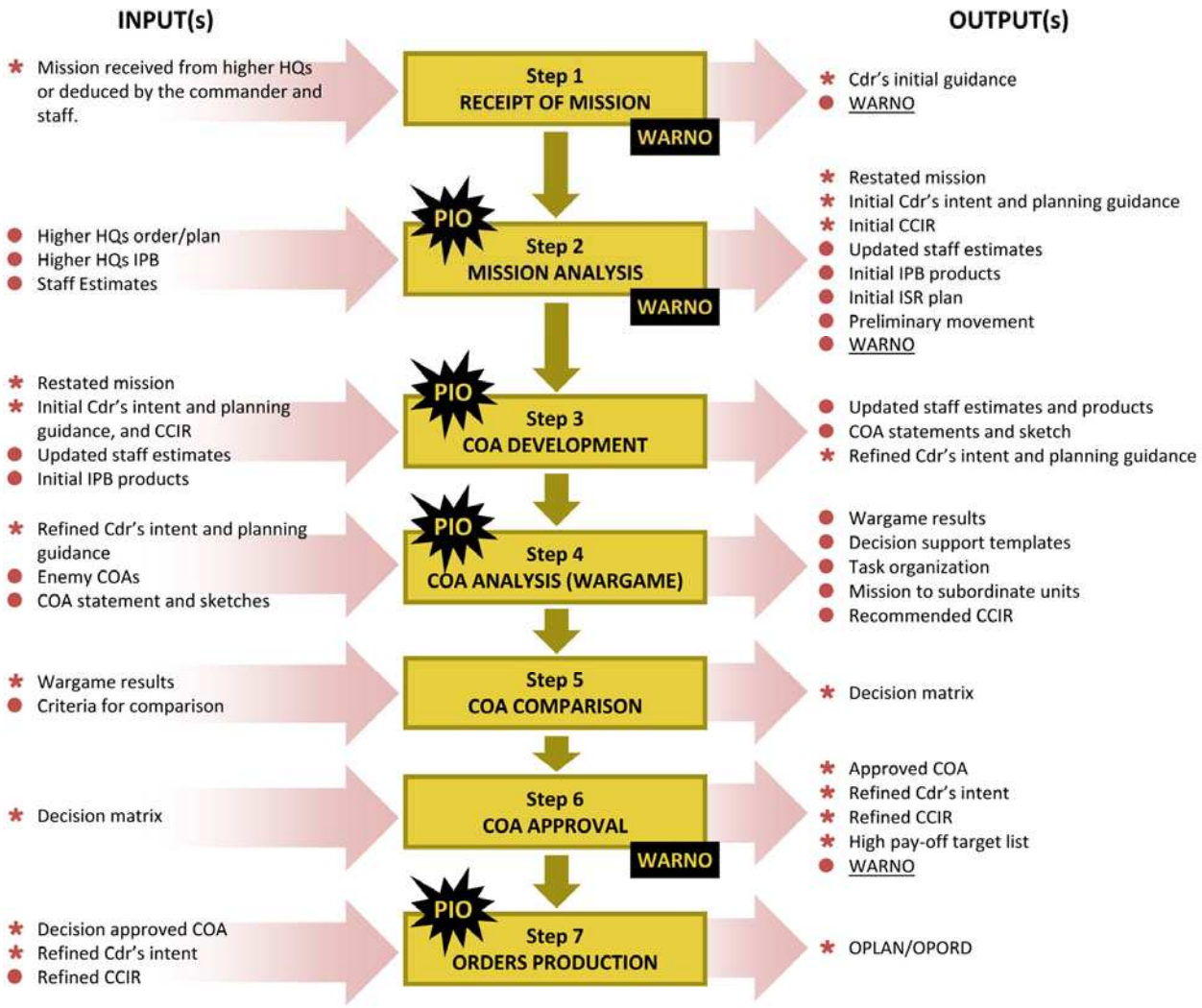


Figure 3 – PIO Integrated into MDMP

Vignette: Multi-national force experience in Iraq and Afghanistan has shown that if any component of the legal system (police, prosecution, judiciary or penal) ceases to function, the entire system breaks down. Example: as of late 2008, Afghanistan had a robust corruption investigations unit with over 300 active criminal cases, yet the system as a whole failed to process cases through judicial review due to a lack of prosecutorial follow-through and appropriate court with venue.

Vignette: In 2007 in Fallujah, local judges failed to report for work and perform their duties due to al Qaida intimidation. As a result, detention facilities remained intolerably overcrowded, and the police became frustrated and saw no point in making additional arrests or conducting thorough investigations. Absent due process, many innocent detainees languished in sub-standard prison facilities and became prime recruitment candidates for al Qaida. Furthermore, due to overcrowded conditions, some detainees were released.

Information gathered from the police environment assessment can be used to identify operational requirements and drive future information collection efforts. Based on mission analysis, recommendations can be made for input into the commander's critical information requirements

(CCIR) and the intelligence, surveillance and reconnaissance (ISR) synchronization plan. Running estimates serve to support the creation of the MP concept of employment and police operations.

By developing running estimates on events and activities across a specific geographical region (e.g., neighborhood, village, city, municipality) Army forces can track variances that may warrant adjustments to current or future operations. Running estimates provide valuable tools to fill information gaps in the common operational picture and focus efforts on items and activities that provide general indicators of the nature of security. Examples of indicators of security challenges include: violent crime, carjacking, robberies, kidnappings, police corruption, detentions and treatment of detainees and prisoners, no-show rates for local police, weapons charges, black-market activities, assaults on police / security forces, a decrease or marked shift in citizen daily activities, vandalism, and ethnic/religious/cultural/racial specific crimes.

During course of action (COA) development and analysis, MP/CID provide vital information and evaluation criteria to ensure COA comparison includes policing considerations which may affect a commander's COA selection. Analysis of the "POLICE" considerations is completed using the tools provided in FM 3-19.50.

During the prepare phase, MP/CID task organize and prepare forces to support the selected COA. At the company level and below, troop leading procedures ensure forces are adequately prepared to execute PIO tasks, and police information collection efforts are assigned.

During the execution phase of operations, commanders make execution or adjustment decisions based on the current situation. MP/CID running estimates inform and influence these decisions. MP/CID make recommendations to commanders on how to prioritize resources to best affect police operations and ensure PIO capabilities and resources are task organized for success. It is vital that MP/CID integrate within the key operations forums such as working groups, boards, bureaus, centers and cells (WGB2C2) (i.e. effects working group, fusion working group, targeting boards) to advise commanders on the use of police capabilities, engagement with host nation, indigenous, and/or multi-national military and police forces, to ensure they provide direct input for current and future operations.

Assessing. As operations progress, and new operations begin, MP/CID monitor and conduct continuous assessments of all operations within the police domain. In doing so, they provide a critical evaluation of the effectiveness and performance of police specific tasks/objectives. Examples of reportable items include:

- Percentage of change in crime rates
- Percentage of change in police force structure and capabilities
- Volume of investigations initiated
- Volume of arrests and prosecutions
- Volume of detainee/prisoner releases
- Major geographic shifts in criminal activity (i.e., crime displaced to an area with less police activity)

- Major changes to patterns of life (i.e., local businesses opening, re-opening, closing)
- Major shifts in local population (i.e., migrations, resettlements)
- New, emerging or refined criminal operational tactics, techniques and procedures (TTP)

Conducting intelligence operations generally follows five functions that constitute the intelligence process: plan, prepare, collect, process, and produce. These functions are continuous, not necessarily sequential. In addition to these functions of the intelligence process (Figure 4), there are three common tasks: analyze, assess and disseminate that occur throughout. The intelligence process provides a common model with which to guide one's thinking, discussing, planning, and assessing the threat and operational environment.

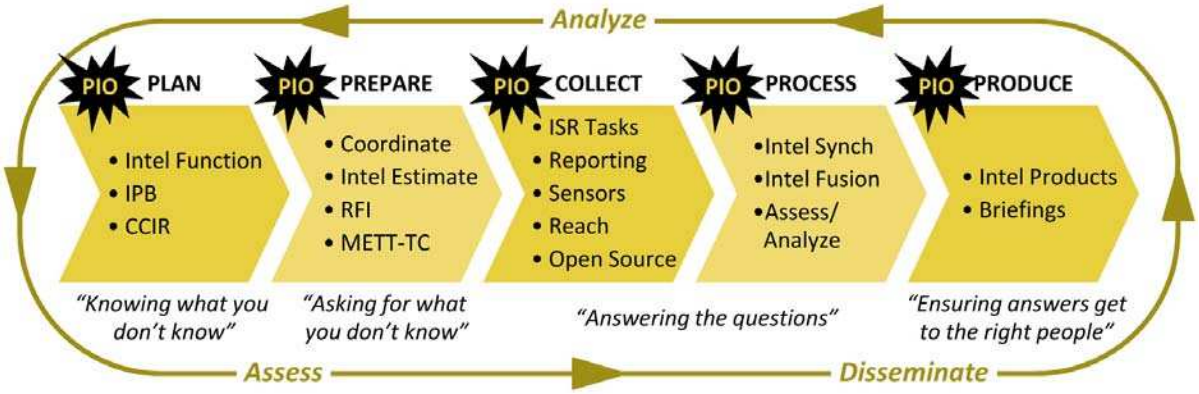


Figure 4 – Intelligence Process

Information and intelligence fusion helps commanders manage the volume of information by providing a means to merge various sources of data from all sources and intelligence disciplines into a more coherent intelligence picture for commanders and leaders. The Distributed Common Ground System-Army (DCGS-A) provides automated fusion to assist the analyst in processing police information and generating criminal intelligence products.

In expeditionary environments, PIO products aid the maneuver unit S2/G2 in producing the intelligence summary and intelligence estimate supporting OPLANS and OPORDS. However, in CONUS-based PIO operations, MI is in support of PIO because of specific intelligence oversight regulations which limit MI from maintaining U.S. persons' data. During the Plan phase, PIO identifies pertinent information and intelligence requirements (IR), develops a strategy for ISR operations to satisfy those requirements, directs intelligence operations, and synchronizes the ISR effort. In the Prepare phase, PIO participates in producing the intelligence estimate, helps identify an analytical collaborative framework, and presents briefings and situation updates to support the common operational picture (COP).

Throughout the Collect phase, PIO capabilities are focused on the Commander's Critical Information Requirements (CCIR). Policing specific collection tasks are identified and fill information requirements supporting the CCIR. Through active MP/CID participation, collection requirements are placed in the ISR synchronization plan, assigned, and information requirements are acted on. The process of identifying and collecting information is dynamic and constantly changing. As such, a

focused effort is needed to ensure PIO considerations are understood and contribute to the overall intelligence effort. At the tactical level, police on the ground gather information through active and passive collection. The information reported must be formalized and integrated in both the intelligence and operational processes. Small unit level in-briefings and debriefings must follow a disciplined system in order to ensure information gathered during all operations is timely and valuable for the overall Intelligence process.

During the Process phase, criminal intelligence analysts convert information into a form suitable for analysis and use, identify additional information requirements and facilitate situational understanding. During the Produce phase, PIO integrates evaluated, analyzed, and interpreted information into finished intelligence products with the goal of answering CCIRs, thereby enabling commanders to make critical decisions and take decisive action.

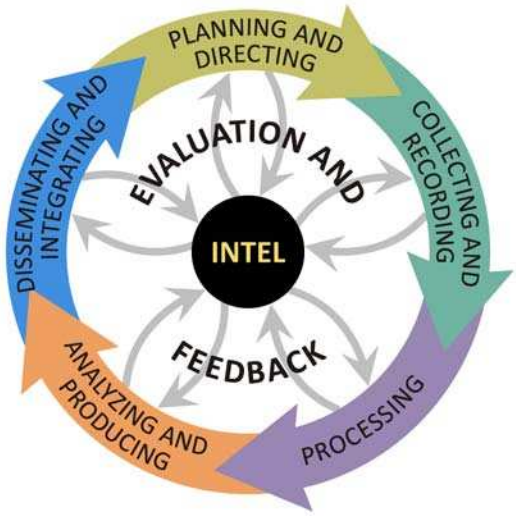


Figure 5 – Criminal Intelligence Process

By integrating PIO within the operations and intelligence processes, policing efforts inform the targeting process by assisting in the nomination of specific targets by generating detailed knowledge of the police domain. To ensure unity of effort, MP/CID actions must complement and be coordinated with maneuver/installation commander efforts, processes and priorities. MPs must know who and what is on the target list and what actions and procedures to follow to report information. Police representation in the targeting process ensures appropriate recommendations are made based on the target's value and level of development. PIO considerations include:

- Target selection and timing
- Methods of engagement (lethal or nonlethal)
- Method of delivery (MP, THT, CA, PSYOP, maneuver unit)
- Desired results (destroy, disrupt, compel, control, influence)
- Impact on local or HN police primacy and/or legitimacy

MP/CID must understand where and when their involvement is appropriate or necessary while simultaneously working within the commander's intent. MP/CID direct involvement is needed for

targeting that involves police transition teams, detention operations, and biometrics and forensics collection. Within the targeting process, an assessment loop provides feedback that allows commanders to adjust operations accordingly.

When planning and integrating PIO support to various lines of operation, contingent upon the specific objectives of a military campaign, MP/CID must develop indicators and collect police information that identifies trends, patterns and associations that indicate a possible criminal nexus disrupting or targeting the Army operations. Based on these indicators, PIO can focus on developing plans for collecting and analyzing information related to criminal activities and crimes. The criminal intelligence produced from this analysis should be focused on future coordination with local/HN police and potential incorporation into the targeting process.

The collection efforts must identify what is predictable in the society, what cycles occur within the society, and analyze how criminal elements are most likely to affect these cycles. Key society-based environmental factors to assess and continuously monitor include:

- Civil Control: information and media cycles; school cycles; transportation systems
- Civil Security: holidays, pilgrimages, sporting events, religious observances, public remembrances, periods of increased crime
- Essential Public Services: electricity, water, sewage, trash, transportation, and businesses
- Economic Development: markets, goods and services, agriculture, labor forces, distribution of wealth
- Governance: election process, political process, crimes against political figures / parties, transfers of power between party lines
- Civil Considerations: social, ethnographic and cultural considerations

6.3 PIO Capabilities in an Expeditionary Environment

The purpose of PIO in an expeditionary environment is to integrate unique police capabilities into forward deployed maneuver unit and task force operations. By integrating PIO, leaders and commanders will better understand enemy networks and how they leverage illicit activities to facilitate subversion, lawlessness, and insurgency. This understanding and insight will facilitate Army operations designed to disrupt enemy actions by targeting criminal activities.

The goal of PIO in an expeditionary environment is to integrate and collaborate within the operations and intelligence functions of expeditionary maneuver units and task forces in order to produce or contribute to the production of actionable intelligence.

Collection

MP, throughout all of their missions (Police Intelligence, Law & Order, Internment/Resettlement, Maneuver & Mobility Support, and Area Security) gather volumes of information vital to the full understanding of an area of operation and the specific crime factors that influence a safe and secure environment. MP gather information through passive and active collection, in both garrison and expeditionary environments. MP perform information collection while:

- Conducting MP combat patrols (Maneuver & Mobility Support, Area Security)
- Conducting community policing
- Receiving and responding to citizen complaints and emergencies
- Conducting criminal investigations
- Conducting detention operations and interacting with detainees and their visitors
- Debriefing police informants
- Exploiting forensic and biometric data
- Interacting with Other Governmental Agencies (OGA)
- Interacting with Non-Governmental Organizations (NGO)
- Interacting with other host nation officials, military forces and police forces
- Interacting with local religious and tribal leaders
- Interacting with other multi-national military and police forces
- Interacting with media and public information forums

Active Collection

Active collection is the specific, deliberate and targeted collection of information focused on answering priority intelligence requirements (PIR), specific information requirements (SIR), specific orders or requests (SOR), or other deliberate collection plans. When MP are given a specific mission to actively collect information, commanders must ensure they are properly manned and equipped to collect the information. Throughout their collection efforts, MP must closely coordinate with maneuver units to ensure active collection efforts do not adversely impact the maneuver unit mission or collection plan. By fully integrating PIO within the key operations forums (i.e. effects working group, fusion working group, targeting boards), potential conflicts are proactively addressed.

Passive Collection

Passive collection is non-specific collection gathered by observations while performing other MP missions. In concert with the doctrinal principle of “Every Soldier a Sensor” - - every encounter is a collection opportunity. When an MP makes an inquiry to clarify or elaborate on something that he/she has heard or observed, it is still considered passive collection.

In support of the greater collection effort, it is desirable that every Soldier be a sensor and contribute to situational awareness. Soldiers, while able to observe the environment, are often limited by language barriers and translator availability. However, basic skills of observation can lead to the gathering of valuable information, if the Soldier is trained on what to look for. For example, when police officers work a “beat,” their baseline of knowledge consists of knowing three fundamental facts about their area: who lives there, what do they do, and when do they do it. When these key facts are understood, all other observables become a variant of what is deemed “normal” and is therefore more easily collected.

Police Information Sources

MP gather information from all available sources. Major sources include:

- Law enforcement/police and other emergency responders
- Host nation security forces (i.e. military and police forces)
- Criminal activity
- Walk-in complainants
- Telephone "tip lines" and emergency calls
- Informants
- Interaction with the local community
- Religious and tribal leaders
- Police Mentor Teams (PMT) and Police Transition Teams (PTT)
- Biometrics and forensic materials
- Databases
- Technical intelligence gathering
- Interagency organizations working in the theater of operation
- Other Governmental Agencies (OGA)
- Non-Governmental Organizations (NGO)
- Internet, print and broadcast media

Key Themes in MP Collection of Information

Community policing, information collection, investigative skills, handling of sources, and criminal intelligence analysis expertise must be supported and sustained while MP perform their installation law enforcement function. Because of their unique interaction with the community and law enforcement agencies, MPs are a great source for collecting all types of information and can be used for targeted collection.

When working with host nation or indigenous law enforcement personnel, commanders must be cautious when directing MP to perform active collection tasks. This is especially true when the collection effort will target the very people with whom MP work and partner. This type of collection can jeopardize the mission MP are performing, be counterproductive to their sphere of influence, and place them in dangerous situations.

MP require access to databases to input police information which can then be easily queried and analyzed. The databases should be accessible for data entries at the lowest level. Information within the database should be viewable by analysts at all levels and in all type of units. The information residing in the database must be able to be analyzed by criminal analysts and investigators for its investigative and prosecutorial value. Simultaneously, the data must be shared with MI analysts for

actionable intelligence. The database should use a taxonomy that facilitates analysis and exploitation with supporting hardware and software tools that facilitate decision making.

Analysis

Soldiers from all types of units indirectly collect police information. Therefore, maneuver commanders responsible for a specific area of operation (AO) require the capability to analyze this information through a criminal investigative lens. To accomplish this, criminal intelligence analyst capabilities are required at the Brigade Combat Team (BCT) level. These criminal intelligence analysts provide the commander with a required set of skills to identify adversaries who use criminal tactics. Criminal intelligence analyst capabilities must reside at all levels in which information analysis is occurring within the maneuver unit.

The purpose of integrated criminal intelligence analyst capabilities is to analyze police information and support the production of actionable intelligence (in close coordination and collaboration with MI and maneuver units) and the development of a strategy to reduce the effect of overall crime. By working as a collaborative team, MI helps MP develop targeted information collection requirements, while MP provides MI with a law enforcement perspective for analyzing criminal information.

Trained criminal intelligence analysts possess the following capabilities:

- Provide advice and information on how criminals and criminal organizations operate
- Identify funding sources and criminal activity that support adversary groups
- Assist in categorizing hostile actors (i.e., criminal, supporter, affiliate, financier, corrupt official, supplier, trafficker, smuggler, recruiter, etc.)
- Recommend and assist in the development of police information collection strategies
- Assist in developing targeting strategies
- Conduct “human terrain” analysis from a criminal standpoint
- Conduct consequence analysis
- Identify gaps in information and nominate Information Requirements (IR)
- Interface with MP assets operating within the AO
- Prepare products and predictive analysis on criminal activities
- Develop actionable intelligence for subsequent targeting

Criminal intelligence products and reports should maximize the use of the data and provide commanders useful tools to augment a holistic assessment of the security environment across the AO. Characteristics of the criminal intelligence analyst products include:

- Distinct: support other intelligence products but is a stand-alone analysis
- Tailored: to any geographic, demographic and other parameters

- Actionable: provide commanders situational understanding to support decision making by identifying parameters wherein the intelligence is actionable
- Accessible: accessible to stake holders (commanders, operations / intelligence staffs, other analysts, host nation security forces, OGAs, other LE agencies)
- Timely: supports the commander's battle rhythm, objectives and intent for on-going operations / effects

In addition to raw data shared throughout the theater, products developed by criminal analyst must be shared up, down and laterally throughout the organization. These products must be developed and stored in a searchable and interoperable database and produced in a standardized format to facilitate expedited analysis and query. In addition to analytical reports, other examples of police intelligence products are shown in Figure 6 below.

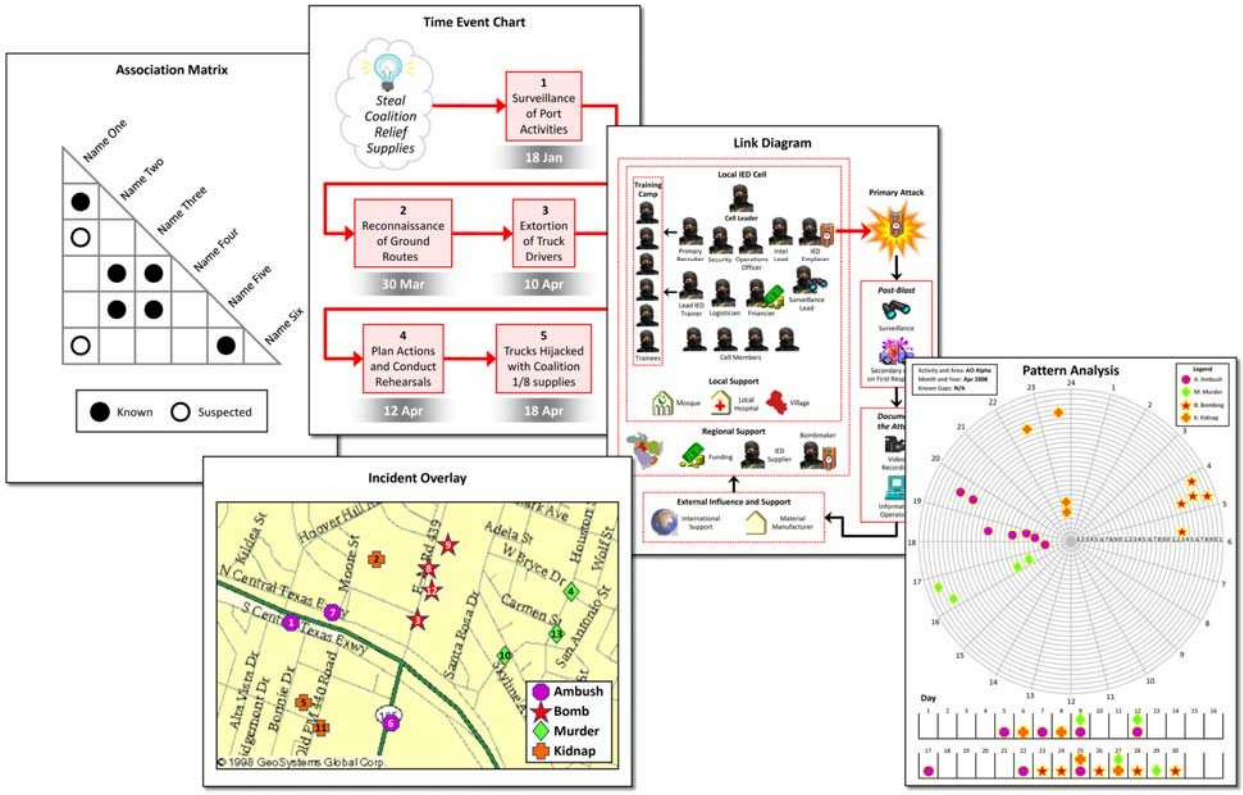


Figure 6 – Police Intelligence Products

The process for passing information must flow from the individual collector upward and from analysts downward. Forensic examiners working in joint expeditionary forensic facilities (JEFFs) (deployable forensics labs) must be able to access and input data into this database. JEFFs, along with organizations such as the Combined Explosives Exploitation Cell (CEXC) process forensic material and help facilitate criminal prosecution and the ability of multi-national forces to attack criminal networks.

Vignette: During clearing operations in Zandubahr, elements of 2-3 Infantry located a cache which included a suicide vest, plastic explosives, weapons, ammunition, Google Earth maps, and more than 150 pieces of photo identification. The cache was processed for evidentiary purposes and later the suicide vest, maps and pieces of identification were submitted to CEXC for forensic examination. The results of the exam revealed multiple sets of identifiable latent fingerprints. Three latent fingerprints were identified as belonging to persons processed through a host nation detention facility, with one of the subjects still detained. Further exploitation of the cache indicated that, in addition to being a suicide bomb cell, its members planned and executed kidnappings.

Maneuver units from Company to BCT level may have organic MP, or MP units or patrols may be operating within their AO. When they are operating within a maneuver commander's AO, it is imperative that MP are able to share information with the maneuver unit targeting or effects coordination cell, within the operations and intelligence sections, so that information and/or intelligence can be actioned. Both MP and MI analysts require access to each other's databases and products, which will require them to have an equal level of security clearance. It is imperative to keep as much law enforcement-related evidence, information and intelligence as possible at the unclassified level, so it can be used as evidence in judicial proceedings. Law enforcement access and use of classified intelligence products should be used to identify leads and followed up through investigative efforts designed to capture the required information or evidence in an unclassified category. Figure 7 depicts a construct for PIO information flow for an operational theater.

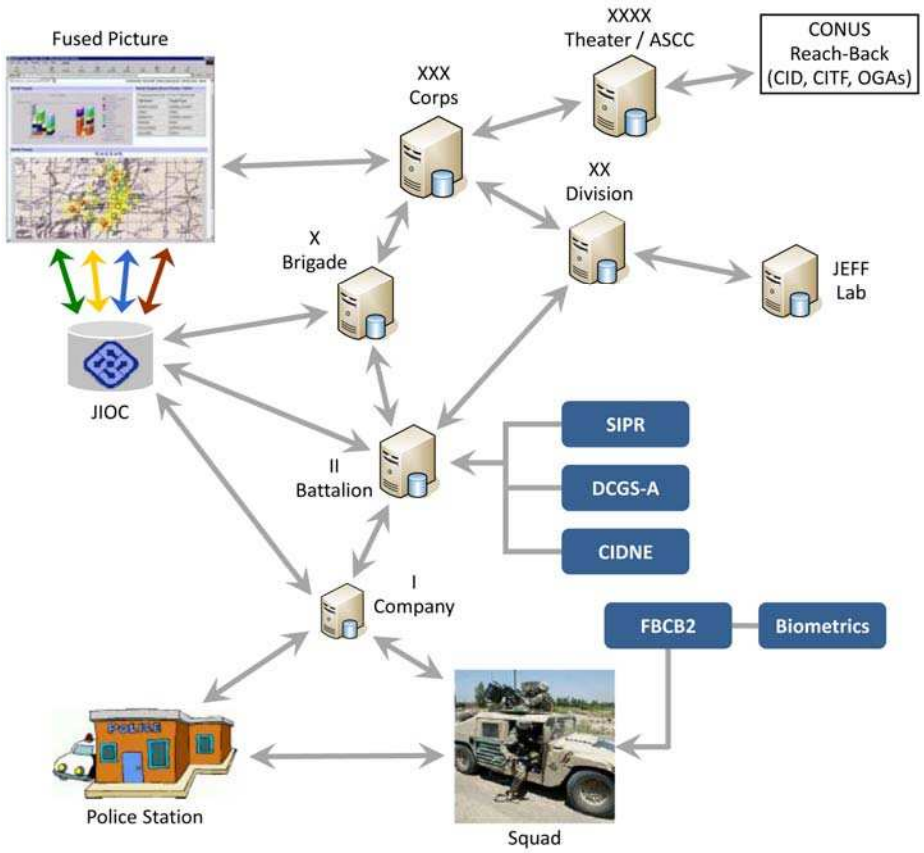


Figure 7 – Police Information Flow for a Theater of Operation

The establishment of information and intelligence fusion cells within expeditionary units, from special operations forces to general purpose forces, is increasingly more prevalent. Although Army doctrine for the employment of fusion cells is not yet developed, fusion cells in operational environments have proven valuable given the complex environments and disparate information from multiple organizations that must be combined and analyzed to support a common operational picture. From a PIO perspective, fusion enables commanders to have a "see, decide and act" advantage over criminal networks, terrorist groups, cells, and individuals by ensuring police information and police intelligence is integrated as vital pieces of the overall battlefield visualization.

With effective integration into the operations and intelligence process, PIO can enhance battle command by helping commanders to understand, visualize, describe and direct operations. PIO can also fill in the gaps between enemy order of battle, situational template, or network and enemy TTPs versus criminal or non-affiliated negative impact actors in the AO. Moreover, by incorporating PIO analysis and products into the operations and intelligence processes (including MDMP, targeting, effects, and strategies), the overall integration will ensure the criminal aspects of the area threat are considered for all operations.

Vignette: The vast majority of the information and data collection is performed at the small unit level where units have direct interaction with the community and host nation / indigenous security forces. Information gathered is reviewed and receives initial analysis at both the MP and maneuver company level, where additional, focused collection efforts can be directed. Information from the lowest level is entered into a universal, networked database following a standardized data entry protocol to enable rapid data analysis and exploitation. Battalion and higher level headquarters access the information via the universal database. Each unit level takes appropriate action within their AO based on development of intelligence, and, in turn, adds additional data and analytical products to the universal database. The result is a wide area network criminal intelligence picture to support MP/CID, BCT and division operations and continuous analytical processes. Data from the lowest levels is accessible by the JEFF labs for synchronization and exploitation. By using a universal, networked database, units at the tactical level can act on criminal activities within their AO, while operational and strategic levels identify organized criminal elements that cross geographical and national boundaries. The end result facilitates the effective targeting of the entire network (from tactical to strategic levels) consisting of planners, financiers, supporters, trainers, and facilitators.

Detention operations provide a valuable source for passive and active criminal information collection and the identification of exploitable information for other operations. Army forces exploit detainees by gathering physical evidence at the time of capture. MP exploit detainees through passive and active information collection throughout the detention process, and through directed criminal interviews. Because of their unique training and experience, law enforcement personnel should be integrated into detainee processing at the lowest levels (i.e., at the point of capture). If point of capture integration is not possible, law enforcement expertise is required from the first detainee processing stop (i.e. Detainee Holding Area) all the way up to the theater internment facility (TIF) level. The value of law enforcement personnel at the lowest level is their ability to identify potential evidence, support the witness/suspect interview process, assist in preservation of evidence and documenting detainee affirmation statements, establishing chain of custody documentation, and initiating criminal case development. Throughout the entire theater

internment system, all personnel involved (from point of capture through court proceedings) with detainee processing should understand that information and evidence gathered and linked to a specific detainee must pass sufficient legal scrutiny to support eventual prosecution. Regardless of whether active or passive collection methods will be used, MP and MI must coordinate their activities when it comes to collecting against detainees and their visitors.

The primary responsibility for submitting criminal prosecutions during expeditionary operations resides at the battalion level (MP or maneuver unit). The staff judge advocate (SJA) should develop and implement a prosecutorial process that fulfills all requirements of the respective judicial body (e.g., host nation, tribunal, military courts, etc.) in support of establishing RoL. As such, the investigative case receives close coordination with attorneys, criminal investigators, forensic examiners, and analysts, and therefore can withstand the scrutiny of the judicial body.

Vignette: The DoD's Criminal Investigation Task Force (CITF) has a unique mission of combining intelligence with law enforcement information in order to develop prosecutable cases against terrorists and war criminals in venues that range from military commission to the central criminal court of Iraq and the Afghanistan national security court. Over the almost seven years of its existence the CITF's investigative model has evolved, and they now use the "agent, analyst and attorney" (A3) model. Early in its evolution, CITF learned that special agents and analysts process information differently, and they achieve the most efficient investigation by having special agents and analysts work in peer teams where both review the same information and collaborate on what it means and how best to develop investigative leads. By adding an attorney to the model, CITF learned that this kept investigations focused and brought another unique skill set to bear on case development. As currently staffed, CITF is organized with one analyst for every two special agents and one attorney to every investigative unit. Whether to institutionalize the A3 model as an enduring Army capability warrants further review.

As military operations transition away from combat operations, PIO considerations support the transition from a safe and secure environment to RoL. Database management considerations (criminal data, forensic and biometric) must be planned and integrated early on during combat operations in order to ensure appropriate transition of information as host nation security forces assume greater roles and eventual primacy.

Vignette: A seasoned law enforcement professional coached and mentored the implementation of a community-based policing program with the elders in Metr Lam, Afghanistan, which focused on the security of bridges and culverts and the prevention of improvised explosives device (IED) attacks. The security program, led by Afghan citizens, included the daily inspection of over 600 bridges and culverts. The program reduced the occurrence of IEDs from three per week to zero.

6.4 Integrating PIO Principles for the Garrison Environment

The PIO principles and capabilities which support the expeditionary Army (discussed in section 6.3 above) have a direct application for the garrison operating environment (CONUS and OCONUS). Some specific information restrictions apply for peacetime operations in a garrison which must be considered during the planning and execution of law enforcement and protection operations. Those restrictions are discussed in paragraph 7.1 of this CONOPS.

The PIO principles (collection, analysis and exploitation) provide a solid operational framework for garrison commanders and leaders to understand, visualize, describe and direct operations and ensure effective PIO integration. PIO has the capability to assist the garrison and installation commander in his decision to employ various types of policing strategies to ensure a safe and secure environment for tenant units and families.

Vignette: A VCSA report concerning sexual assaults and reviews of the Military Police Daily Blotter and Journal prompted a Senior Commander and Garrison Commander to create a Sexual Assault Task Force (SATF) to examine sex crimes impacting the life, health, and safety of the installation community. The Installation Commanding General tasked the Garrison Commander to provide sexual assault information in an IPB format. The fusion cell was tasked as the lead for the SATF IPB effort. This was possible because the fusion cell included personnel from the intelligence and police disciplines and was able to not only fuse information into intelligence, but to fuse types of information analysis (actionable - preventive and prosecutorial). The fusion cell used various databases to conduct data mining to identify sexual crimes, person crimes, and property crimes. Products included developing graphic products (maps) that pinpointed crime locations and identification of the top crime areas on the installation, with associated security lighting data. This provided target areas for lighting efforts, installation of CCTV, and adjustments to law enforcement patrol distribution plans. Through analysis, the fusion cell was able to define the crime environment, a criminal and victim profile, as well as social-behavioral factors. Solutions addressed and refined initial attempts to solve the issue without analysis. Analysis provided the ability to pinpoint specific problem locations and specific social issues, which in turn allowed the focus of limited funding. The solutions went beyond traditional police and included recommended environmental and social changes. Information collected included police information as well as non-police information. Analysis includes the comparison and correlation of both unrestricted and restricted data. The process fused intelligence tools and methods through a police lens.

The ability of law enforcement and security forces to provide police information, critical criminal intelligence, and criminal investigations support is predicated on the ability to effectively organize within the resources available, fuse threat information, and direct actions to achieve desired effects. In order to achieve this, installations require a criminal intelligence analytical capability which can interact with the multitude of local, county, state, federal, and tribal law enforcement and all source intelligence agencies. By organizing effectively, using the operations and intelligence process, establishing relationships, and fusing all source threat information, garrisons and installations can sustain a COP for all threats.

Vignette: At 0345 hours, 6 March 2008, a bomb was detonated at the Times Square (New York City) Recruiting Station causing damage to the front of the facility. At the time of the bombing, law enforcement agencies were conducting an active investigation of three alleged anarchists with ties to France and Canada. Weeks prior to the bombing, a New York City Police Detective informed a member of the recruiting station of a possible threat. According to the Detective, during a vehicle search at the Canadian border, law enforcement officials discovered anarchist pamphlets along with photographs of Times Square, including several photographs appearing to show the Times Square Recruiting Station. No imminent threat to the Recruiting Station was ever identified. Moreover, the Detective informed the recruiter there was no direct threat to the Recruiting Station, but NYPD was increasing law enforcement presence in the area and would continue to monitor the situation. He also indicated the FBI and NYC JTTF were investigating the case. On 27 February 2008, the Times Square Recruiting Station Commander submitted an

official incident report to the United States Army Recruiting Command for situational awareness and implemented internal security and awareness measures. The report was forwarded as a Suspicious Activity Report (SAR) through AT/FP staff channels to four Army Commands and the Services for situational awareness (SA). There were no specific identified threats towards any particular location within the Times Square area of New York City. On 3 March 2008, USARNORTH received additional detailed Law Enforcement Sensitive information concerning the ongoing investigation from JTTF channels but held release of the information awaiting FBI approval for a redacted release of the information. Of concern was the fact that the report revealed the three individuals were actually stopped by Canadian law enforcement officials at the US-Canadian border on 31 January 2008, four weeks prior to the Times Square Recruiting Station being informed of the situation. Although there is no positive link between the initial suspicious activity report and the bombing investigation, and no known association between the vehicle stopped and searched at the Canadian border, the incident shows excellent cooperation and police intelligence sharing at the lowest levels.

MP/CID expeditionary forces maintain PIO expertise while supporting a safe and secure garrison environment. The garrison law enforcement mission supports a safe and secure environment, but also sustains critical warfighting skills for contingency operations. A garrison-based fusion cell can serve as a model and training venue for PIO expeditionary forces while at home station.

Organizing for Intelligence Fusion within the Garrison

Garrison headquarters require a criminal intelligence analytical capability. However large and wherever the capability resides within the garrison staff, the capability must support the installation commander's overall intelligence effort. Raw information as well as analysis and products must be fused from multiple sources and shared with the appropriate consumers. At garrisons with increased capabilities, a possible fusion cell composition may include MP, CID, DA Civilian Police, MI analyst (all source), and include reach-back support to the Army Counterintelligence Center (ACIC) and 902d Military Intelligence Group for criminal nexus.

A fusion cell located within the garrison staff provides a unique service that can address the complexities of the threat to a military community and installation and be an asset to the garrison and local civilian community. It has the ability to work closely with multiple local, federal, and DoD agencies. It does not have constraints that are emplaced on MI activities within the US, because it operates under the auspice and oversight of the police discipline and standards. At the garrison level, the fusion cell is static (non-deploying) which provides a level of continuity that allows for in-depth institutional knowledge of threat, physical and social environs, as well as long-term relationships with local and federal law enforcement agencies. A garrison fusion cell can also be a flexible analytical cell that can grow to form focused, ad hoc, threat-specific cells to address, prevent or react to a specific hazard.

Vignette: A Stryker Brigade Combat Team (SBCT) was preparing to move equipment to a port of embarkation (POE) for deployment. The shipment required the movement of 300 vehicles across eight law enforcement jurisdictions. Based on previous threat fusion expertise, the garrison's force protection (FP) fusion cell was uniquely qualified to be the lead intelligence producer to support the movement. The fusion cell coordinated police information, intelligence and civilian security with over 22 local, federal, and DoD agencies. The fusion cell produced in-depth analysis of the threat to the SBCT equipment and advised the SBCT and garrison commanders on protection. The coordinated effort gave law enforcement agencies the knowledge to identify and

prevent disruptive actions by violent protesters. The operation was considered by Corps leadership to be a watershed event for in-depth involvement of a garrison-based FP fusion cell in support of unit deployments. Moreover, the Corps headquarters integrated the fusion cell into other operations where the G2 is constrained by intelligence oversight rules, or there is a need for police information / intelligence assessments and analysis.

A fusion cell is valuable when separate data streams, information sources, or other disparate information from multiple organizations must be combined and analyzed in a coherent process to present a common operational picture for a decision maker. A fusion cell follows a network approach to integrate police and other information for the purpose of analyzing criminal information to target crime prevention/reduction and overall security. A fusion cell provides the installation commander a collaborative effort of two or more agencies that provide expertise, and information, with the goal of maximizing the ability to detect, prevent, apprehend and respond to criminal threats. The principal role of the fusion cell is to collect, analyze and exploit police information to anticipate, identify, prevent and/or monitor criminal activity.

In this post 9/11 era, relationships between Army garrisons and local, county, state, federal, tribal and host nation law enforcement and security agencies are greatly increased. Fusion cells are a conduit for implementing portions of the *National Criminal Intelligence Sharing Plan (*see DOJ/DHS *Fusion Center Guidelines* pamphlet, July 2005*)*. There is a deeper appreciation for the need to integrate military and civilian police intelligence and security activities. These efforts are visible during the planning and preparation of security for events both on and off the installation (i.e., ROTC programs, recruiting stations, military events in the local community, National Special Security Events). Because of the recognized and increased value of collaborative planning, substantial progress has been made to generate multi-jurisdictional threat-based assessments and analysis. Based on these joint assessments, interagency investigations have become more prevalent.

The increased interaction with the local community law enforcement and intelligence agencies expands the commanders' ability to understand the nature of the threat on and in the immediate vicinity of the garrison. It also allows commanders to establish risk management decision support structures for threat-based protection programs. From a power projection platform perspective, garrison commanders must see beyond the traditional boundaries of the installation. They must be postured to support the in-transit flow of expeditionary forces deploying for contingency operations.

Information Flow and Intelligence Fusion

Fusion is the practice of turning information and intelligence into actionable data that leaders and commanders can use to counter criminal threats. Fusion enables commanders to have a significant "see, decide and act" advantage over criminal networks, terrorist groups, cells, and individuals. Many activities produce observable data that human and electronic sensors detect. The combination of trained and experienced analysts, coupled with open information sharing agreements, and advances in technology allows agencies to process and analyze a variety of collected observables from different, but complementary systems, and more rapidly produce actionable intelligence for decision makers.

Level I fusion consumes uncorrelated single-source data and correlates that data for use in analysis or targeting. Level II fusion consumes correlated data and aggregates it for situational awareness. The intelligence professional seeks to provide decision makers with every advantage possible over his opponents. Knowledge and the ability to predict an adversary's next course of action allows commanders to act in a more agile manner and align forces and resources to better protect its assets.

Fusion acts as a critical enabler supporting current and future, joint, and Army concepts. The application of intelligence fusion impacts several operational imperatives and spans all echelons. Fusion must enable analysts to rapidly and accurately answer the commander's Priority Intelligence Requirements (PIR) and support the creation of the COP and the intelligence running estimate (IRE). Fusion supports battle command, achievement of desired effects, and feeds the commander's assessments while simultaneously supporting law enforcement.

Fusion takes place simultaneously at multiple echelons and across broad networks and organizations. No single sensor will be capable of collecting every bit of observable information. Commanders, leaders and staffs must reach out to multiple sources and organizations to gain access to all available data that can be used to paint a clear threat picture. The staff and analyst ability to provide intelligence, and the commander's ability to manage large amounts of information effectively, depend on the capabilities and processes established to fuse data and produce timely, concise, understandable, and accurate depictions of the operational environment.

The fusion model in figure 8 serves as a guide for analysts, garrison threat working groups and commanders. The fusion levels indicate information refinement; it does not imply a rigid, sequential process.

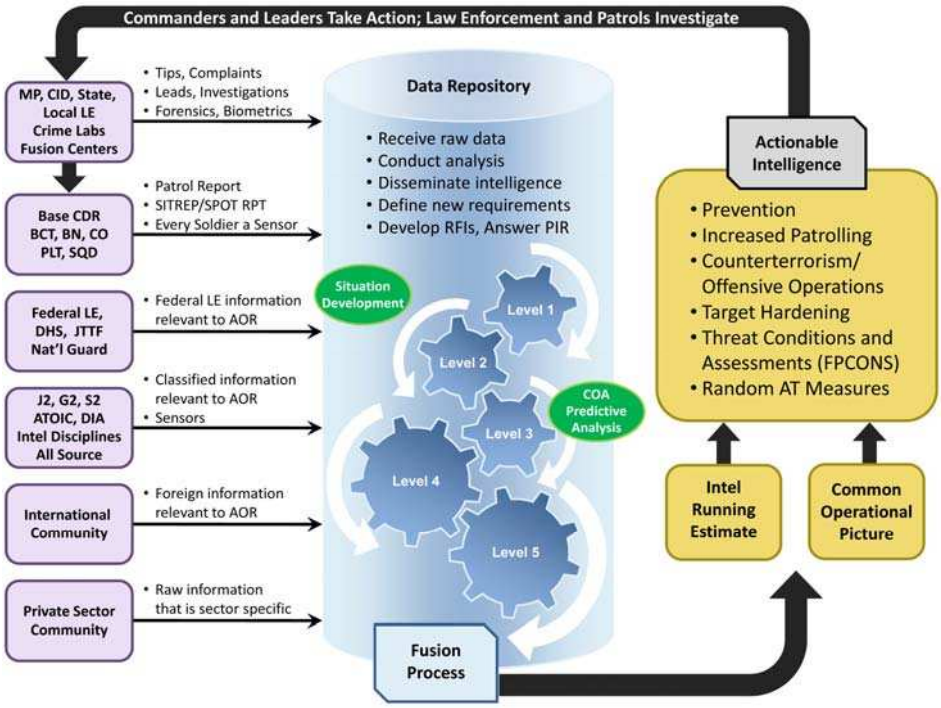


Figure 8 – The Intelligence Fusion Process

The COP is the current set of command and staff estimates, situation graphics, and other relevant data. As a consolidation of the best available information, the COP reduces the need for queries; forms the basis for discussions, plans, estimates and orders; and accelerates decision cycles. The staff uses shared mission focused information to present a tailored graphic display to the decision maker.

The COP is derived from a common database created from multi-information sources. As a shared reference, the COP provides the structure necessary to support visualization, and, as plans mature, shared situational understanding within the command. The IRE is a continuous flow and presentation of relevant information and predictive intelligence to the decision maker. The IRE requires constant verification to support situational understanding as well as predictive assessment for future operations.

Interagency collaboration through the use of the fusion process is consistent with national and military procedures and guidelines. Liaison personnel are instrumental in bridging gaps and issues between organizations. Successful collaboration depends on the following factors which are not all inclusive:

- Establish strong relationship networks
- Build mutual trust and respect for colleagues
- Share a common vision
- Minimize territorial issues
- Encourage continuous communication
- Eliminate impediments to information sharing

Vignette: Army criminal investigations special agents receive information from a source that an unknown subject is trafficking in large quantities of illegal drugs and selling them to a violent criminal organization operating in close proximity to an Army installation. The source reveals the method of transport, transfer locations, storage and distribution methods of the illegal narcotics. Coordination with local, state and federal law enforcement agencies reveals a prior criminal record and multiple police engagements with the subject and identifies the structure and individuals within the violent criminal organization. Analysis and fusion of newly developed police information, in conjunction with previously captured data by other civilian law enforcement agencies, links the subject with possible associates and the criminal network. The analysis identifies specific information gaps which, if answered, could associate key figures. The analysis leads to a targeted police information collection plan designed to gather additional information and document evidence to corroborate criminal activity and link specific crimes to a wider group, as well as implicate key leadership figures within the criminal organization. Army investigators, with the assistance and support of a violent crime task force, continue to investigate and collect the additional information needed. After the new information is entered into the crime database, further analysis reveals a pattern that allows analysts and investigators to link a foreign source to the drugs, ties illegal weapons smuggling to the criminal organization, and implicates three known criminals in multiple homicides. The result of the interagency investigation is the dismantling of a violent criminal organization and the arrest, prosecution and imprisonment of five high ranking members of the organized crime group. Further, over two

dozen other criminal associates were identified, leading to the initiation of several additional criminal investigations.

The fusion process works well for analyzing complex criminal organizations because it is constructed so there is no single point of failure. At the same time, it identifies and eliminates any unnecessary duplication of intelligence capabilities. The intelligence fusion process is applicable across the full spectrum of operations. Developed properly, the process can incorporate the capabilities of the national, international, and service intelligence organizations as well as the private sector, while simultaneously supporting the commander's common operational picture.

Additional Vignettes:

Vignette: The Puerto Rico Branch Office [3d MP Group (CID)], has geographic responsibility for the Caribbean. This is a large and diverse area, covered by only a few agents. As such, agents rely heavily upon a robust criminal intelligence network to police the area effectively. One of the agents developed a source working at the Fort Buchanan commissary. The commissary also has a large warehouse operation that has been plagued by failed efforts to automate the inventory. Initial analysis assumed warehouse workers were intentionally moving property pallets around after inventories, making it impossible to complete accurate daily counts of current stock. The source was targeted to collect information regarding warehouse operations. The source reported that a warehouse employee who had previously been on the day shift was moved to another shift following arguments with the supervisor. The employee told the source that the entire shift was involved in large scale theft from the warehouse. Drivers delivering items paid the shift supervisor in cash, and he in turn had employees load items the driver wanted onto their truck. The drivers then sold the item to local merchants for a reduced price. The supervisor split the illegal profits with the employees at the end of each day. After coordination with the FBI and the US attorney's office, the source agreed to wear a recording device to capture another conversation with the employee. The source later arranged a meeting between the employee and CID agents where the employee was confronted with the evidence against him and agreed to assist with the investigation after the Assistant US Attorney agreed to give him immunity from prosecution contingent on his cooperation. The employee was then presented to the Grand Jury where he detailed the magnitude of the theft scheme, which was operating undetected in the warehouse for 10 years. The grand jury handed down five indictments, and the asset forfeiture branch of the US attorney's office seized four houses which were purchased with the illegal proceeds.

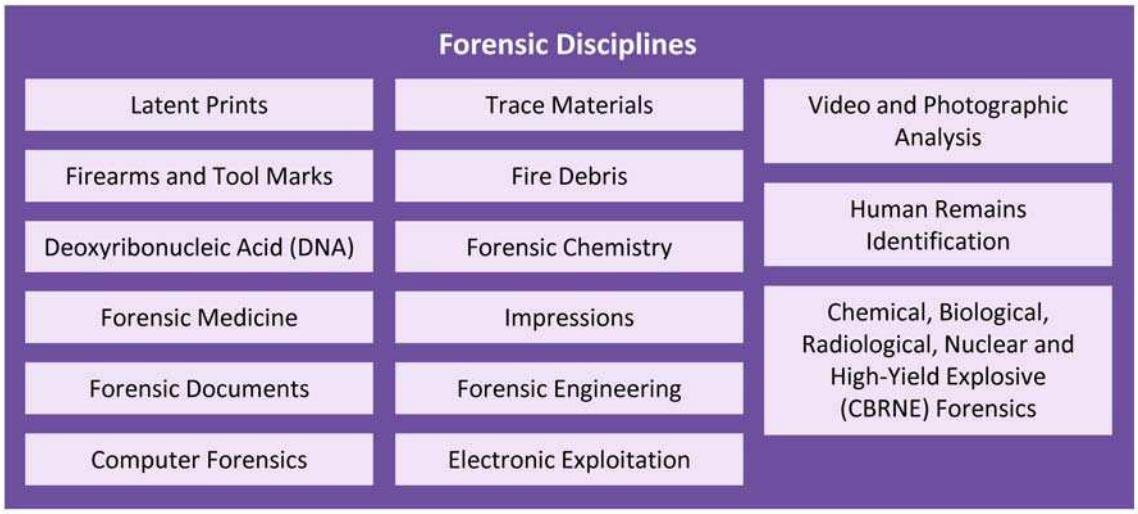
Vignette: A special agent at the Aberdeen Proving Ground Resident Agency received a request for assistance from an agent in Korea. The agent in Korea reported a general officer's identity was stolen through the officer's banking information. The agent set up a meeting with a security specialist from the bank. During the conversation the security specialist stated that he had worked on several cases involving senior military members dating back six months, and the bank corporate staff was trying to cover up the problem. He agreed to work as a source for the agent and provided an initial list of 127 senior ranking DoD officials who were victims of identity theft and provided the address where the cards were sent. The agent next coordinated with the US Postal Inspection Service (USPIS) who interviewed the local carrier and determined that he delivered hundreds of cards to a specific residence. The residence was currently abandoned, but USPIS provided identity information of the occupant. Since the victims spanned all branches of the military, coordination was conducted with Air Force Office of Special Investigations (AFOSI) and the Naval Criminal Investigative Service (NCIS). The AFOSI reported they discovered a web-

site where the names and social security numbers of 4,700 DoD officials were listed. Because the investigation was expanding, a Joint Investigative Task Force was formed with CID as lead agency. CID agents contacted the US Attorney's office, who wished to investigate and prosecute the case. The US Attorney's Office assisted in the formation of a task force which included all the military criminal investigative organizations, Social Security Administration, US Postal Inspection Service, the Internal Revenue Service, and the US Secret Service. A list of the compromised social security numbers was given to the bank, which produced a list of 11,000 potentially fraudulent accounts. CID agents then contacted the Regional Intelligence System Service (RISS) and provided the data from the bank. Through link analysis RISS was able to identify 32 identity theft rings operating in 26 states. The subsequent investigation resulted in numerous prosecutions and convictions.

6.5 Linking Police, Forensic and Biometric Information

One cannot overstate the unique relationship and importance of linking police information with forensic evidence and biometric data. By leveraging the capabilities of all three, criminal investigators are able to identify associations (people, places and things) based on scientific data and irrefutable evidence and produce actionable criminal intelligence.

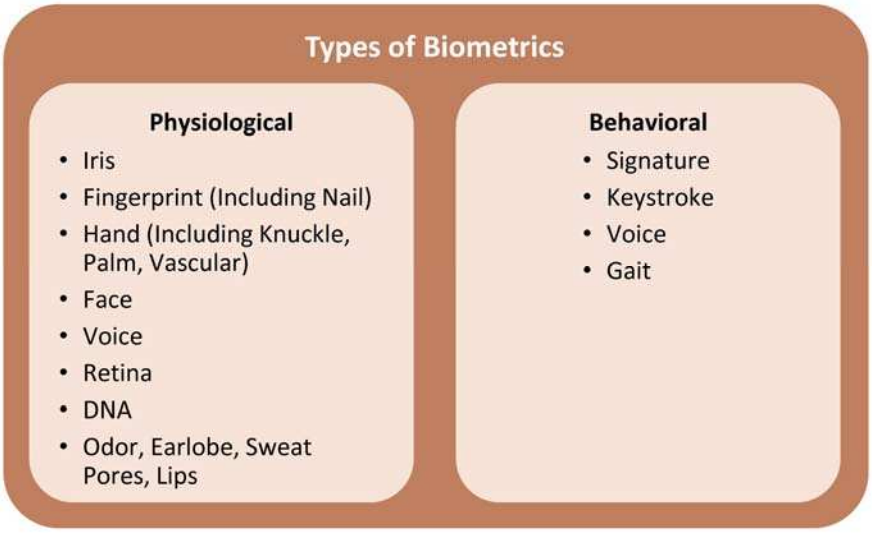
Forensics is the application of multi-disciplinary scientific processes to establish fact. Forensic functions recognize, preserve, collect, analyze, store and share information in the process of establishing fact. Forensic capabilities include, but are not limited to, the following disciplines:



Development and use of forensic information for policing is predicated on the understanding that:

- Crime is often networked, connected, and traceable
- Biometric data and forensic information can associate criminal activity
- Crime can be targeted from multiple angles and levels (activities, associations, funding, modus operandi, etc.)
- Crime reduction requires multi-agency collaboration and cooperation

Biometrics are measurable, physiological and/or behavioral characteristics that can be used to verify the identity of an individual. Types of biometrics include, but are not limited to:



PIO support for contingency operations hinges on the ability to "map" the population. Police map population demographics to provide positive identification, quantify population segments, identify changes in demographic patterns, associate persons with events and, ultimately, identify combatants from noncombatants. Mapping the population allows Army forces to conduct population control, track detainees, corroborate evidence, manage prosecutorial case files, target individuals, vet civil service recruiting, and establish accountability and registration programs (e.g., vehicle, weapons, national identity, etc.).

Vignette: An Army maneuver unit operating in Iraq developed a very good rapport with a local villager who they encountered regularly during patrols. While on one of their routine patrols, the villager approached the unit and provided information regarding the location of a possible enemy weapons cache. The patrol proceeded to the described location and discovered a buried cache containing weapons, currency and documents. The unit, previously trained on site exploitation (SE) and battlefield forensics, collected and processed the evidence as they were trained to do. Much of the evidence, to include the documents, was delivered to forensics units for analysis and exploitation. A single latent fingerprint lifted from one of the seized documents was sent to a stateside forensics laboratory where the fingerprint was run through a database for comparison and resulted in a match. This piece of evidence led to the identification, subsequent arrest and prosecution of the individual. Noteworthy is the fact that the original fingerprint on file at the stateside facility, and used for comparison, was submitted several years prior to the cache find by another maneuver unit as the result of a Biometrics Automated Toolset (BAT) record. During the intervening years, the individual became a high value target and was placed on several wanted lists.

7. Risks and Mitigation

Implementing this CONOPS incurs risks, which can be categorized into four areas: regulatory, operational conditions, information management, and force management. Developing a detailed approach to implementation and mitigation will reduce risk.

7.1 Regulatory

Execution and implementation of PIO principles, applications, measures and processes, and the desire to develop and exploit actionable intelligence, may create potential for increased concerns for intelligence oversight, accreditation and other regulatory issues. Coordinated doctrine, standards, capabilities, and solutions for Army PIO must be built on the foundation of applicable laws, regulations, policies and directives.

Legal Considerations

Legal considerations apply to MI gathering, sharing intelligence with civilian law enforcement agencies, commanders' authorizations, jurisdictions and use of force. An understanding of the threat can be achieved by collecting intelligence, both foreign and domestic. Collecting on American soil, or on American citizens, however, must be done in strict compliance with laws, directives, and regulations.

Primary intelligence policy documents include Executive Order 12333, Department of Defense Directive (DoDD) 5200.27, DoDD 5240.1, DoDD 5240.1-R, AR 381-10, and DoD Strategy for Homeland Defense and Civil Support.

- EXECUTIVE ORDER (EO) 12333 (US Intelligence Activities) authorizes the acquisition of intelligence to protect the United States and its interests with emphasis on guarding US persons' civil liberties. EO 12333 applies to all US departments and agencies that make up the intelligence community.
- DoDD 5200.27 (Acquisition of Information Concerning Persons and Organizations not Affiliated with the Department of Defense) establishes the general policy, limitations, procedures, and operational guidance pertaining to the collection, processing, storage, and dissemination of information concerning persons and organizations not affiliated with the DoD.
- DoD 5240.1 (DoD Intelligence Activities) applies to all intelligence activities of the DoD components but does not apply to authorized law enforcement activities carried out by the DoD intelligence components having a law enforcement mission.
- DoD 5240.1-R (Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons) addresses procedures governing the activities of DoD intelligence components that affect United States persons. These procedures permit DoD intelligence components to function effectively without jeopardizing US persons' constitutional rights and privacy.

AR 381-10 (US Army intelligence Activities) states MI may assist civilian and military law enforcement. However, it does not itself authorize intelligence activity. An Army element must first have the mission and authority to conduct the intelligence activity. This is assigned by other regulations. Nothing in the regulation is intended to authorize any US Army intelligence component to conduct activities or obtain approvals for activities that would not be in accordance with the procedures established in DoD 5240.1-R. ***Due to AR 381-10 restrictions on U.S. person information, consolidated (MI and criminal intelligence data) threat statements cannot be filed, stored or maintained as an intelligence product. These statements must be filed, stored and maintained within law enforcement or operations channels (i.e., Provost Marshal (PM), Director of Emergency Services (DES), USACIDC, DCSOPS/G-3/DPTMS).***

- Department of Defense Strategy for Homeland Defense and Civil Support (24 June 2005) centers on a layered defense integrating US capabilities globally. The layered defense applies to US territory, forward regions, air and maritime approaches to US territory, space and cyberspace. One of the strategy's five objectives is to achieve maximum awareness of threats accentuating the need for superior intelligence, which requires MI gathering on American soil and sharing intelligence with civilian law enforcement agencies.

According to AR 381-10, military intelligence may assist civilian law enforcement agencies for the following purposes:

- Investigating or preventing clandestine intelligence activities conducted by foreign powers, international narcotics organizations or international terrorist activities.
- Protecting DoD employees, information, property, facilities, and information systems.
- Preventing, detecting or investigating other violations of law.

Commanders' Authorization and Jurisdiction

When in Title 10 USC status, personnel engaged in law enforcement or security duties are governed by DoDD 5210.56. This directive authorizes DoD personnel to carry firearms while engaged in law enforcement or security duties, protecting personnel, vital Government assets, or guarding prisoners. It does not apply to DoD personnel engaged in military operations and subject to authorized rules of engagement.

Legal responsibility and authority for immediate response, containment, and resolution of security incidents is a command responsibility. Commanders have jurisdiction of their installations. Should an incident be assessed as an act of terrorism, the FBI, DOS or the HN will assume jurisdiction of area and personnel.

Jurisdiction of Personnel

- Jurisdiction of personnel generally follows the limitations of jurisdiction of the installation.
- MP forces have jurisdiction and authority over personnel as described in Army Regulation 190 series publications.

Intelligence Oversight

Intelligence oversight is a collection of policies and procedures designed to regulate and control the activity of intelligence functions and organizations. It is the body of law that balances the constitutional and privacy interests of Americans with the need for the federal government to conduct national foreign intelligence activities for national security purposes. It includes measures taken to ensure the conduct of intelligence activities conform to Executive Orders, DoD Directives, and Army regulations.

- Executive Order 12333, United States Intelligence Activities, stipulates that certain activities of intelligence components that affect US persons be governed by procedures issued at the Departmental or Agency level and approved by the Attorney General.
- AR 381-10, US Army Intelligence Activities, establishes the responsibility for intelligence activities concerning US persons, includes guidance on the conduct of intrusive intelligence collection techniques, and provides reporting procedures for certain federal crimes. AR 381-10 implements Executive Order 12333, the Crimes Reporting Memorandum of Understanding between the Department of Justice and Intelligence Community members, Department of Defense Directive 5240.1, DoD Regulation 5240.1-R, and DoD Instruction 5240.4. These regulations apply to the active Army, the Army National Guard (ARNG), and the US Army Reserve (USAR).

Civil Liberties

The United States Constitution states that the government should provide for the common defense of US citizens while also securing their liberties. One of the challenges is acquiring intelligence domestically without violating civil liberties.

- Executive Order 12333, United States Intelligence Activities, [as amended by Executive Orders 13284 (2003), 13355 (2004) and 13470 (2008)] states that the United States Government has a solemn obligation, and shall continue in the conduct of intelligence activities under this order, to protect fully the legal rights of all United States persons, including freedoms, civil liberties, and privacy rights guaranteed by federal law.
- According to the DoD Strategy for Homeland Defense and Civil Support, DoD will collect homeland defense threat information from relevant private and public sector sources, consistent with US constitutional authorities and privacy law. This means that Army intelligence components may collect US person information when the component has the mission or function to do so, and the information falls within one of the categories listed in DoD 5240.1-R and AR 381-10.

7.2 Operational Conditions

The Army must be capable of conducting PIO across a broad range of conditions. These conditions range from remote, austere operational sites under combat conditions, to peacekeeping missions, and operations supporting installations/fixed site and separate facilities in CONUS and OCONUS.

Emerging expeditionary operations add a unique set of variables. Variables include the operational environment, application of police information and criminal intelligence, time requirements, collaboration and sharing, legal issues, and the availability of resources.

The below characteristics of the Operational Environment (OE) are likely to have the most impact on future military operations:

- Competing cultures, civilizations, and associated ideologies
- The proliferation of information and communications technology
- Positive and negative implications of globalization
- The proliferation of weapons of mass destruction (WMD)
- Advancements in science, technology and engineering (ST&E)
- Increased resource constraints (energy, water, and sustainability issues)

The application of the PIO principles (collection, analysis and exploitation) must be flexible and adaptable to meet the needs of Commanders, while limiting unnecessary redundant capabilities and processes. To mitigate the risk of a narrowly focused approach to PIO, all branches, especially intelligence and maneuver branches, should be involved throughout the entire PIO capability development process. Moreover, commanders at all levels must understand the application of PIO as a mission enabler.

7.3 Information Management

The law enforcement, criminal investigative, and intelligence communities have unique processes, needs, and legal constraints for information that must be considered. These same constraints must be considered across the Army to ensure proper protocols for sharing, storing and using data and information. This may include conditions from remote, austere operational sites to installations or fixed site facilities in CONUS or OCONUS.

The protection of police and criminal data, especially US Persons information, must always be considered when developing operational processes. Collectors, investigators, and managers/commanders of police data must ensure that Information Assurance (IA) measures and standards are applied to their information systems. Managing and protecting data in a distributed network environment is necessary to protect privacy, security, and assets. It is critical to protect the integrity and availability of individual identity and criminal files, maintain the credibility of the authoritative source, and safeguard data utility. The information must be available to the end user at the appropriate classification level. A comprehensive data architecture and information management plan must be developed in accordance with applicable policy, such as DoD Regulation 5240.1-R, Procedures Governing the Activities of DoD Intelligence Components That Affect United States Persons.

As the Army leverages biometrics and forensics information capabilities in support of PIO, it will likely continue to see increased interaction and information sharing. It is therefore vital that all involved communicate effectively using similar terminology. Those involved might include people

from the Intelligence, scientific and law enforcement communities, as well as other government agencies, both domestic and international.

7.4 Force Management

The establishment of improved PIO capabilities will demand the Army revisit force structure planning and projections. The increased use of PIO capabilities on the battlefield or during any contingency operation, and increased interagency/host nation collaboration in garrison, could significantly strain an already high-demand, low-density skill set. These manpower issues must be addressed as early as possible to support necessary force development.

Necessary training and education must be in place across the scope of PIO functions in order to generate the expertise required from individual Soldiers to criminal analysts and commanders/decision makers. In order to effectively leverage PIO, doctrine, policy, and education on the capabilities, limitations, and uses of PIO should be incorporated throughout the force. Training and education must account for increased linkages to biometrics and forensic capabilities.

8. DOTMLPF Implications

It is only through the proper integration of Police Intelligence Operations DOTMLPF capabilities that the Army will fully implement and enable PIO concepts and principles. Police Intelligence Operations have implications across all the DOTMLPF domains, as shown below.

8.1 Doctrine

- Update doctrine to drive change across all DOTMLPF domains.
- Revise Field Manual (FM) 3-19.50, "Police Intelligence Operations" (July 2006) to reflect current principles, concepts, processes and applications from this CONOPS and strengthen the linkage to FM 3-19.13 (Law Enforcement Investigations) and FM 3-19.10 (Law and Order Operations).
- Develop a new doctrinal manual for the Army on Criminal Intelligence Analysis.
- Incorporate PIO principles, concepts, processes and applications into the series of FM 3-0 (Operations), series of FM 2-0 (Intelligence), and the family of MP doctrinal manuals such as FM 3-19 (Military Police Operations), FM 3-19.10 (Military Police Law and Order Operations), and FM 3-19.40 (Internment/Resettlement Operations).
- Standardize the PIO definition across all Army doctrinal publications including the definitions in FM 7-15, The Army Universal Task List (AUTL) and FM 1-02, Operational Terms and Graphics.
- Define and describe criminal intelligence (CRIMINT) as it relates to the other "INTS" (HUMINT, IMINT, SIGINT, MASINT) within FM 2-0.
- Determine the utility of adopting the CITF's A-3 model as a standard within the Army.
- Establish minimum standards for intelligence analysis (on par with the International Association of Law Enforcement Intelligence Analysts) to ensure products are accurate, timely, factual and relevant.
- Integrate throughout Army doctrine the need to inculcate basic evidence training and battlefield forensics (crime scene preservation & collection) for all Soldiers.

8.2 Organization

- Maneuver units (BCT and above) require the ability to integrate criminal intelligence analytical capabilities and police investigative capabilities into their operations, intelligence and decision making processes. This capability does not need to be organic (i.e., TOE) to the maneuver unit as long as supporting MP/CID structure includes the capability, an appropriate and documented Rule of Allocation (ROA), and an established habitual deployment relationship.

- Deployable forensics labs (i.e. JEFFs) require staffs that possess all analytical capabilities (i.e., CEXC, DOCEX, etc.).
- Garrison headquarters require a criminal intelligence analyst and police investigations capability integrated or available to the commander. This capability does not need to be organic to the garrison as long as supporting MP/CID structure includes the capability and an established habitual relationship.
- The Army and/or Department of Defense should consider developing an enduring organization that combines the capabilities of the Law Enforcement Professional Program (LEPP) with the capabilities of the Criminal Investigation Task Force (CITF) capable of expeditionary operations.

8.3 Training

- A training course is required to provide noncommissioned officers, warrant officers, officers, and DA civilians with the ability to conduct the full array of crime and criminal intelligence analytical operations and to generate associated products [Crime and Criminal Intelligence Analysts Course – currently under development at USAMPS].
- A training course is required to provide noncommissioned officers, warrant officers, officers, and DA civilians with the skills required to serve as an investigative member within a Crime and Criminal Analysis Unit. [Police Intelligence Collection Course – currently under development at USAMPS].
- A training course is required to provide Commanders and Staff Officers that manage PIO assets (including BCT commanders/staff, provost marshals, MP leaders, and Directors of Emergency Services) knowledge of the PIO process, how it is employed, and how they can leverage PIO capabilities. [Commander and Staff Police Intelligence Management Course – currently under development at USAMPS].
- All programs of instruction (POI) and training support packages (TSP) across MP functions must be updated to reflect current PIO doctrine.
- The USAMPS OIF Police Transition Team and OEF Police Mentor Team TSPs must be updated to integrate current PIO doctrine.
- Training must be centralized on standardized hardware, software and information databases.
- Inculcate basic evidence collection and battlefield forensics training (crime scene preservation & collection) for all Soldiers and all military occupational specialties.
- Develop PIO training products to support unit pre-deployment training at home station, combat training centers (CTC) and post-mobilization training sites.

8.4 Materiel

- Establish a centralized, standardized, universal database (with back-up) which is accessible, searchable, intuitive, interactive, shareable, and has warehousing capability. The database must be fully compatible with, and able to fully interface with the other MI database systems

so that PIO information and intelligence can be readily shared with and fused with information and intelligence from MI.

- Establish integrated hardware, software and network capabilities that are compatible with other DoD Services.
- Create standardized hardware/software for analytical processes and products.
- Create PIO information system capabilities that are compatible with (or part of) the Distributed Common Ground System – Army (DCGS-A). This system must also be compatible with Centralized Operations Police Suite (COPS) database.
- Link the Handheld Interagency Identity Detection Equipment (HIIDE) to Force XXI Battle Command Brigade & Below (FBCB2) and Blue Force Tracker (BFT).
- Make the system compatible for interaction with forensic and biometric databases.
- Increase connectivity between the Detainee Management System (DMS) and the Biometrics Automated Toolset (BAT).

8.5 Leader Development

- Both maneuver and garrison commanders require education and training on the employment of criminal intelligence analytical and investigative capabilities [Commander and Staff Police Intelligence Management Course – currently under development at USAMPS].
- Add PIO awareness and understanding as a learning objective during BCT Pre-Command Courses (Fort Leavenworth, KS), BSTB Pre-Command Courses (Fort Leonard Wood, MO), and MANSCEN-consolidated Pre-Command Courses (Fort Leonard Wood, MO).
- Establish new opportunities and partnerships with leading academic and law enforcement institutions to expand and grow professional development for noncommissioned officers, warrant officers, officers, and DA civilians, specifically within the realm of criminal intelligence and analysis.

8.6 Personnel

- Garrison staffs require a criminal intelligence analytical capability. This capability does not need to be organic to the garrison as long as supporting MP/CID structure includes the capability, an appropriate and documented Rule of Allocation (ROA), and an established habitual deployment relationship.
- MP expeditionary units (MP/CID Detachment, MP Company, MP/CID Battalion, and MP/CID Brigade or Group) require a criminal intelligence analytical capability.
- MP units (MP/CID Detachment, MP Company, MP/CID Battalion and MP/CID Brigade or Group) require an increased police investigations capability.
- The Installation Director of Emergency Services / Provost Marshal requires access to an increased police investigations capability to support law and order.

- Garrison Commanders require access to increased criminal intelligence analysis capability to support law and order.
- Foreign language linguist capabilities must be sufficient in capacity, must be trained and skilled in their task, and must be readily available to MP/CID to support interviews and investigations.

8.7 Facilities

- Establish suitable organizational facilities to support an enduring Criminal Investigation Task Force (CITF) type capability.
- Establish suitable training facilities to support increased student course loads across all training programs discussed above.

8.8 Policy Implications

Coordinated doctrine, standards, capabilities, and solutions for Army PIO must be built on the foundation of applicable laws, regulations, policies and directives. The MP and intelligence community must be involved in the planning, development, and application of Army doctrine and any evolving policy implications. For example, despite a movement toward joint basing, currently DOD and Joint guidance does not mandate unity of effort for investigations, crime reporting and collection/sharing of criminal intelligence. However, in some instances, pooling of resources and intelligence sharing (within legal constraints) may enhance the overall policing effort for a specific geographic location. Currently, differences in service component police and criminal reporting systems and procedures prevent effective use of resources and implementation of policing strategies.

Appendix 1 – References

The following references are of use in understanding the concepts, processes and applications used in this Concept of Operations (CONOPS).

- FM 1, *The Army*, 14 June 2005.
- FM 1-02, *Operational Terms and Graphics*, September 2004.
- FM 2-91.4, *Intelligence Support to Urban Operations,* 20 March 2008.
- FM 3-0, *Operations*, February 2008.
- FM 3-24, *Counterinsurgency*, December 2006.
- FM 3-19.1, *Military Police Operations*, 22 March 2001.
- FM 3-19.13, *Law Enforcement Investigations*, 1 October 2005.
- FM 3-19.50, *Police Intelligence Operations*, 21 July 2006.
- FM 5-0, *Army Planning and Orders Production*, January 2005.
- FM 5-0.1, *The Operations Process*, 21 March 2006.
- FM 7-15, *The Army Universal Task List*, August 2003.
- FM 34-130, *Intelligence Preparation of the Battlefield*, 8 July 1994.
- Executive Order 12333, US Intelligence Activities, 4 December 1981.
- DoDD 5200.27, *Acquisition of Information Concerning Persons and Organizations not Affiliated with the Department of Defense*, 7 January 1980.
- DoD 5240.1, *DoD Intelligence Activities*, 25 April 1988.
- DoD 5240.1-R, *Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons*, December 1982.
- AR 381-10, *US Army intelligence Activities*, 1 July 1984.
- AR 190-14, *Carrying of Firearms and Use of Force for Law Enforcement and Security Duties*, 12 March 1993.
- AR 195-2, *Criminal Investigation Activities*, 30 October 1985.
- AR 195-3, *Acceptance, Accreditation, and Release of US Army Criminal Investigation Command Personnel*, 22 April 1987.
- DoD Regulation 5200.1-R, *Information Security Program*, 14 January 1997.
- DoD Directive 5230.11,*Disclosure of Classified Military Information to Foreign Governments and International Organizations*, 16 June 1992

- DoD Directive 3115.09, *DoD Intelligence Interrogations, Detainee Debriefings, and Tactical Questioning*, 3 November 2005.
- CJCSM 3500.4D, *Universal Joint Task List*, 1 August 2005.
- *Department of Defense Protection Joint Functional Concept*, June 2004.
- *Capstone Concept for Joint Operations,* Version 2.0, August 2005.
- CJCSI 3010.02B, *Joint Operations Concepts (JOpsC) Development Process*, January *27, 2005.*
- DOD Directive 3000.05, *Military Support for Stability, Security, Transition, and Reconstruction (SSTR) Operations,* November 28, 2005.
- *Department of Defense Major Combat Operations Joint Operating Concept*, Version 1, September 2004.
- Joint Chiefs of Staff, *Joint Functional Concept for Battlespace Awareness*, 31 October 2003.
- Joint Pub 1-02, *Dictionary of Military and Associated Terms*, 31 August 2005.
- Stability Operations Joint Operating Concept, Version I, September 2004.
- TRADOC Pamphlet 525-66, *Force Operating Capabilities*, 1 July 2005.
- Department of Defense, *Capstone Concept of Operations for DoD Forensics*, 8 July 2008.

Appendix 2 – Glossary

The following list provides definitions for key terms used in this Concept of Operations (CONOPS).

Adversary. A party acknowledged as potentially hostile to a friendly party and against which the use of force may be envisaged. (FM 3-0 / JP 3-0)

Analysis (Intelligence). The process by which collected information is evaluated and integrated with existing information to produce intelligence that describes the current, and predicts the future, impact of the threat and/or environment on operations. (FM 34-3)

Coalition. An ad hoc arrangement between two or more nations for common action. (FM 3-0 / JP 5-0)

Biometric. Measureable physical characteristic of personal behavior trait used to recognize the identity or verify the claimed identity of an individual. (JP-02)

Biometrics. The process of recognizing and individual based on measureable anatomical, physiological, and behavioral characteristics. (JP-02)

Collecting. An activity of information management: the continuous acquisition of relevant information by any means, including direct observation, other organic resources, or other official, unofficial, or public sources from the information environment. (FM 1-02)

Collection Plan. A plan for collecting information from all available sources to meet intelligence requirements and for transforming those requirements into orders and requests to appropriate agencies. (FM 1-02)

Combatant Command (COCOM). Nontransferable command authority established by title 10 ("Armed Forces"), United States Code, section 164, exercised only by commanders of unified or specified combatant commands unless otherwise directed by the President or the Secretary of Defense. Combatant command (command authority) cannot be delegated and is the authority of a combatant commander to perform those functions of command over assigned forces involving organizing and employing commands and forces, assigning tasks, designating objectives, and giving authoritative direction over all aspects of military operations, joint training, and logistics necessary to accomplish the missions assigned to the command. Combatant command (command authority) should be exercised through the commanders of subordinate organizations. Normally this authority is exercised through subordinate joint force commanders and Service and/or functional component commanders. Combatant command (command authority) 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 (command authority). (FM 3-0 / JP 1)

Commander's Critical Information Requirements (CCIR). An information requirement identified by the commander as being critical to facilitating timely decision making. The two key elements are friendly force information requirements and priority intelligence requirements. (FM 3-0 / JP 3-0)

Concept of Operations. A statement that directs the manner in which subordinate units cooperate to accomplish the mission and establishes the sequence of actions the force will use to achieve the end state. It is normally expressed in terms of decisive, shaping, and sustaining operations. (FM 3-0)

Criminal Analysis. Criminal analysis is the application of analytical methods and products to raw data that produces intelligence within the criminal justice field. (Law Enforcement Analytic Standards, U.S. Department of Justice Office of Justice Programs, NOV 04)

Criminal Intelligence (CRIMINT). Law enforcement information derived from the analysis of information collected through investigations, forensics, crime scene and evidentiary processes to establish intent, history, capability, vulnerability, and modus operandi of threat and criminal elements. (AR 525-13)

Crime-Pattern Analysis. A process that looks for links between crimes and other incidents to reveal similarities and differences that can be used to help predict and prevent future criminal activity. (Law Enforcement Analytic Standards, U.S. Department of Justice, Office of Justice Programs, NOV 04)

Data. Representation of facts, concepts, or instructions in a formalized manner suitable for communication, interpretation, or processing by humans or by automatic means. Any representations such as characters or analog quantities to which meaning is or might be assigned. (FM 1-02)

Database. Information that is structured and indexed for use access and review. (Capstone CONOPS for DoD Forensics)

Detainee. An individual who is captured by or placed in the custody of a duly constituted governmental organization for a period of time. (FM 34-52)

Detention Operations. Operations that involve taking into custody, maintaining, protecting, and accounting for all categories of detainees who are a threat to U.S. forces, 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. (Capstone CONOPS for DoD Forensics)

Exploitation. Taking full advantage of any information that has come to hand for tactical, operational or strategic purposes. (JP 1-02)

Forensics. The application of multi-disciplinary scientific processes to establish fact. (Capstone CONOPS for DoD Forensics)

Homeland Defense. The protection of US sovereignty, territory, domestic population, and critical infrastructure against external threats and aggression or other threats as directed by the President. (JP 3-26)

Homeland Security. A concerted national effort to prevent terrorist attacks within the United States, reduce America's vulnerability to terrorism, and minimize the damage and recover from attacks that do occur. (JP 3-26)

Host Nation (HN). A nation that receives the forces and/or supplies of allied nations, coalition partners, and/or NATO organizations to be located on, to operate in, or to transit through its territory. (FM 3-07)

Informant (Source). 1. A person who, wittingly or unwittingly, provides information to an agent, a clandestine service, or the police. 2. In reporting, a person who has provided specific information and is cited as a source. (FM 1-02 / FM 6-0)

Information Requirement. All information elements the commander and staff require to successfully conduct operations, that is, all elements necessary to address the factors of METT-TC. (FM 1-02 / FM 6-0)

Intelligence. 1. The product resulting from the collection, processing, integration, analysis, evaluation, and interpretation of available information concerning foreign countries or areas. 2. Information and knowledge about an adversary obtained through observation, investigation, analysis, or understanding. (FM 2-91.4 / JP 2-0)

Intelligence Cycle. The process by which information is converted into intelligence and made available to users. (FM 1-02)

Intelligence-led Policing. The collection and analysis of information to produce an intelligence end product, designed to inform police decision making at both the tactical and strategic levels. (Law Enforcement Analytic Standards, U.S. Department of Justice Office of Justice Programs, NOV 04)

Intelligence Preparation of the Battlefield (IPB). The systematic, continuous process of analyzing the threat and environment in a specific geographic area. Intelligence preparation of the battlefield is designed to support the staff estimate and military decision-making process. Most intelligence requirements are generated as a result of the IPB process and its interrelation with the decision making process. (FM 2-91.4 / FM 34-130)

Intelligence Process. The process by which information is converted into intelligence and made available to users. The process consists of six interrelated intelligence operations: planning and direction, collection, processing and exploitation, analysis and production, dissemination and integration, and evaluation and feedback. (JP 2-01)

Interagency Coordination. Within the context of Department of Defense involvement, the coordination that occurs between elements of Department of Defense and engaged U.S. Government agencies for the purpose of achieving an objective. (FM 3-0 / JP 3-0)

Joint Force. A general term applied to a force composed of significant elements, assigned or attached, of two or more Military Departments, operating under a single joint force commander. (FM 3-0)

Law Enforcement (Police) Intelligence. The collection and analysis of information to produce an intelligence end product designed to inform law enforcement decision making at both the tactical and strategic levels (National Criminal Intelligence Sharing Plan, Office of Justice Programs, WASH DC)

Operational Environment (OE). A composite of the conditions, circumstances, and influences that affect the employment of capabilities and bear on the decisions of the commander. (FM 3-0 / JP 3-0)

Operations Process. The major command and control activities performed during operations: planning, preparing, executing, and continuously assessing the operation. The commander drives the operations process. (FM 3-0)

Police Information. The products from the collection, analysis, and interpretation of all available information concerning known and potential enemy and criminal threats and vulnerabilities of support organizations. It involves intelligence preparation of the battlefield, criminal intelligence preparation of the battlefield, and the police information assessment process. (FM 1-02)

Police Intelligence Operations (PIO). PIO is the military police integrating function that supports the operations and intelligence processes through the inclusion of police engagement, police information collection, and police investigations to enhance situational understanding, battlefield visualization and protection, to focus policing operations and support social order (Rule of Law).

Priority Intelligence Requirements (PIR). An intelligence requirement stated as a priority for intelligence support, that the commander and staff need to understand the adversary or the operational environment. (FM 3-0 / JP 2-0)

Processing (Intelligence). A system of operations designed to convert raw data into useful information. (JP 1-02)

Production (Intelligence). Conversion of information into intelligence through the integration, analysis, evaluation, and interpretation of all-source data and the preparation of intelligence products in support of known or anticipated user requirements. (FM 2-0)

Raw Data. Data that is collected by officers or analysts that has not yet been subjected to the intelligence process and thus is not intelligence. (Law Enforcement Analytic Standards, U.S. Department of Justice, Office of Justice Programs, NOV 04)

Rule of Law (RoL). A principle under which all persons, institutions, and entities, public and private, including the state itself, are accountable to laws that are publicly promulgated, equally enforced, and independently adjudicated, and that are consistent with international human rights principles. (FM 3-07)

Specific Information Requirement (SIR). A complete SIR describes the information required, the location, where the information can be collected, and the time during which it can be collected.

Specific Orders or Requests (SOR). Orders or requests given to subordinate or supporting commands, which include breaking down a Specific Information Requirement into questions that can be easily understood and reported.

Stability Operations. An overarching term encompassing various military missions, tasks, and activities conducted outside the United States in coordination with other instruments of national power to maintain or reestablish a safe and secure environment, provide essential governmental services, emergency infrastructure reconstruction, and humanitarian relief. (JP 3-0)

Vignette. A concise narrative description that illustrates and summarizes pertinent circumstances and events from a scenario. (Capstone CONOPS for DoD Forensics)

Appendix 3 – Acronyms

A3	Agent, Analyst and Attorney (CITF investigative model)
ACIC	Army Counterintelligence Center
AFOSI	Air Force Office of Special Investigations
AO	Area of Operations
AQI	Al Qaida in Iraq
ASI	Additional Skill Identifier
AUTL	Army Universal Task List
BAT	Biometrics Automated Toolset
BCT	Brigade Combat Team
BFT	Blue Force Tracker
CA	Civil Affairs
CBRNE	Chemical, Biological, Radiological, Nuclear and High-yield Explosives
CCIR	Commander's Critical Information Requirements
CEXC	Combined Explosives Exploitation Cell
CID	Criminal Investigation Command
COA	Course of Action
CONOPS	Concept of Operations
CONUS	Continental United States
COP	Common Operational Picture
CRIMINT	Criminal Intelligence
CTC	Combat Training Center
DA	Department of the Army
DCGS-A	Distributed Common Ground System-Army
DES	Director of Emergency Services

DHA	Detainee Holding Area
DMS	Detainee Management System
DNA	Deoxyribonucleic Acid
DO	Detention Operations
DOCEX	Document Exploitation
DoD	Department of Defense
DOTMLPF	Doctrine, Organization, Training, Materiel, Leader Development, Personnel and Facilities
DPTMS	Director of Plans, Training, Mobilization and Security
DSCA	Defense Support to Civil Authorities
EFP	Explosively Formed Penetrator
FBCB2	Force XXI Battle Command Brigade & Below
FP	Force Protection
FSO	Full Spectrum Operations
HD	Homeland Defense
HIIDE	Handheld Interagency Identity Detection Equipment
HME	Homemade Explosive
HN	Host Nation
HTT	Human Terrain Team
HUMINT	Human Intelligence
IA	Information Assurance
IALEIA	International Association of Law Enforcement Intelligence Analysts
IED	Improvised Explosive Device
IMINT	Imagery Intelligence
IPB	Intelligence Preparation of the Battlefield
IR	Information Requirement

IRE	Intelligence Running Estimate
ISR	Intelligence, Surveillance and Reconnaissance
IW	Irregular Warfare
JEFF	Joint Expeditionary Forensic Facility
JIEDDO	Joint Improvised Explosive Device-Defeat Organization
JIM	Joint, Interagency, and Multinational
JOC	Joint Operating Concept
LE	Law Enforcement
LEP	Law Enforcement Professional
LEPP	Law Enforcement Professional Program
MASINT	Measurement and Signatures Intelligence
MCO	Major Combat Operations
MI	Military Intelligence
MP	Military Police
NCIS	Naval Criminal Investigative Service
NGO	Non-Governmental Organization
OCONUS	Outside Continental United States
OE	Operational Environment
OEF	Operation Enduring Freedom
OGA	Other Government Agencies
OIF	Operation Iraqi Freedom
OPLAN	Operation Plan
OPORD	Operation Order
PIO	Police Intelligence Operations
PIR	Priority Intelligence Requirements
PMT	Police Mentorship Team

PMO	Provost Marshal Office
POD	Port of Debarkation
POI	Program of Instruction
POLICE	Police/prison, Organized crime, Legal systems, Investigations, Crime conducive conditions, Enforcement mechanisms and gaps
PSYOP	Psychological Operations
PTT	Police Transition Team
RISS	Regional Intelligence System Service
RoL	Rule of Law
SBCT	Stryker Brigade Combat Team
SIGINT	Signals Intelligence
SIR	Specific Information Requirements
SJA	Staff Judge Advocate
SOR	Specific Orders and Requests
SSTRO	Security and Stability Transition and Reconstruction Operations
TDA	Table of Distribution and Allowances
THT	Tactical HUMINT Team
TIF	Theater Internment Facility
TOE	Table of Organization and Equipment
TSP	Training Support Package
TTP	Tactics, Techniques and Procedures
USACIDC	United States Army Criminal Investigation Command
USCENTCOM	United States Central Command
USPIS	United States Postal Inspection Service
WMD	Weapons of Mass Destruction