ATP 3-39.20

Police Intelligence Operations

April 2015

Headquarters, Department of the Army

***ATP 3-39.20 (ATTP 3-39.20)**

Army Techniques Publication
No. 3-39.20

Headquarters
Department of the Army
Washington, DC, 6 April 2015

Police Intelligence Operations

Contents

*This publication supersedes ATTP 3-39.20, 29 July 2010.

Figures

Tables

Preface

ATP 3-39.20 is aligned with FM 3-39, the Military Police Corps Regiment foundational publication. It provides guidance for commanders and staffs on police intelligence operations (PIO). PIO is an integrated military police function that supports the operations process and protection supporting tasks by providing police information and police intelligence to enhance situational understanding, protect the force, and assist homeland security. This publication emphasizes that PIO collects, analyzes, integrates, and portrays relevant criminal threats and police intelligence that may affect the operational environment. The military police, the United States Army Criminal Investigation Command (USACIDC), and Soldiers gather information as they conduct operations throughout the operational area. PIO supports tasks of decisive action (offensive, defensive, and stability or defense support of civil authorities).

This publication is written for military police and USACIDC Soldiers and civilians conducting police intelligence. This publication focuses on establishing the framework of police intelligence, establishing how police intelligence supports military police and Army operations, and establishing how to integrate police intelligence within the three military police disciplines (police operations, detention operations, and security and mobility support). This publication describes PIO executed across the range of military operations and operational environments, with specific emphasis on the integration of police intelligence into the operations process and its integrating processes.

The principal audience for ATP 3-39.20 is Army leaders and Army professionals at all echelons tasked with planning, directing, and executing PIO. Trainers and educators throughout the Army will also use this publication.

Commanders, staffs, and subordinates ensure that their decisions and actions comply with applicable United States (U.S.), international and, in some cases, host nation laws and regulations. Commanders at all levels ensure that their Soldiers operate according to the law of war and the rules of engagement. (See FM 27-10.)

Unless stated otherwise, masculine nouns or pronouns do not refer exclusively to men.

ATP 3-39.20 uses joint terms where applicable. Selected joint and Army terms and definitions appear in both the glossary and the text. For definitions shown in the text, the term is italicized and the number of the proponent publication follows the definition. This publication is not the proponent for any Army terms.

ATP 3-39.20 applies to Active Army, Army National Guard/Army National Guard of the United States, U.S. Army Reserve unless otherwise stated.

The proponent of ATP 3-39.20 is the U.S. Army Military Police School. The preparing agency is the Maneuver Support Center of Excellence (MSCoE) Capabilities Development and Integration Directorate; Concepts, Organizations, and Doctrine Development Division; Doctrine Branch. Send comments and recommendations on DA Form 2028 (*Recommended Changes to Publications and Blank Forms*) to Commander, U.S. Army Maneuver Support Center of Excellence, ATTN: ATZT-CDC, 14000 MSCoE Loop, Suite 270, Fort Leonard Wood, MO 65473-8929; by e-mail to <usarmy.leonardwood.mscoe.mbx.cdidcodddmpdoc@mail.mil>; or submit an electronic DA Form 2028.

Introduction

Police intelligence has been included in U.S. Army military police doctrine since the 1960s. The principles have generally remained the same; military police collect police information pertaining to individuals, activities, or locations where military police have an interest. Police intelligence is the analysis of that information into a meaningful pattern to predict illegal, criminal, or subversive activities so that military police (or other forces) may plan and prepare for a required action. PIO is easily associated with law enforcement and police operations in support of bases and base camps. For many years, military police leaders relegated PIO to USACIDC personnel and select military police Soldiers who were trained to recognize associations and identify patterns and trends. With the emergence of hybrid threats, more and more often, belligerents are using criminal techniques of organized criminal networks to conduct attacks against the United States, their allies, and their interests. Countering this hybrid threat involves police information collection and analysis, which increasingly demonstrates the need for PIO. The law enforcement and investigative skills that military police and USACIDC Soldiers employ while conducting law enforcement on bases and base camps have made them a valuable asset for police information collection and analysis in the modern operational environment.

Police intelligence drives military police activities across the range of military operations and greatly enhances the situational understanding of maneuver commanders. The conversion of the five military police functions to the three military police disciplines better depicts PIO as an integrated function throughout military police operations.

This publication builds on the experiences of military police and USACIDC forces over the past decade of conflict. The lessons learned from these and other experiences serve as invaluable tools to expand the understanding, appreciation, and complete application of PIO as an integrated function of the Military Police Corps Regiment that supports activities of decisive action. PIO is not solely applicable to law enforcement and criminal investigations. PIO encompasses the continuous analyses and production by military police and USACIDC personnel; information collected by military police, USACIDC, and others; and subsequent dissemination of police information and police intelligence (as appropriate) to police agencies, other military units, and the Army intelligence community. Soldiers conducting military police activities (in any of the three disciplines) collect police information for further analysis.

Military police analysts are referred to as police intelligence analysts, and USACIDC analysts are referred to as criminal intelligence analysts (due to the focused criminal investigative mission of USACIDC) after completing the Crime and Criminal Intelligence Analyst Course at the U.S. Army Military Police School. For the purpose of brevity in this publication, police intelligence analyst is used to refer to a military police analyst or USACIDC analyst.

Military police leaders must be able to articulate the value of PIO to maneuver commanders so that they may recognize the effectiveness and value of PIO products and their contributions to mission success. The expansion of PIO capabilities (to include the recent introduction of USACIDC personnel, law enforcement professionals, biometrics, and expeditionary forensic laboratories) has contributed to the success of PIO by providing valuable police intelligence to attack insurgents and other organized criminal networks. Formerly static and primarily positioned in the continental United States, reachback capabilities (such as the Defense Forensics Science Center) are now providing modular elements in-theater, thus ensuring expedient and dedicated analyses. These analyses are available to support evidence or potential evidence for use in criminal cases and to support targeting by conventional forces.

PIO focuses the collection efforts of military police formations to ensure that the proper police information is collected and forwarded. At times, this collection effort will be in response to a specific requirement from a commander's request to address an enemy course of action. A specific requirement may include a priority intelligence requirement (PIR) or intelligence requirement. At other times, information will come directly from an investigation or event without any preconception of its value. This information feeds into the operations process and the commander's targeting cycle. This process enables informed decisionmaking and the targeting of people, groups, and networks for lethal and nonlethal effects; and it depends on the commander's assessment

and the selected engagement method. Targets may be identified for further informational exploitation as conduits to attack an enemy, criminal, or terrorist network. Sometimes, PIO results in a prosecution in a court of law. If the prosecution takes place in an emerging democracy, it shows the people of that nation the value of a professional police force that operates within the rule of law. PIO activities also provide information critical to determining measures required to protect the force.

This publication is organized into five chapters and three appendixes that provide additional detail on selected topics. The following is a brief description of each chapter and appendix:

- Chapter 1 describes the framework of PIO and how it is integrated into the three military police disciplines.
- Chapter 2 provides information on how PIO feeds the operations process and the intelligence process.
- Chapter 3 describes sources of police information used to support analysis.
- Chapter 4 focuses on the analysis of police information. This chapter discusses the critical thinking and predictive analysis techniques applied by trained police intelligence analysts to support the formation of a holistic common operational picture and continuously feed the operations process.
- Chapter 5 discusses the production of police intelligence products. This chapter provides a brief description of some of the more common products that may be produced by the military police or USACIDC personnel and their associated analysts. The chapter also discusses police intelligence networks.
- Appendix A addresses applicable laws, regulations, and directives most relevant to the PIO collection efforts. Additionally, it provides a summary of each document (with respect to its relevancy and applicability to the PIO function) and its restrictions and previsions to Army law enforcement and the conduct of PIO.
- Appendix B provides information on briefing and debriefing requirements in support of PIO.
- Appendix C identifies initiatives used by other agencies in an effort to facilitate necessary interaction and the timely exchange of police information and police intelligence.

The development of this manual resulted in the change of some Army terms and definitions (see introductory table-1).

Introductory table-1. Modified Army terms

Term	*Remarks*
criminal intelligence	FM 3-39 is now the proponent manual for this term.
police information	FM 3-39 is now the proponent manual for this term.
police intelligence	FM 3-39 is now the proponent manual for this term.

This page intentionally left blank.

Chapter 1
Police Intelligence Foundation

FM 3-39 eliminated the five military police battlefield functions and created the three military police disciplines. PIO was retained as an integrating function throughout military police operations. This chapter presents PIO in this new context, explains the role of PIO and how military police forces conduct PIO, and describes how police information is integrated into the three military police disciplines.

OPERATIONS FRAMEWORK

1-1. PIO is a military police function that is integrated within military police operations. PIO supports the operations process through analysis, production, and dissemination of information collected as a result of police activities to enhance situational understanding, protection, civil control, and law enforcement. Information gathered as a result of PIO (whether information directly supporting law enforcement investigations or intelligence requirements generated by a commander or staff) is gathered while conducting military police operations and, upon analysis, may contribute to a commander's critical information requirements (CCIR) and focus policing activities required to anticipate and preempt crime or related disruptive activities to maintain order. Military police Soldiers and USACIDC agents develop PIO skills while supporting police operations at home camps and stations, enabling them to integrate these skills across military police operations in support of decisive action. Other key definitions that provide framework and understanding for police intelligence include the following:

- *Police information* is the available information concerning known and potential enemy and criminal threats and vulnerabilities collected during police activities, operations, and investigations (FM 3-39). The analysis of police information produces police intelligence.
- *Police intelligence* is the application of systems, technologies, and processes that analyze applicable data and information necessary for situational understanding and focusing policing activities to achieve social order (FM 3-39).
- *Criminal intelligence* is a category of police intelligence derived from the collection, analysis, and interpretation of all available information concerning known potential criminal threats and vulnerabilities of supported organizations (FM 3-39).

1-2. USACIDC and provost marshal staffs provide criminal intelligence analysis to commanders that identify indicators of potential crimes and criminal threats against Army property, facilities, or personnel. Criminal intelligence is a subset of police intelligence focused on criminal activity and specific criminal threats. Criminal intelligence is more focused in scope than police intelligence, which has a broader focus (police systems, capabilities, infrastructure, criminal activity, and threats). All criminal intelligence is police intelligence; however, not all police intelligence is criminal intelligence.

ROLE OF POLICE INTELLIGENCE OPERATIONS

1-3. The role of police intelligence is to support commanders, provost marshals, and their staffs in gaining a situational understanding of threats, criminal activities, and criminal networks and to describe the operational environment with a police focus. Police intelligence supports the planning, preparation, execution, and assessment of operations. The ultimate goal of police intelligence is to—

- Enhance the commander's protection program and feed the Army operations process and its integrating activities.
- Assist provost marshals in the prevention and deterrence of crime on bases and base camps.

1-4. Due to the complexity of operational environments, units often need to respond to multiple threats simultaneously. The commander must understand how current and potential threat systems organize, equip,

and employ their forces. It is also vitally important that the commander understand how friendly elements organize, equip, and employ their organizations. This is especially true of host nation policing organizations responsible for police and prison systems critical to stability and security in the operating environment. Military police forces provide the capability to rapidly identify and assess these entities. PIO provides a unique police capability that supports military police operations and the missions and operations of multifunctional commanders. When integrated into the operations process, PIO helps leaders and commanders to better understand criminal networks and how they facilitate criminal activity, subversion, general lawlessness, and insurgency. This understanding and insight can facilitate Army operations designed to disrupt these actions by targeting criminal activities and criminal networks.

1-5. In support of decisive action, PIO will occur as an integrated activity within other military police missions. During offensive and defensive operations, police intelligence can enable the staff to identify organizations and networks (police and criminal) in the area of operations that may provide indications of disruptive activities and conditions requiring corrective action to establish stability. As operations become more protracted and conventional threat levels are reduced from a traditional military threat to a hybrid threat, the lines between criminal, terrorist, and insurgent activities normally associated with stability operations become blurred. PIO planned and integrated by military police staffs and provost marshal sections contribute to the operations process and enhance the commander's situational understanding. This is especially true during stability operations where the role of the military police focuses on developing the ability of a country to protect its communities and establish or reestablish civil security and civil control.

1-6. PIO provides essential products and services in support of military operations at bases and base camps. In particular, police intelligence provides the commander and provost marshal with the situational understanding necessary to reduce threats against Army installations. In addition, PIO provides criminal threat intelligence for in-transit security and focuses the development and implementation of threat countermeasures to safeguard Army personnel, material, and information. Regardless of the operational environment, PIO helps bridge the information gap between what a commander knows and does not know. Information derived from PIO and PIO networks can support the intelligence process.

INFORMATION GAP BRIDGING

1-7. PIO activities provide capabilities that can bridge the gap between traditional military intelligence and information focused on policing and the criminal environment. When the battalion or brigade intelligence staff officer (S-2) or the assistant chief of staff for intelligence (G-2) identifies a gap in the commander's knowledge of the threat and the current threat situation, that gap may be included as PIR or selected as warnings intelligence. (See JP 2-0 for information on warning intelligence.) The S-2 or G-2 will then develop a collection plan to help the commander fill this information gap. Military police staffs and provost marshal sections will also identify information gaps pertinent to policing activities and develop intelligence requirements to fill those gaps. The intelligence requirement findings may also be included in the PIR of the echelon commander.

Note. Military intelligence personnel may collect U.S. person information only when it is necessary to fulfill an assigned function and when it falls within one of several categories. (See DODD 5240.01.) Military intelligence personnel will not direct military police or USACIDC elements to conduct such collection activities. (See AR 381-10.)

1-8. Part of the commander's collection strategy is to select the best collection asset available to cover each information requirement. After a thorough analysis (to include availability, capability, and performance history), the intelligence collection manager identifies which collection assets can best be used. In military police brigades and battalions, military police commanders and staffs identify information gaps; develop intelligence requirements; develop, synchronize, and integrate collection plans; and task or coordinate for collection assets. In echelons above brigade, a brigade combat team, or a maneuver enhancement brigade structure, the provost marshal section coordinates with the S-2 or G-2 to ensure that military police-related intelligence requirement information is synchronized and integrated into the overall information collection plan. When military police or USACIDC personnel are tasked with the police information collection mission, they are provided specific guidelines and a prioritized collection requirement.

1-9. In the United States or its territories, effective PIO can provide installation commanders and provost marshals with situational understanding and address information gaps to ensure that threat assessments are valid and reliable. Provost marshals and staffs responsible for law enforcement operations conduct PIO in support of bases and base camps. USACIDC elements conduct PIO in their area of operations to support investigative and other support requirements. PIO capitalizes on connectivity between installation law enforcement and domestic civilian agencies.

Note. Domestically, military intelligence involvement is limited. However, military intelligence personnel may actively participate in PIO activities when supporting law enforcement missions while assigned to a law enforcement agency. Maximum reliance shall be placed on domestic civilian investigative agencies (federal, state, and local), excluding specific law enforcement and protection-related missions where collection activities are authorized to meet an essential requirement for information. (See DODD 5200.27.)

1-10. Military police and USACIDC elements conduct policing, detention, and security and mobility support operations as a part of decisive action. Police information and police intelligence, when integrated into these operations, facilitate effective decisionmaking that shapes the execution of policing activities. Military police commanders direct PIO in their respective operations sections. Provost marshals conduct PIO within their staff sections in support of the commander and subordinate military police elements.

1-11. The hybrid threats faced in modern operational environments operate from positions intermingled in the population. These threats operate in small groups, cells and, occasionally, as individuals. Many of the threat methods employed mirror organized criminal and terrorist activities. These threat methods increase the relevance of military police and USACIDC units with capabilities to assess the criminal threat environment, gather relevant police information, conduct analysis, and produce usable police intelligence.

1-12. On bases and base camps, military police and USACIDC personnel are the lead for targeting, collecting, and interdicting against a broad range of threat activities, including terrorism, organized crime, contraband trafficking, and other illegal activities. Military police and USACIDC assets collect police information in this environment through deliberate surveillance missions or through missions tasked to law enforcement patrols and conducted in the course of routine patrol or investigative activities.

1-13. In support of decisive action, military police personnel may be tasked as the primary collectors of information on enemy forces operating along extended lines of communication, on main supply routes, or in support of a movement corridor. (See FM 3-81.) Concurrent with the requirements to collect information in support of identified intelligence requirements, personnel conduct police information collection to support PIO. This information collection, pertinent to the police and criminal environment, facilitates the transition to stability operations and the establishment and maintenance of civil security and civil control. As the major operation transitions from offense and defense to stability operations, the weighted focus for military police units generally shifts from security and mobility support to police operations. Military police and USACIDC personnel generally increase police intelligence efforts during stability operations to focus support to host nation police and detention activities. USACIDC elements increase the documentation of threat criminal activity identified during military operations in preparation for potential criminal prosecution. During stability operations, technical police collection and assessment efforts increase significantly.

1-14. Military police staffs and provost marshal sections at all levels perform PIO to varying degrees, depending on mission requirements, the personnel and capabilities available, and the commander's guidance. The focus at any echelon is dependent on the specific mission, commander's intent, investigative requirements, and CCIR. At the company level, the application of police intelligence is extremely limited, focusing on current and projected tactical missions. At the brigade level and higher, the police intelligence focus is broader, addressing operational and strategic concerns affecting an entire area of operations.

1-15. In military police battalions and brigades, the battalion or brigade operations staff officer (S-3) is responsible for the day-to-day conduct of PIO. The S-3 ensures that basic police information collection activities are implemented and that the activities support the commander's intent and information requirements. This includes ensuring that PIO is fully integrated into all military police operations and synchronized with the operations process. The S-3 works closely with the S-2 to ensure this

synchronization. At the division and higher echelons, the police intelligence process is managed by the provost marshal section, operating as part of the S-3 or assistant chief of staff for operations (G-3). In these organizations, the provost marshal section ensures that the PIO process is synchronized with other staff processes. The continuous flow of collected police information and police intelligence enables a fused intelligence picture and provides constant input to the operations process and its integrating processes.

MILITARY POLICE DISCIPLINES

1-16. The PIO process is integrated into the three military police disciplines—

- Police operations.
- Detention operations.
- Security and mobility support.

POLICE OPERATIONS

1-17. PIO is commonly associated with police operations, more specifically law enforcement and criminal investigations. The skill sets and capabilities required for PIO are honed during police operations. The military police support commanders, Soldiers, family members, and visitors on bases or base camps through comprehensive policing activities. Law enforcement operations are normally the most visible aspect of this support, with military and DA civilian police forces providing for a safe and secure environment on installations and in training areas. PIO, when properly resourced and employed, also provides critical support to personnel on and near installations.

Law Enforcement and Criminal Investigations

1-18. PIO directly supports law enforcement and criminal investigations. Commanders, provost marshals, and law enforcement investigators generate intelligence requirements needed for situational understanding and decisionmaking regarding criminal investigations, disruption of criminal activity, distribution of law enforcement assets, and mission focus. The analysis of information gathered during law enforcement activities can provide critical linkages, associations, and patterns necessary to conduct law enforcement investigations, identify criminal networks, solve crimes, and close criminal investigations.

1-19. The analyses of crime trends, patterns, and associations enable commanders, provost marshals, and military police staffs to plan and make decisions regarding patrol distribution, resource requirements, and areas requiring increased police engagement and focus. Interagency cooperation and coordination provide critical information that can be further analyzed and fused by military police and USACIDC personnel and police intelligence analysts in support of Army law enforcement efforts.

Criminal Investigation Task Force

1-20. The Department of Defense (DOD) criminal investigation task force is a strategic-level organization with a mission to develop and fuse police intelligence with military intelligence for building criminal cases against terrorist criminals that have attacked U.S. interests. The organization conducts complicated criminal investigations that target terrorists and complex criminal organizations. These cases typically cross international borders and involve criminals captured because of military operations, requiring coordination with international police and intelligence agencies.

1-21. The criminal investigation task force combines USACIDC special agents (and criminal investigators from other Services), police and intelligence analysts, and attorneys into teams. These teams synchronize and fuse information and intelligence from available sources to conduct criminal investigations that enable criminal prosecution in U.S. or host nation legal systems.

Police Engagement

1-22. Police engagement is the most basic police information collection activity conducted by military police. The military police Soldier's and civilian police officer's continual interaction with the populace, host nation police, and media personnel allow personnel to gather and share information while conducting police operations and provide valuable information that can be analyzed and disseminated as police

intelligence. The information collected should be documented on field interview cards, which are useful to assist law enforcement patrols in obtaining relevant information. Police engagement as a means to gather police information can be formal or informal. See ATP 3-39.10 for additional information on police engagement.

1-23. Police information is continuously gathered through the interpersonal information networks established during the conduct of military police operations in support of decisive action while performing law enforcement and investigations. Whether formally collected for a specific law enforcement purpose or informally as a by-product of daily interaction and situational awareness by military police or USACIDC personnel, information collected by police personnel provides valuable insight to the operational environment.

1-24. The relationship between the police and the population is critical in the ability to interact with and operate around the local population. Just as mistrust and a weak social order can enable criminals and terrorists, a strong relationship between the population, police, and security forces is key to assisting with investigations, understanding the social order, defeating criminal networks, and collecting police information.

1-25. On bases and base camps, military police should remain cognizant of the importance of a positive relationship with residents, installation workers, and the public. During support to decisive action, military police must remain aware of the importance of establishing this same professional reputation with the local population. This difficult task requires a thorough understanding of the rules of engagement and support at every level of leadership.

Host Nation Police Capability and Capacity

1-26. In support of host nation police organizations, the analyses of trends, patterns, and associations in an organization can provide insight into systemic problems internally in the police organization (training deficiencies, administrative issues). PIO integrated within policing operations in support of decisive action can provide critical analysis and a situational understanding of civil considerations as they relate to host nation police systems, organizations, capability, and capacity. See ATP 3-39.10 for additional information on building host nation police capability and capacity.

1-27. In operations where building police capacity and capability are key measures of effectiveness, it is imperative to train and resource the developing host nation police and security forces so that they can also leverage the ability to connect people to locations and events, while at the same time recognizing trends, patterns, and associations. Military police and USACIDC personnel conducting host nation police training and support not only train host nation police and security forces to conduct PIO, but also place them in an advantageous position to gain information about the police force, criminal environment, and other information about the population in which the host nation police operate. When sharing classified military information or controlled unclassified information with foreign partners and host nation law enforcement agencies, foreign disclosure considerations and policies must be adhered to as outlined in AR 380-10. Since not all information likely proposed for disclosure falls under the purview of the *National Disclosure Policy* (information marked law enforcement-sensitive), early and continuous coordination with the supporting foreign disclosure officer is essential.

1-28. Information sharing among the elements operating in the area of operations is a critical factor in a successful police intelligence analysis and the production of relevant and timely police intelligence products. These cooperative efforts can result in the substantial exchange of threat information; enable police intelligence analysts to produce vital police intelligence products that provide early warning to commanders, provost marshals, and law enforcement investigators; and allow them to develop protection strategies to counter complex criminal threats.

1-29. Information and police intelligence regarding locations, capability, and disposition of host nation police and security elements can be critical to military police conducting host nation police development, enabling them to plan for host nation response forces and potential safe havens. It can also identify host nation police elements that may be infiltrated by criminal or insurgent elements, arming personnel with the knowledge to avoid those locations and exercise caution when interaction is required.

1-30. Military police conducting missions to build host nation police capability and capacity may be required to engage in the vetting, hiring, training, leading, and safeguarding of new police forces (often across a widely dispersed area of operations). Some former police who may wish to return to their previous modes of operation to increase personal wealth and influence may staff these new police forces. There may also be criminal or insurgent elements that infiltrate newly forming police organizations for the same reasons or to carry out direct attacks on U.S. military and host nation police forces. The ability to conduct effective PIO is a critical task in these situations.

Host Nation Police Intelligence Capability

1-31. Building host nation police intelligence capability and capacity requires a detailed assessment of the host nation police organization, followed by the training and mentoring of host nation police personnel by military police Soldiers and multinational and civilian law enforcement personnel supporting host nation police development.

1-32. The ability of host nation police to support and conduct the full range of PIO and enabling tasks may be limited by education, training, available resources, societal norms, host nation legal systems, and tactical environments. For example, taking a photograph of a person is not accepted in some societies. These populations may resist being photographed or having iris images captured. In other areas and societies, many of the modalities of biometrics and forensic analysis may not be understood and, therefore, will not be accepted. However, where acceptable, these capabilities can be invaluable to host nation police intelligence capability. Deliberate police engagements with prospective leaders of emerging police forces are vital in establishing a hierarchy of available and planned police intelligence capabilities.

DETENTION OPERATIONS

1-33. Police information collection activities conducted in support of detainee operations are generally passive in nature, gained through military police Soldiers' observations of the patterns and associations of detainees.

1-34. The analysis of information that is gathered during detention operations can provide valuable associations and patterns to military intelligence personnel, enabling personnel to further refine their intelligence picture, develop additional intelligence requirements to support operations, and maintain a holistic common operational picture. See FM 3-63 for additional information on detainee operations.

1-35. Detention operations provide a valuable source for criminal information supporting law enforcement efforts and the identification of exploitable information supporting other decisive action tasks. Military police Soldiers, by virtue of their detention mission, are in a position to gather information for exploitation by operational elements and in support of law enforcement investigations throughout the detention process. Current (and likely future) operating environments require criminal prosecution of detainees captured in the conduct of decisive action. Military police personnel should be integrated into detainee processing as close to the point of capture as possible. This facilitates operational exploitation and follow-on law enforcement investigations (as required). If military police integration at the point of capture is not possible, military police oversight is required at the first detainee processing point after the point of capture (typically a detainee holding area). The integration of PIO by military police Soldiers conducting detention operations as close to the point of capture as feasible enables law enforcement and police intelligence analysts to—

- Identify police-related information early in the operation.
- Preserve and report potential police information (to include forensic and biometrics data) and criminal evidence quickly.
- Analyze collected information and produce police intelligence.
- Disseminate information and police intelligence for integration into the operations process and law enforcement investigations.

1-36. PIO enables the ability of military police Soldiers, law enforcement investigators, and police intelligence analysts to connect persons to other individuals, organizations, objects, and events relevant to the criminal domain. These associations may be relevant to incidents inside a detention facility; however, they may also associate the individual with persons outside the facility and events that may have occurred before detention. These associations can be especially relevant during counterinsurgency operations. For

example, military police Soldiers in one area may obtain evidence from a crime scene that implicates a detainee at a U.S. or host nation detention facility. This may be confirmed through detention facility biometrics enrollment data. This confirmation may result in a request for additional information on the detainee, initiating a follow-on interrogation by military intelligence (for human intelligence [HUMINT] interrogation) or law enforcement or criminal investigators (for law enforcement interrogation supporting a criminal investigation). Military police Soldiers in a facility may find evidence connected to another person or incident outside the facility. This information would be documented, secured, and passed through the chain of command to the appropriate supporting military intelligence unit and law enforcement element for additional action and investigation.

Safety and Security

1-37. Police intelligence is critical to maintaining good order and discipline in detention facilities. Detainee operations are inherently risky due to the high numbers of detainees and relatively low numbers of guard personnel supporting operations. PIO in the detention environment supports the commanders risk management efforts. (See ATP 5-19.) Detainees may benefit from a break down in good order and discipline in facilities and take steps to facilitate that process. To limit or prevent cooperation with U.S. authorities, detainees may attempt escapes, form organizations and associations to control the internal workings of a facility, or intimidate other detainees. Military police commanders and staff responsible for these facilities must continuously determine intelligence requirements and conduct ongoing analysis to identify and counter these activities and the associated risks.

1-38. In a facility, military police Soldiers will have extensive contact and visibility with detainees. The effort to maintain good order and discipline requires cooperation across functional lines. Military police commanders and staffs should ensure that personnel supporting detainee operations from other functional specialties are briefed to be alert to activities, writings, or conversations that can fulfill intelligence requirements for commanders and staffs. Critical information can be obtained through coordination and information sharing with military intelligence HUMINT teams. Medical personnel who treat injured and sick detainees can provide observations regarding detainee behavior, interaction, or spontaneous statements. Engineers performing repairs on damaged facilities may note changes in other physical characteristics. Host nation and U.S. interpreters are in a position to hear detainee conversations, read graffiti, and screen inbound and outbound mail. All of these interactions are opportunities to gather information that can lead to the commanders increased understanding of their area of operations.

Criminal Investigations

1-39. Police intelligence can assist law enforcement investigators to develop patterns and criminal associations in a facility. This can lead to identification and documentation of criminal behavior and individual perpetrators. This information enables the commander and military police staff to identify criminal groups that are forming and take steps to interdict these groups before serious breaches of security occur. Information collected may also be valuable to law enforcement investigators conducting criminal investigations focused on crimes within and outside the facility. PIO can link detainees in the facility to crimes, criminals, and activities outside the facility.

1-40. Commanders may also direct criminal investigations concerning events in a facility. These events may include a variety of serious criminal infractions, including attacks on other detainees or U.S. personnel, contraband smuggling, and escape attempts. Care must be taken to recognize, preserve, collect, and process items with evidentiary value. Once collected, this evidence is packaged and forwarded to a supporting forensic laboratory for further examination and analysis.

Intelligence Support

1-41. Doctrine and legal requirements call for close cooperation between intelligence and military police personnel during detainee operations. Proper coordination ensures the maximum benefit to the commander and the mission and ensures that U.S. forces stay within the limits of U.S. and international laws and treaties. (See FM 3-63 for additional information.) Due to the extensive contact and visibility military police Soldiers and support personnel maintain with detainees, they receive large amounts of information. This information is collected passively through activity observations, contraband, writing (notes, graffiti),

and overheard conversations. These observations are reported through the chain of command and collated by staff and police intelligence analysts. Simultaneously, this information is passed to the supporting intelligence personnel through intelligence channels. The sharing of information enables intelligence personnel to capitalize on collected information, further enhancing their ability to provide situational understanding to the commander and to answer the commander's PIR.

SECURITY AND MOBILITY SUPPORT

1-42. Security and mobility support is a military police function conducted to protect the force and noncombatants and preserve the commander's freedom of action. Military police conducting security and mobility support are generally dispersed across the area of operations. This dispersion of military police Soldiers regularly places military police in close contact with U.S. and host nation personnel and offers substantial opportunities for police engagement and information collection.

1-43. The mobility and communication capabilities of military police units enable them to detect threat elements and rapidly report these contacts. Security and mobility support operations place military police Soldiers in the position to frequently observe and make contact with the local population, facilitating police engagements and information collection. PIO integrated throughout security and mobility support missions may result in collection opportunities that satisfy intelligence requirements and increase situational understanding. Typically, military police Soldiers are the first to respond to an incident in the area of operations, particularly in support areas. Their knowledge of evidence collection and incident site preservation can prove critical to protecting key police information for future analysis.

1-44. PIO integrated into security and mobility support planning and execution enables more informed decisionmaking by commanders, military police staffs, Soldiers, and leaders conducting security and mobility support missions. Used in conjunction with or integrated within the organization intelligence preparation of the battlefield, police intelligence products assist in identifying areas of threat activity or other obstacles. These products enable commanders to make prudent decisions regarding the security of convoys transiting the areas and provide military police with the information necessary to mitigate the risk through the staff planning process.

1-45. Military police elements observe the area around them at all times and remain aware that changes in the anticipated social order may be indicators of enemy action or coercion. Military police conducting security and mobility support operations seek out host nation police and security elements operating in their assigned area of operations. This facilitates the collection of data pertaining to civil considerations, specifically focused on the variables of police and prison structures, organized criminal elements, legal systems, investigations and interviews, crime-conducive conditions, and enforcement gaps and mechanisms (POLICE). (See chapter 2 for additional details on the POLICE memory aid.)

1-46. Military police patrols may also identify indications of criminal activity. This data, when reported through the chain of command, contributes to overall situational understanding and enables the staff and analyst to identify patterns and activities that indicate the existence of organized criminal activity or areas of significant criminal activity.

1-47. The analysis of police information allows military police staff, Soldiers, and leaders conducting security and mobility support to plan and execute measures to counter the effects of criminal activity on military operations. These countermeasures may include—

- Implementing vulnerability assessments.
- Developing procedures to detect terrorist actions before they occur.
- Hardening likely targets.
- Conducting offensive operations to destroy an enemy.
- Identifying high-threat areas and recommending bypass routes.

Main Supply Route Regulation and Enforcement

1-48. Military police units use traffic control posts and roadblocks to control the movement of vehicles, personnel, and materiel and to prevent illegal actions that may aid the enemy. These control measures serve as a deterrent to terrorist activities, saboteurs, and other threats. Information and police intelligence

regarding locations, capabilities, and dispositions of host nation police and security elements can enhance operations and identify friendly capabilities and host nation police elements that may be infiltrated by criminal or insurgent elements.

1-49. Military police tasked to conduct main supply route regulation are in a position to observe suspicious behavior and identify potential threats against U.S. interests by recognizing patterns of movement, suspicious trends, and other indicators of nefarious behavior amongst users of the main supply route.

Support to Dislocated Civilian Operations

1-50. Dislocated civilian operations are conducted to provide safety and security for dislocated civilians. Unlike detainee operations, dislocated civilians are not typically detained against their will. Dislocated civilian facilities, however, can manifest some of the same safety and security issues inherent in detainee operations. Any facility housing hundreds or thousands of individuals in a confined space is likely to experience safety and security issues. These situations may be a result of anger and frustration of individuals under significant amounts of stress. These situations may also be the result of criminal elements in the population seeking to intimidate or exploit their fellow dislocated civilians. In some operations, the same information-gathering techniques employed to identify individual criminals, counter criminal elements, and enable criminal investigations in detention facilities may also be required within the context of dislocated civilian operations.

1-51. Dislocated civilian operations place military police Soldiers in regular contact with the dislocated populace and can provide significant amounts of potentially valuable police information. Military police conducting these tasks may receive police information regarding persons wanted for crimes or questioning. Their continual interaction with the population can facilitate the collection of biometrics and background data on persons that can later be compared against databases of other biometrics data, enabling the identification and location of persons of interest.

Logistics Security

1-52. Logistics security is concerned with the integrity of the logistics system through the prevention, identification, and investigation of criminal acts committed by terrorists, criminal elements, or insider threats that range from the U.S. Army logistics provider to the military force on the ground. USACIDC personnel are assigned the responsibility of conducting logistics security. Police information collected passively by security personnel and passed on to USACIDC personnel may lead to indications of criminal elements attempting to participate in forms of economic crimes. Police intelligence analysts might analyze reports of theft, suspicious behavior, or other questionable acts that might focus the efforts of USACIDC personnel in the apprehension of criminal elements.

This page intentionally left blank.

Chapter 2

Integration Into the Operations Process

Police information and police intelligence is incorporated into the operations process via the integrating processes. This chapter provides a discussion of how PIO, integrated in military police operations, is integrated into the Army operations and intelligence processes. It provides information on PIO across the range of military operations and to unified action. Commanders, supported by their staffs, use the operations process to drive the conceptual and detailed planning necessary to understand, visualize, and describe their operational environment; make and articulate effective and ethical decisions; and direct, lead, and assess military operations. (See ADRP 1 and ADRP 5-0 for additional information.) PIO feeds the operations process along with its three integrating processes (intelligence preparation of the battlefield, targeting, and risk management).

OPERATIONS PROCESS

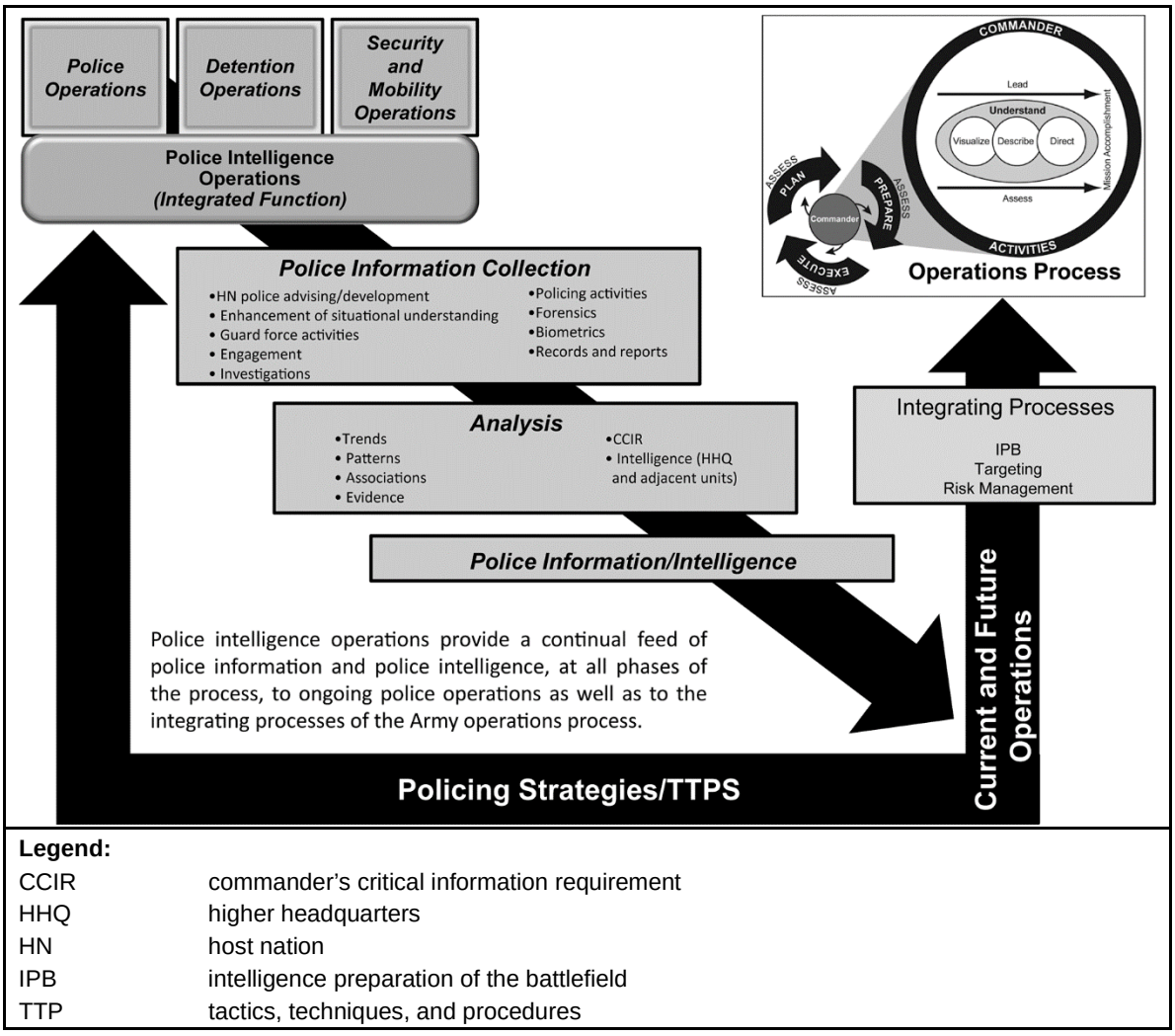
2-1. The *operations process* is the major mission command activities performed during operations: planning, preparing, executing, and continuously assessing the operation (ADP 5-0). The activities of the operations process are not discrete; they overlap and recur as circumstances demand. Planning starts an iteration of the operations process. (See ADRP 5-0.) There are four principles of the operations process. Commanders—

- Drive the operations process.
- Build and maintain situational understanding.
- Apply critical and creative thinking.
- Encourage collaboration and dialogue.

2-2. PIO, if properly planned and integrated into military police operations, leads to the continuous feed of police intelligence into the operations process through the integrating processes or ongoing police operations. The integration of police intelligence is continuous and assists commanders and provost marshals in gaining situational understanding and determining the right force tailoring to accomplish the mission. Figure 2-1, page 2-2, provides a graphic representation of the PIO integration into the operations process.

2-3. PIO represents the military police capability to collect, analyze, and process relevant information from many sources, generally focused on policing activities and military police operations. PIO is continuously conducted by military police and USACIDC personnel to collect, analyze, and disseminate police information and police intelligence on infrastructure, systems, populations, and individuals gathered while conducting military police operations. Information is collected and analyzed from a policing viewpoint. (See FM 3-39.) Information and intelligence from other operational elements are fused with information collected by military police and USACIDC Soldiers to develop a common operational picture. Police information is gathered during the conduct of military police operations, focusing on the three military police disciplines.

2-4. Information collected through the execution of PIO is disseminated throughout the policing community and pushed into the operations process. This process ensures a continuous flow of police information to promote the development of a holistic common operational picture for commanders.



Legend:

CCIR	commander's critical information requirement
HHQ	higher headquarters
HN	host nation
IPB	intelligence preparation of the battlefield
TTP	tactics, techniques, and procedures

Figure 2-1. PIO support to military police operations and the operations process

2-5. Police information and police intelligence are used to verify the effectiveness of policing strategies when applied in the conduct of policing, specifically law enforcement operations. The analysis of police information can lead a commander or provost marshal to increase or decrease military police presence or modify the techniques used in particular areas.

INTELLIGENCE PREPARATION OF THE BATTLEFIELD

2-6. Intelligence preparation of the battlefield is a systematic process of analyzing and visualizing the operational environment in a specific geographic area for a specific mission or in anticipation of a specific mission. Although staff integration of intelligence preparation of the battlefield is generally led by the S-2 or G-2, all staff elements must fully participate and provide their individual areas of expertise to the effort. (See ATP 2-01.3 for more information on intelligence preparation of the battlefield.) Commanders and staffs develop the intelligence preparation of the battlefield and apply it in all phases of the operations process. They ensure that there are tactics, techniques, and procedures in place for the continual assessment, development, and dissemination of intelligence preparation of the battlefield products. All staff members must understand and participate in the intelligence preparation of the battlefield process. PIO is a reciprocating effort that feeds and draws from intelligence preparation of the battlefield to help commanders understand the environment, mitigate vulnerabilities, and exploit opportunities. In addition to the tactical information that may be obtained through the conduct of policing activities, police intelligence

provides additional information on possible criminal threats and threats to social order that may support or drive current operations and change the friendly threat posture.

2-7. Military police planners use several tools to assist in framing and understanding the complexity of the operational environments in which military forces operate. Military police can provide relevant information to the analysis of the operational environment using the operational variables of political, military, economic, social, information, infrastructure, physical environment, and time (PMESII-PT) analyzed and viewed using a policing lens. (See FM 3-39 for additional information on the operational variables analysis with a policing focus.)

2-8. The POLICE memory aid provides a framework for assessing the police and criminal focused civil considerations, and it serves as a tool for organizing information and developing information requirements, some of which may become CCIRs. This assessment helps shape military police planning and the execution of military police operations.

2-9. Military police and the USACIDC elements identify existing host nation police organizations, to include personnel and leadership. PIO integrated within military police operations enables the staff and police intelligence analysts to analyze and assess police structures and identify current police capability and capacity, to include the existence or lack of a functioning legal system. Military police conduct crime and criminal analysis to assess the criminal environment, to include the existence of organized criminal elements, crime-conducive conditions, and general levels of criminal activity. The factors of POLICE are used to determine—

- **Police and prison structures.** What police and prison structures exist? This factor may answer information requirements.
  - Does a functional police or security force exist?
  - What police infrastructure is available? Is it in operational condition? What is needed?
  - Is the indigenous police force corrupt?
  - How does the community receive the police force?
  - Can the indigenous police force be relied on as an asset to assist U.S. and joint forces?
  - What equipment, communications, and other capabilities do the indigenous police force have if it is reliable? What equipment and capabilities are needed?
  - Does the police force have adequate systems in place to operate effectively (such as administrative, training, logistic, and investigative systems)?
  - How many prison structures exist in the area of operations? What are the prison structure types and capacities? Are they operational?
  - Are jurisdictional boundaries established? What is the historical reason for the establishment of jurisdictional boundaries?
- **Organized criminal elements.** Is organized criminal activity present? If so, what are the—
  - Indications of organized crime?
  - Motivation factors for the organized criminal activity—financial or facilitating insurgent activity?
  - Specific criminal activities identified?
  - Public attitudes toward organized criminal activities?
  - People, organizations, or businesses targeted by organized criminal elements?
- **Legal systems.** What is the composition of the legal system?
  - Is there a law-enforcing mechanism? If so, what is it?
  - Is there an adjudicating body?
  - Does the legal system operate based on the rule of law? If not, what is the basis?
  - Are all three elements of the criminal justice system (police, prisons, and judiciary) present, functional, and synchronized?
  - Are appropriate administrative record systems in place to support the legal system?

- **Investigations and interviews.** Are adequate criminal investigative systems functioning and enforced?
  - Do adequate investigative capabilities exist to perform police and administrative investigations (criminal, traffic, internal affairs, administrative functions)?
  - Are adequate administrative and database systems in place to support investigations, to include PIO?
  - How are internal and external investigations, inquiries, and assessments initiated, managed, tracked, and reported? Are records appropriately transparent to the public? Are they consistently applied?
  - Are police and criminal investigative capabilities leveraged to support site exploitation and targeting?
- **Crime-conducive conditions.** What conditions exist that contribute to the initiation, development, and expansion of crime?
  - What specific resources or commodities are available and attractive to criminals?
  - What locations are vulnerable to criminals?
  - What security gaps exist that could create vulnerabilities to criminal behavior (systems, procedures, physical security measures)?
- **Enforcement gaps and mechanisms.** What enforcement gaps are present and what assets are available? Are enforcement gaps present or imminent due to the movement or elimination of an asset or capability? Do these enforcement mechanisms include—
  - Local security or police forces?
  - Guards?
  - Response forces (special response teams, civilian police special weapons units, military and paramilitary response forces)?
  - Informal religious, ethnic, or family structures and influence?
  - Organized criminal elements?
  - Multinational or interagency organizations?
  - Informal social authorities?

TARGETING

2-10. *Targeting* is the process of selecting and prioritizing targets and matching the appropriate response to them, considering operational requirements and capabilities (JP 3-0). Targeting means can range from lethal engagements, nonlethal weapons, and informational engagements. Targeting begins in the planning process and continues throughout the operation. The Army targeting process is described in the framework of decide, detect, deliver, and assess (D3A). This targeting methodology facilitates engagement of the right target, at the right time, and with the most appropriate assets (lethal or nonlethal), based on the commander's targeting guidance, objectives, and desired effect.

2-11. In many operational areas, the threat is more criminal than conventional in nature. In these environments, belligerents use or mimic established criminal enterprises and practices to move contraband, raise funds, or generally further their goals and objectives. In all operational areas, criminal activity impacts the mission of Army forces and threatens Army personnel and assets. Assessing the impact of criminal activity on military operations and properly identifying that activity from other threat or environmental factors can be essential to effective targeting and mission success.

2-12. Developments in biometrics technology, the introduction of evidence collection and examination at incident sites, and collected material in operating environments outside the United States have proven the effectiveness and relevance of police intelligence and its ability to provide timely and accurate intelligence to the geographic combatant commander. The technical capabilities and knowledge of complex criminal organizations and activities leveraged by military police and USACIDC personnel provide methods and reachback that increase the commander's ability to identify threats.

2-13. Police intelligence contributes to the targeting process by providing timely, relevant, and accurate police information and police intelligence regarding crime and criminal threats in the area of operations.

Military police personnel, USACIDC personnel, and police intelligence analysts must understand their role in the targeting process and how police intelligence supports the targeting process.

2-14. Military police and USACIDC personnel and police intelligence analysts integrate information and police intelligence into the targeting process. The activities that support the operations process are integrated into the targeting process during the military decisionmaking process, targeting meetings, coordination with the fires cell, and other staff functions. The D3A methodology provides the structure for staffs to integrate analysis, monitor operations, and make recommendations enabling commanders to make informed targeting decisions. (See FM 3-60 for additional information on the targeting process.) Table 2-1 illustrates D3A key activities and shows how military police and USACIDC personnel that conduct PIO integrate into the overall targeting process.

Table 2-1. Targeting methodology

D3A Activities		***Military Police and USACIDC Personnel and Police Intelligence Analysis Support to Targeting***
Decide which targets to engage.	Perform continuous activity based on the mission, commander's intent, concept of the operation, and planning guidance to produce or determine— • Intelligence requirements. • Priorities of reconnaissance, surveillance, target acquisition, sensor allocation, and employment. • Target acquisition taskings. • High-payoff target lists. • Target selection standards. • Assessment criteria. • Prioritization of the targets. • Measures of performance and effectiveness. • Attack guidance matrix. (Enables the commander or leader to make a decision on who, what, when, where, and how to engage.)	• Develop intelligence requirements pertinent to policing operations. • Develop the police information collection plan. • Ensure that police intelligence requirements and the collection plan are integrated and synchronized with the overall information collection plan. • Identify change indicators relevant to the police and criminal environment. • Identify military police, USACIDC, or other collection assets capable of collecting against specific police intelligence requirements. • Nominate police-related intelligence requirements as priority intelligence requirements (as required). • Nominate criminal or police-related targets as high-payoff targets (as required). • Make recommendations regarding engagement means. • Assess probable effects of recommended engagements. • Task appropriate military police or USACIDC collection elements (if applicable).
Detect the targets.	• Produce an information collection synchronization matrix. • Dedicate assets to collect information. • Report and disseminate information. • Update information requirements as they are answered. • Develop a target. • Vet a target. • Determine the threat/target validity.	• Participate in information collection synchronization to ensure that police information collection efforts are synchronized with maneuver and other collection elements. • Monitor collection efforts. • Gather reports, evidence, and other pertinent police-related information. • Conduct debriefings of collection elements to ensure that all available police-related information is gathered and collated. • Conduct the analyses of collected data to determine trends, patterns, and associations regarding crime, criminals, and associated data. • Identify potential targets (criminals, crime conditions, populations). • Develop police intelligence folders for specific cases or targets. • Recommend adjustments to the police information collection plan and policing strategies.

Table 2-1. Targeting methodology (continued)

D3A Activities		*Military Police and USACIDC Personnel and Police Intelligence Analysis Support to Targeting*
Detect the targets (continued).		• Identify specific targets (criminals, crime conditions, populations) and timelines for recommended engagement. • Monitor change indicators for causal relationships (cause and effect).
Deliver (conduct the appropriate engagement operation).	• Identify and task specific engagement units. • Identify engagement methods (ordnance, tasked information). • Consider the desired effect on the target (classified as light, moderate, or severe). • Identify the engagement timeline selected and tasked. • Coordinate, synchronize, and monitor the engagement.	• Task military police or USACIDC personnel to conduct engagement missions (if applicable). • Identify and include the method of engagement, required timeline, and desired effect in the tasking order. • Obtain or develop proper information themes and messages to ensure consistency with military actions. • Monitor military police and USACIDC elements conducting target engagement and other elements engaging police-related targets. • Identify personnel and capabilities required for site exploitation. • Task military police and USACIDC elements (as required) for participation as part of the site exploitation team. • Use the proper chain of custody to obtain reports, evidence, witness statements, and other pertinent police-related information from the site exploitation team. • Conduct debriefings of site exploitation team participants (if available) to ensure that all available police-related information is gathered and collated.
Assess the effects of the engagement.	Measure and analyze results to determine if— • The targeting objective was met. • Additional engagement is required. • A different engagement method is required.	• Conduct assessments based on approved measures of effectiveness, measures of performance, and identified change indicators. • Determine if additional target engagement is required (on the same or new target). • Determine if the method of engagement achieved the desired effect; determine if alternative engagement methods are justified. • Recommend engagement actions and adjustments, as required. • Conduct the analyses of post engagement data. • Produce police intelligence, as required. • Disseminate police information and police intelligence as required, within mission, regulatory, and policy constraints. • Update running estimates and associated staff products.
Legend: D3A decide, detect, deliver, and assess USACIDC United States Army Criminal Investigation Command		

2-15. Targeting in the Army targeting construct is typically understood as an activity executed in military operations abroad against a foreign threat. The identification and targeting of criminal threats in the context of policing and protection of U.S. personnel and infrastructure follow the same basic methodology. Police intelligence, integrated into police operations (specifically law enforcement operations) in support of bases and base camps, is critical to understanding the criminal environment, developing linkages between criminal actors, establishing critical correlations in time and space, or identifying trends and patterns in criminal activity. Crime and criminal target analysis is further discussed in chapter 4. All these variables are valuable in narrowing the scope of policing activities and investigations so that persons of interest can be identified and interviewed, locations or material can be identified for examination and collection for evidentiary value, and criminal threats can be appropriately targeted for apprehension.

RISK MANAGEMENT

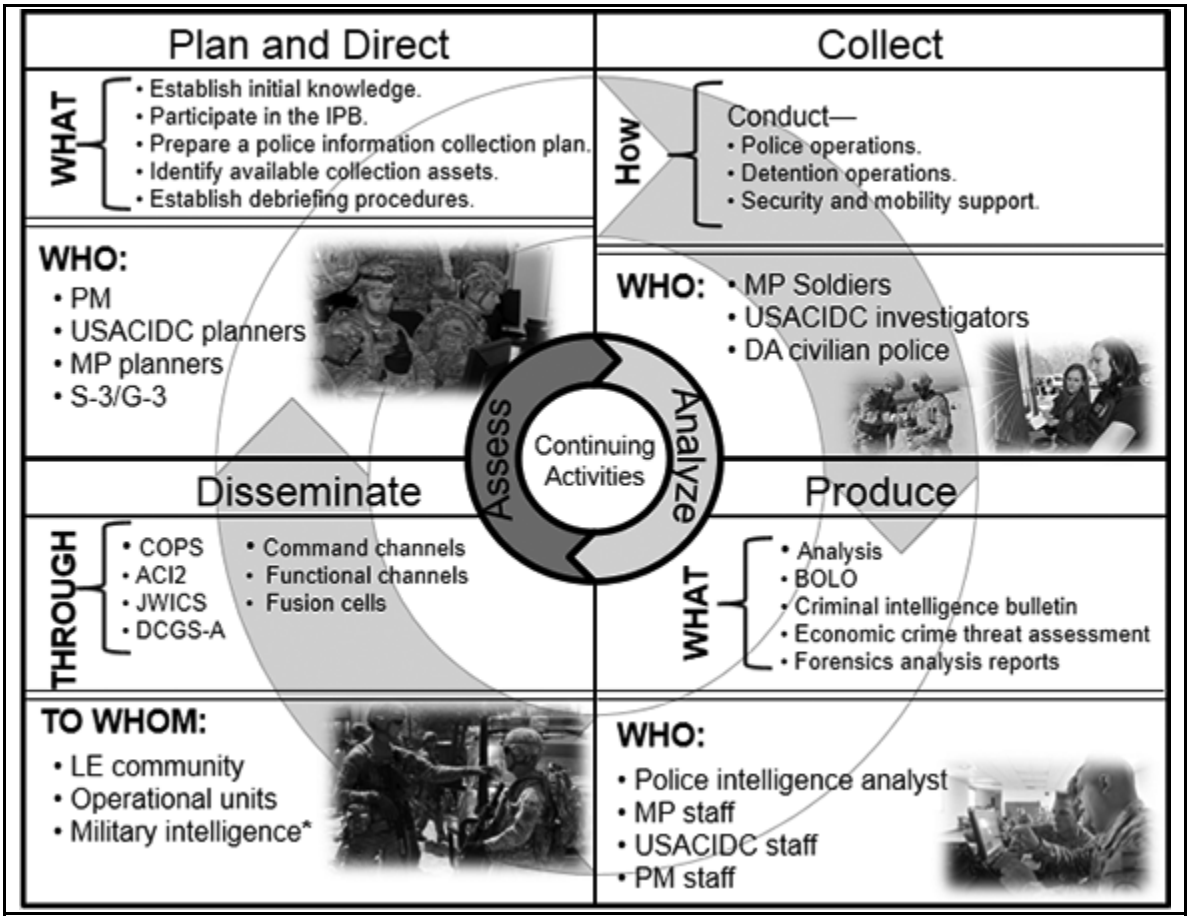
2-16. *Risk management* is the process of identifying, assessing, and controlling risks arising from operational factors and making decisions that balance risk cost with mission benefits (JP 3-0). Information obtained through PIO directly contributes to the risk management process through the identification of potential threats and conditions that pose a risk to U.S. forces and civilians. These risks may be in the form of a credible threat of direct terrorist actions against a unit or base, the presence of criminal activity directed at U.S. assets or personnel, or the identification of environments where police organizations and enforcement are lacking or corrupt. Thus, lawlessness is prevalent and random crime poses a threat. (See ATP 5-19 for additional information on risk management.)

2-17. Police information and police intelligence resulting from PIO may identify threats before they manifest themselves. These threats may be conventional, criminal, or environmental. The continuous flow of information and intelligence from military police and USACIDC elements into and out of the Army operations process, to include the risk management process, can provide early identification of potential threats to personnel and equipment. This provides commanders and staffs time to properly assess the threat, determine the risk to personnel and equipment, and develop and implement control measures to mitigate the threat.

INTELLIGENCE PROCESS

2-18. PIO follows the Army intelligence process to execute activities required to generate information, products, and knowledge that enhance the situational understanding of the police and criminal environment and guide policing activities in the operational area. The intelligence process is composed of four steps (plan and direct, collect, produce, and disseminate). In addition, there are two continuing steps (analyze and assess). (See ADRP 2-0 for additional information on the army intelligence process.)

2-19. Although PIO follows the intelligence process, it differs in several distinct ways. The first distinction is that the general application of PIO focuses on the collection of information relating to policing, detention, investigations, and criminal activity in a particular area of operations. There are two ultimate objectives of this information: to provide the commander or provost marshal a more complete understanding of the criminal and security threats within the operational environment and to prevent criminal activities. The second distinction is the application of PIO by military police and USACIDC personnel operating in a law enforcement capacity. This capacity allows for the information collection of criminal investigations and is not restricted in the same manner as the intelligence community (non-law enforcement) when collecting against U.S. personnel. The third distinction is that the PIO is not an intelligence discipline. PIO is a policing function conducted in the operations section and conducted by operational elements. PIO staff and analysts coordinate with and synchronize their activities and share police and criminal information with intelligence personnel (within mission and legal constraints). Figure 2-2, page 2-8, provides a graphic representation of how the intelligence process is applied in the context of PIO.



*See appendix A for legal considerations.

Legend:

ACI2	Army Criminal Investigative Information System
BOLO	be on the lookout
COPS	Centralized Operator's Police Suite
DA	Department of the Army
DCGS-A	Distributed Common Ground System–Army
G-3	assistant chief of staff, operations
IPB	intelligence preparation of the battlefield
JWICS	Joint Worldwide Intelligence Communications System
LE	law enforcement
MP	military police
PM	provost marshal
S-3	battalion or brigade operations staff officer
USACIDC	United States Army Criminal Investigations Division Command

Figure 2-2. PIO and the intelligence process

2-20. Throughout the intelligence process (conducted in the context of PIO), military police Soldiers analyze and assess police information. These two integrating activities are performed continuously and simultaneously, and they occur throughout the conduct of all four steps in the process. The process is not linear or sequential; police information is continuously injected. Similarly, police information and police intelligence is continuously pushed into the Army operations process to complement and enhance integrating processes (intelligence preparation of the battlefield, targeting, risk management). Police intelligence is used by military police and USACIDC organizations to focus planning for future police

activities and operations. Police intelligence contributes to the commander's situational understanding, enhances the common operational picture, and adds critical police information to the intelligence process. (See ADRP 2-0 for additional information on the intelligence process.)

PLAN AND DIRECT

2-21. Military police and USACIDC personnel who are planning PIO must first thoroughly understand the commander's intent and concept of the operation. This understanding leads to the identification of information gaps. Planners must then collect all available existing information through reachback, research, or any other means necessary to establish a baseline of knowledge. Information not available may be designed as an intelligence requirement. Planners review the CCIRs, establish priorities, and provide guidance for the management of collection assets. Consideration is given to identifying who, what, when, where, and why.

Plan

2-22. Military police and USACIDC planners preparing to integrate police intelligence access information and conduct collaboration and information sharing with other units and organizations across the operating environment. This planning includes using available means to ensure that planners and analysts have a clear picture of the operational environment before arrival and throughout operations. Planning results in identified police information collection requirements that may become CCIR. The commander's intent, planning guidance, and CCIR drive the planning of PIO. The CCIRs (PIR and friendly force information requirements) drive the planning of the police information collection effort and establish priorities for the management of collection assets.

2-23. The S-3 or G-3, the provost marshal, and the S-2 or G-2 must work closely to ensure that the police information collection plan is synchronized and integrated with the overall information collection effort at all echelons (based on staff planning) to achieve the desired results. Military police or USACIDC personnel with specific collection capabilities or knowledge to perform collection activities are also identified.

2-24. PIO planning and directing activities are broad in nature, but may include—

- Establishing initial police intelligence knowledge through research, reachback, and analysis of the operational environment.
- Participating in intelligence preparation of the battlefield.
- Identifying and managing police information requirements.
- Preparing the police information collection plan.
- Establishing guidelines in the commander's intent to focus collectors.
- Disseminating CCIR and police information requirements to subordinate units and collection assets.
- Providing input and continuous updates to military police running estimates.
- Identifying appropriate collection assets.
- Reviewing intelligence flow to synchronize tasks and resources.
- Evaluating collected and reported information.
- Establishing the communications and dissemination architecture.
- Providing input (in the form of a police information collection plan) and coordinating the development and revision of the intelligence synchronization plan and the information collection plan as mission requirements change.
- Establishing debriefing procedures to gather collected information (includes debriefing patrols with no deliberate collection mission to gain information gathered during the execution of normal operations).
- Participating in crime prevention program analysis, law enforcement, threat working groups, fusion cells, and other applicable meetings. (Chapter 4 discusses working groups, fusion cells, and interagency coordination.)

Developing the Police Information Collection Plan

2-25. Prioritized information requirements are used to develop a police information collection plan. The police information collection plan is prepared based on specific police intelligence requirements, commander's guidance, available collection assets, and other factors. The plan is developed to document and prioritize information requirements and assign against collection assets. Identifying and evaluating potential collection resources are critical to the collection plan. Potential collection assets should be evaluated for availability, capability, and reliability.

2-26. Intelligence requirements are filled through a number of methods and capabilities. Collection to fulfill intelligence requirements may result from deliberate tactical reconnaissance and surveillance efforts, law enforcement surveillance, active police engagement during tactical or law enforcement patrols, and passive observation and collection during the execution of other military police activities. They may also occur through coordination and liaison with other military units (U.S. and multinational), including civil affairs, elements conducting reconnaissance, other policing agencies, and nongovernmental organizations. Military police Soldiers, USACIDC personnel, or civilian law enforcement professionals supporting U.S. forces may also conduct technical assessments based on unique technical training, equipment, knowledge, and capabilities. Information derived from biometrics data and forensic analysis can be used to fill information requirements, provide the critical data needed to complete the analysis, and form relevant and accurate police intelligence.

2-27. The activities of assigned police information collection assets must be identified. Information collectors are typically assigned multiple tasks during the course of a mission. It is imperative that their tasks be prioritized based on the mission, intelligence requirements, and available time. Appropriate tasking orders or requests are issued to request collection assets or a capability beyond those organic to the initiating command. Tasking orders or requests should specify—

- The collection objectives.
- The specific collection tasks (PIR with indicators) and where to look (named area of interest or targeted area of interest).
- The start and termination times for collection or surveillance operations and the time the information is needed.
- The reporting procedures (to whom, how often, what frequency net to use).
- The location and activity of other elements operating in the area of operations.
- The identification and coordination for linguists or special skills personnel (civilian or host nation police, engineers, psychological operations personnel, civil affairs personnel, military intelligence personnel, reconnaissance assets).
- Other necessary information bearing on operations in the area of operations.

Identifying Collection Assets

2-28. The commander or provost marshal, supported by the operations staff, selects and prepares collection assets, based on their capabilities and limitations. Military police and USACIDC Soldiers are trained collectors and highly adaptable to any collection plan. These Soldiers operate in direct contact with the local population, allowing them to identify, assess, and interact with potential sources of information. Military police personnel can effectively collect information as a deliberate collection action or concurrent with the conduct of other missions and functions. Information can be collected actively (through direct observation and engagement with target personnel) or passively (by observing and listening to the surrounding environment and personnel). These collection activities span across operational areas and across the range of military operations, from routine and relatively stable environments associated with law enforcement in support of bases and base camps, to the extreme instability of large-scale combat.

Direct

2-29. To finalize the information collection plan, the staff must complete several important activities and review several considerations to achieve a fully synchronized, efficient, and effective plan. Updating information collection activities during the execution and assessment activities of the operations process is crucial to the successful execution and subsequent adjustments of the police information collection plan. As

military police and USACIDC personnel and leaders assign collection tasks to assets, they provide details that clearly define the collection requirements. The requirements include—

- What to collect (police information requirements).
- Where to collect it (named area of interest or targeted area of interest).
- When and how long to collect (specific times if required).
- Why to collect (answer a CCIR, intelligence requirement, or request for information).

2-30. After a thorough evaluation of the availability, capability, and disposition of the potential collection resources, the police information collection plan is implemented through the execution of asset tasking. The tasking process provides the selected collection assets with prioritized requirements.

2-31. A part of collection planning and directing includes ensuring that coordination with all stakeholders is completed before initiating the collection activities. Possible stakeholders, beyond military police and USACIDC assets, include the supporting judge advocate and other law enforcement agencies operating in the area of operations. This coordination helps to eliminate duplication of effort, interference with an ongoing effort, or violation of legal limitations. In a deployed operational environment, coordination and synchronization is conducted with the S-2 or G-2, and the unit in charge of the area of operations must be notified of activities in their area of operations to ensure appropriate responses to emergencies and to reduce the likelihood of fratricide. Notification also increases the likelihood of receiving information that may be critical to the collection effort.

COLLECT

2-32. Collection consists of collecting, processing, and reporting information in response to police information collection tasks. The collected police information is then available for analysis, production, and dissemination. A successful police information collection effort results in the timely collection and reporting of relevant and accurate information, which supports the production of police intelligence. To be effective, collection efforts are generated and driven by the operations process. The collection efforts must be planned, focused, and directed based on the CCIR, intelligence requirements, or investigative requirements. (See FM 3-55 for additional information on collection techniques and activities.)

Collecting

2-33. The development of a viable collection strategy, including management and supervision of the collection effort, is critical to successful police information collection. Military police, USACIDC, or other collection assets collect information and data about criminal or other threats and police systems, infrastructure, processes, capabilities, and resources. Collection may also target and answer intelligence requirements concerning environmental and geographical characteristics, cultural and ethnic norms, formal and informal authority structures, and other factors affecting policing activities and the criminal environment. A successful PIO effort results in the timely collection and reporting of relevant and accurate information. The collection and management of police information and police intelligence are enabled by, and subject to, the laws, regulations, and policies described in appendix A. These documents ensure the proper conduct of PIO. While restrictions may be present in an operational area where police intelligence targets individuals other than U.S. persons, the ability to collect and share police information and police intelligence is less restrictive. Restrictions and guidance regarding the collection and maintenance of police information and police intelligence may be included in the following:

- U.S. codes.
- Executive orders.
- National Security Council intelligence directives.
- Army regulations.
- Status-of-forces agreements (SOFAs).
- Rules of engagement.
- Other international laws and directives.

2-34. Military police forces support a wide range of operations. The versatility of military police forces allows for significant police information collection opportunities. Chapter 3 provides further detail on

sources and collection of police information. Military police activities that may result in police information collection include the following:

- Deliberate collection activities.
  - Route reconnaissance and surveillance.
  - Area and zone reconnaissance.
  - Law enforcement surveillance.
- Concurrent deliberate or passive collection activities.
  - Tactical patrols (mounted and dismounted).
  - Law enforcement patrols (mounted and dismounted).
  - Cordon and search operations.
  - Checkpoints and roadblocks.
  - Traffic control points.
  - Entry control points.
  - Engagement with local officials and the populace.
  - Detainee operations.
  - Dislocated civilian operations.
  - Site exploitation.
- Routine policing activities.
  - Law enforcement raids.
  - Field interviews.
  - Confinement and detention operations.
  - Emergency response activities.
  - Criminal investigations.
  - Interviews and interrogations.
  - Access control operations.
  - Physical security inspections.
  - Police engagement.
- Open source data. This data can include many sites that cannot be accessed through computers connected to a DOD network (social networking sites, other prohibited sites).

Processing

2-35. Police information processing involves the evaluation of initial information to reduce raw data into manageable portions for analysis and production. Following analysis and production of police intelligence, processing involves an initial evaluation to ensure that the police intelligence is accurate, precise, and relevant. During processing, police information and subsequent police intelligence are prioritized according to current collection and production requirements. The military police and USACIDC personnel responsible for managing police information and police intelligence will—

- Prioritize incoming data according to collection and production requirements.
- Organize police information and police intelligence by category (crime, threat, police systems and capabilities).
- Organize police information and police intelligence by a particular product or user.
- Enter the information into databases.
- Collate police information and police intelligence into interim products.

Reporting

2-36. Established debriefing procedures to gather collected information, including debriefing patrols with no deliberate collection mission to gain information gathered during execution of normal operations, is critical to the collection process. Recording and systematically cataloging information obtained by assigned collection assets and routine patrols are critical to the police intelligence process and may fill important

gaps in the overall situational understanding. Police information may be recorded manually or by direct input into an electronic database. The information is compiled for assessment and analysis by the staff and assigned police intelligence analysts. If raw police information or police intelligence derived from rapid analysis of the information is identified, it is fed into the intelligence process (as applicable).

Note. Due to the restrictions placed on information gathered on U.S. persons, police intelligence must be provided to the provost marshal operations section or military police unit S-3 for further action when the operational area is in the United States and its territories.

PRODUCE

2-37. Production involves the analysis of collected police information and combining it with existing intelligence products to create an accurate, finished police intelligence product. Analysts or staffs create police intelligence products, conclusions, or projections regarding the criminal threat to answer known or anticipated requirements. Production also involves combining new and existing police information and police intelligence to produce updated police intelligence that can be used by commanders, provost marshals, and other members of the staff. Police intelligence products are used to revise military police running estimates, support the military decisionmaking process, and facilitate enhanced situational understanding. During the production phase, military police, USACIDC, or other staff members exploit information by—

- Analyzing the information to isolate significant elements.
- Evaluating the information to determine accuracy, timeliness, usability, completeness, precision, and reliability. It must also be evaluated to determine if it is relevant, predictive, and properly tailored.
- Combining the information with other relevant information and previously developed police intelligence.
- Applying the information to estimate possible outcomes.
- Presenting the information in a format that will be most useful to the user.

2-38. The military police staff deals with numerous and varied production requirements that are based on PIR and intelligence requirements; diverse missions, environments, and situations; and user format requirements. Through analysis, collaboration, and reachback, military police and USACIDC units or the provost marshal section in other units use the collective analysis and production capability of higher, lateral, and subordinate echelons to meet PIO requirements. (See chapter 5 for information pertaining to police intelligence products.)

DISSEMINATE

2-39. Dissemination is the act of getting relevant information to the right personnel, units, or agencies; it is critical to the timely integration of police information and police intelligence. Dissemination entails delivering timely, relevant, accurate, predictive, and tailored police intelligence to appropriate and authorized stakeholders. Dissemination must comply with legal restrictions, mission requirements, and protection considerations. Identifying recipients, determining the product format, and selecting the means of delivery are key aspects of dissemination. Stakeholders may be any element or entity that—

- Possesses an intelligence requirement that can be answered by the police information or police intelligence disseminated.
- Operates in an area of operations that may be directly or indirectly impacted by the police information or police intelligence.
- Possesses an assigned mission that may be directly or indirectly impacted by the police information or police intelligence.
- Provides support to elements impacted by the police information or police intelligence.

2-40. Information presentation may be in a verbal, written, interactive, or graphic format. The type of information, the time allocated, and the directives of the commander, unit, or agency requiring police information and police intelligence influence the information format. In the law enforcement community,

some standard formats and means exist for disseminating police information and police intelligence between agencies; many formats are developed locally. These dissemination conduits are typically closed to personnel and agencies outside the law enforcement community. When conducting operations outside the United States or its territories, police information and police intelligence may be disseminated across tactical mission command systems or appropriate military networks. These networks and systems facilitate the dissemination of answers to CCIRs. (See chapter 4 for information on the dissemination of police intelligence.)

2-41. Military police and USACIDC personnel responsible for police intelligence must identify the appropriate and authorized users of police intelligence products before a mission to ensure that the right products get to the right people at the right time. Typically, police intelligence product users are the personnel or organizations that initiate the requirement and need the products in law enforcement operations in the United States and its territories. Identified law enforcement-sensitive police information and police intelligence are retained in law enforcement channels. When supporting operations in an operational environment outside the United States and its territories, the recipients of police information and police intelligence are typically more broadly defined and are not limited to law enforcement.

2-42. Military police and USACIDC personnel must also determine what method will be used to disseminate police intelligence products. Methods of dissemination may vary from military police reports and police bulletins to threat assessments and information briefs. Geospatial products may assist personnel by highlighting necessary information. (See ATP 3-34.80.) Regardless of the method used, military police and USACIDC personnel must ensure that the products are delivered to the appropriate users when, where, and in the proper form needed. The dissemination of information occurs at every echelon and is entered into the data stream for continued analysis, when applicable. Frequently, when police intelligence products are delivered, additional police information collection requirements are identified.

Note. Local police intelligence files may be exempt from certain disclosure requirements by AR 25-55 and the *Freedom of Information Act*. When a written extract from local police intelligence files is provided to an authorized investigative agency, the following statement below must be included on the transmittal documents: "This document is provided for information and use. Copies of this document, enclosures thereto, and information therefrom will not be further released without the approval of the installation provost marshal."

Granting Access and Sharing Rights

2-43. Granting access to police databases, information, or intelligence ensures that personnel, units, or organizations with requirements and legal authorization for access to police information and police intelligence are provided the means to obtain the required information. Police information and police intelligence may be stored in established law enforcement-sensitive, classified, and unclassified databases and associated programs, networks, systems, and other Web-based collaborative environments. Every effort will be made to ensure that law enforcement agencies operating in the area of operations and any multinational and U.S. military organizations have access, as appropriate and within legal and policy guidelines. Access and sharing rights are granted through responsible national agencies and according to applicable regulations, policies, and procedures for personnel accesses and clearances, individual system accreditation, specialized training for access and systems or database use, and special security procedures and enforcement.

2-44. Sharing access is primarily the result of establishing a collaborative environment for transferring police information and police intelligence. Advances in database technology, combined with an explosion in information sharing and networking among police agencies, has resulted in the development and expansion of these robust information repositories. Army law enforcement personnel continue to access the National Crime Information Center database, but can also turn to databases containing fugitive information from corrections systems and terrorist threat information from the Department of Homeland Security (DHS) and Federal Bureau of Investigation systems. The DOD proprietary automation systems, such as the Centralized Operator's Police Suite (COPS) Information Management System and the Army Criminal Investigative Information System (ACI2), greatly improve interoperability and eliminate seams that criminal and other threats might otherwise exploit. Access to local, theater, DOD, non-DOD, and

commercial databases allow analysts to leverage stored knowledge on topics ranging from basic demographics to threat characteristic information. The challenge for an analyst is to gain an understanding of the structure, contents, strengths, and weaknesses of the database, regardless of the database type.

2-45. Each intelligence discipline has unique databases established and maintained by a variety of agencies. Database access is accomplished through unit or agency homepages via Secret Internet Protocol Router Network (SIPRNET) and the Joint Worldwide Intelligence Communications System. The Distributed Common Ground System-Army (DCGS-A) provides net-centric and enterprised information collection, weather, geospatial engineering, and space operations capability to echelons from battalion and higher. DCGS-A will be the information collection component of the modular and future force battle command system and the Army primary system for information collection tasking, posting, and processing and understanding the threat, terrain, weather, and civil considerations at all echelons. (See chapter 5 for additional information on databases.)

2-46. The laws governing the sharing of police information and police intelligence between the law enforcement and intelligence communities are very specific. Generally, intelligence agencies cannot collect, gather, or store information from law enforcement agencies. For exceptions to this requirement, see EO 12333. Appendix A contains information on sharing information between intelligence communities and other legal aspects of police intelligence collection and sharing.

Updating the Common Operational Picture

2-47. The *common operational picture* is a single display of relevant information within a commander's area of interest tailored to the user's requirements and based on common data and information shared by more than one command (ADRP 6-0). The common operational picture displays relevant information conveyed through reports, automatic updates, and overlays common to all echelons and digitally stored in a common database. It facilitates mission command through collaborative interaction and real-time sharing of information between commanders and staffs.

2-48. To support decisive action, new or updated police information and police intelligence must be regularly input into the common operational picture to provide the most current situation. Military police unit staffs and provost marshal sections coordinate through echelon S-2 or G-2 and S-3 or G-3 personnel to provide continuous results of PIO for inclusion in the common operational picture.

PROCESSING CONTINUING ACTIVITIES

2-49. Analysis and assessment are continuously conducted throughout the intelligence process when applied in the context of PIO. These two continuing activities drive and shape the intelligence process.

Analysis

2-50. Analysis assists commanders, provost marshals, and staffs in framing the problem, stating the problem, and solving the problem. Analysis is the process by which collected police information is evaluated and integrated with existing information to produce police intelligence products. These products attempt to describe the impact of threats on current and future operations.

2-51. During analysis, police information and raw data become police intelligence. Analysis is based on critical examinations of available and relevant information to determine capabilities and trends and to develop predictive analysis for the police and criminal environments and specific criminal threats. The police intelligence analyst specifically analyzes police information and data and conducts predictive analysis in an effort to—

- Determine the course of action that a specific criminal threat is likely to take, enabling commanders, provost marshals, and investigators to identify possible friendly course of actions to counter the threat.
- Predict crime trends in an area of operations, based on extrapolation of statistical crime data, enabling adjustments to patrol and distribution to counter criminal activity.
- Determine presence, capability, and likely actions of organized criminal elements in the area of operations.

- Determine the status and capability of police organizations, infrastructure, and systems.
- Determine capability gaps in existing police organizations, infrastructure, and systems.
- Identify probable trends and effectiveness pertaining to police organizations, based on the analyses of current and historical performance, equipment, and personnel data.
- Identify likely areas of corruption and public distrust of policing systems, based on current and historical data and information.
- Determine patterns in criminal activity and law enforcement in the area of operations that can assist in identifying crime-conducive conditions.
- Determine the construct, capability, and functionality of host nation legal systems, focusing on the police and prisons.
- Determine the identity of individual criminals, criminal groups, and applicable associations.

2-52. During the analysis phase, military police staff and police intelligence analysts evaluate police information and information gained from other sources for relevancy, reliability, and timeliness. Evaluating police information includes determining whether the information is relevant to existing information requirements and if pieces of police information are related. Initially, information may seem irrelevant; however, it should be indexed, queried, and periodically reviewed in future analyses. When reevaluated, this fragmentary piece of information may be fused with additional data and information received to provide an understanding that is not achievable when analyzed as a singular piece of data. Additionally, it must be determined whether the police information is reliable for presentation or if additional confirmation is required. Last, it must be determined if the police information and police intelligence has been collected and analyzed in time to affect operations. (See chapter 4 for additional considerations and techniques specific to police intelligence analysis.)

2-53. Police information and police intelligence must be integrated into the operations process and the common operational picture to affect operations. Integrating police information and police intelligence in tactical plans exploits the information and intelligence gathered, promoting the emergence of the bigger common operational picture. As police information continues to be collected, reported, recorded, and analyzed, a more holistic picture begins to emerge.

Assessment

2-54. Assessment is the continuous monitoring and evaluation of the current situation, especially significant threat activities and changes in the operational environment. Continuous assessment plays a critical role in evaluating the information collected during the PIO process. The continuous assessment of PIO, available information and intelligence, and various aspects of the mission variables are critical to ensuring that the staff—

- Answers the CCIRs and intelligence requirements.
- Provides appropriate input to redirect assets in support of police intelligence collection and assessment of changing requirements.
- Provides clarification to ensure that collection asset elements understand the intent and target to achieve resolution of police intelligence requirements.

2-55. When conducting law enforcement in support of bases or base camps, the effectiveness of policing strategies is continuously assessed by monitoring crime trends or patterns. Effective policing strategies should lead to lower criminal activities in the area of operations.

Chapter 3

Police Information Sources

Military police collect police information from a variety of sources in the area of operations. Information is obtained through—

- Military police reconnaissance, surveillance, threat, and technical assessments.
- Access to law enforcement and intelligence databases and reachback sources.
- Police engagement opportunities with the local population, informants, government officials, nongovernmental organizations, and other military units and law enforcement organizations.

Information collection occurs in operational environments and is focused on intelligence requirements tied to the CCIR or to specific missions being performed. These sources of police information are essential to developing a clearer picture of the networks, trends, patterns, and associations that are critical to combating threat forces and criminal elements, and to identifying and mitigating organizational, system, and infrastructure shortfalls affecting police operations.

INFORMATION REQUIREMENTS

3-1. Collection includes the activities required to gather and report police information to answer intelligence or information requirements. Collection may involve gathering new relevant data and raw information or exploiting existing police intelligence products. Police intelligence requirements drive the collection effort of military police and USACIDC elements. Effective collection efforts are generated and driven by the operations process. They are planned, focused, and directed based on the CCIR, threat assessments, police intelligence, and investigative requirements. No matter the phase of the operation or the operational area, success comes from integrating information gathered during military police collection and assessment activities and conducting analysis and fusion with other sources of information to answer information or intelligence requirements.

3-2. Commanders designate the most important, time-sensitive items of information they need to collect and protect as CCIR; PIO anticipates and responds to the CCIR. As discussed in chapter 2, the intelligence community, law enforcement, or other staff sections and subordinate units may nominate PIR. Police intelligence analysts monitor the PIR and subordinate intelligence requirements for information of value in determining enemy and criminal potential courses of action.

3-3. Requirements related to police and prison systems, policing activities, and criminal environments are of specific interest to military police and USACIDC commanders and staff and to police intelligence analysts. PIR of interest to police intelligence analysts may include the identification of previously unknown criminal or terrorist organizations. This might include methods and routes for the concealment and movement of contraband (weapons, money, drugs). The capability and capacity of host nation police and prison systems and infrastructure, the determination and impact of criminal activity in the area of operations, and the functionality of the criminal justice system are also of specific concern and focus for military police and USACIDC personnel.

3-4. At times, received intelligence requirements may be specific enough to be recognized as having immediate value. Other times, PIR will simply fill in a piece of the puzzle.

INFORMATION COLLECTION

3-5. Collection is a continuous activity. Military police commanders, staff, and USACIDC personnel identify gaps in existing police information and develop intelligence requirements. In turn, a police information collection plan is developed and targets are nominated for collection against the requirement.

3-6. This collection may be completed by many means, to include—

- Military police patrols.
- Police engagement.
- Military police reconnaissance, surveillance, and assessments.
- Criminal investigations.
- Interviews and investigations.
- Evidence collection (biometrics data, forensic evidence).
- Data mining, database queries, and use of reachback centers.

3-7. The reliability of information collected should always be scrutinized to check its viability and credibility. (See chapter 4 for more information on assessing reliability.) This is especially critical when dealing with individuals providing information, regardless of the operational area.

3-8. Military police should be aware of underlying motivations of persons providing information. While conducting law enforcement in support of bases and base camps, persons may be motivated to pass information to military police due to a sense of duty or justice. Military police have the advantage of operating in a culture that has shared values encouraging a sense of duty and honor. This is beneficial when policing military communities. Others may come forward because they may be complicit in criminal activity and are cooperating in hopes of receiving leniency. Some may seek to obtain revenge against an individual who has done something (whether real or perceived) to slight, hurt, or anger them. These are not all-inclusive of the possible factors that may motivate members of a population to come forward to police personnel with information.

3-9. Multiple motivators may compel members of a population to interact and share information with military police operating in support of decisive action. Many of the same motivations mentioned in paragraph 3-8 apply. Additionally, when military police interact with the population, individual sources may be influenced by feelings of support for overall U.S. goals. This support may stem from being victims of a brutal government regime that has been eliminated or subdued or victims of disasters or ethnic strife. In these examples, victims may see the United States as a liberating force. Some may hope for money or support. Motivations of self-interest (such as fear of criminal, terrorist, or insurgent elements) may cause victims to seek out U.S. or other multinational forces. In all environments and circumstances, military police (commanders, staffs, and police intelligence analysts) must be cognizant of the potential motivations behind individuals providing information and their reliability in reporting information on the enemy or criminal threat.

METHODS OF POLICE INFORMATION COLLECTION

3-10. PIO activities are integrated within each military police function. During the conduct of decisive action, military police patrols are arrayed across the area of operations to perform a variety of policing, detention, and security and mobility tasks.

3-11. Police information can be gathered because of passive or active (deliberate) collection efforts during the course of tactical military police patrols, law enforcement activities, or detention operations. Passive collection is the compiling of data or information while engaged in routine tactical missions or law enforcement activities. During passive collection, the military police Soldier or patrol is not on a dedicated reconnaissance, assessment, or collection mission. Passive collection occurs every time military police forces engage with or observe the people or the environment in which they operate. Examples of passive collection include establishing rapport with the local population by establishing and maintaining contact; maintaining efforts to clarify and verify information already obtained through observations or other means; or simply observing activity, lack of activity, or other variations from the normal.

3-12. Active or deliberate collection occurs when military police or other Army law enforcement elements are directed to obtain specific information about an area or target. These requests may be tied to a commander's PIR or provost marshal's intelligence requirements regarding the area of operations or directly tied to specific police investigations. This required information will generally be briefed to military police forces as part of their patrol or mission briefing before mission execution.

SOURCES OF POLICE INFORMATION

3-13. PIO activities are integrated within each of the military police disciplines. During the execution of police operations, detention operations, and security and mobility support, military police perform policing, protection, and other missions. The ability of military police commanders to disperse assets across the area of operations allows for a significant number of specialized sensors and collectors to gather information required to fulfill CCIR, intelligence requirements, and other investigative requirements. In most operational areas, military police patrols are continuously moving in and among the population. This places military police patrols in a unique position to passively observe and actively engage the population to gain general information or satisfy specific intelligence requirements. This continuous presence helps military police build a rapport with the populace in general and with specific persons that may be in a position to provide valuable information.

Military Police Patrols

3-14. Typically, military police patrols are arrayed across the area of operations during the conduct of their assigned missions supporting the military police disciplines. The dispersion of military police patrols (single team, law enforcement unit, or larger squad- or platoon-size elements) makes them effective collection assets. Observation and evaluation skills are inherent in police training; this training further enhances the capabilities of military police patrols to contribute to the collection effort in support of PIO and other requirements. Military police Soldiers regularly observe and interact with the people and environment in which they operate. This regular contact and interaction with the population and environment make military police patrols effective in passive and active collection. Passive collection occurs every time military police Soldiers engage with the people or environment in which they operate. Through this passive collection, military police patrols may fulfill general intelligence requirements applicable to the entire area of operations or military police patrols may discover information that was not requested but has recognized value. That information is provided to commanders and staff, along with the details and circumstances of the discovery.

3-15. Military police patrols may be directed to conduct a deliberate collection mission to obtain specific information about an area or target. These requests may be tied to a commander's PIR, provost marshal's intelligence requirements regarding the area of operations, or specific police investigations. These intelligence requirements will generally be briefed to military police Soldiers as part of their patrol briefing before mission execution. Deliberate preparation specifically for the mission is required. Postmission debriefs are critical to ensure that information collected by military police forces is received by the appropriate staff elements for timely dissemination and analysis. Appendix B provides further information on PIO briefing and debriefing requirements.

Police Engagement

3-16. Police engagement is the foundation to successful, long-term police operations. Successful police organizations interact with, and gain support from, most of the population they serve. This holds true for civilian and military forces in any operational area and is reflected in the military police motto: Assist, Protect, Defend. Police engagement occurs formally and informally anytime military police and USACIDC personnel interact with area residents, host nation police and security forces, and media personnel that allow personnel to gain and share information about threat and criminal activity in an area of operations. (See ATP 3-39.10 for additional information on police engagement.) Data (information) obtained through police engagements must be collected, analyzed, and distributed in a timely fashion to be of maximum value to commanders, Soldiers, and the mission.

3-17. Police engagement is a specific type of information engagement; it occurs between police personnel, organizations, or populations to establish trust and maintain social order and the rule of law. Military police

and USACIDC personnel engage local, host nation, and multinational police partners; police agencies; civil leaders; and local populations to obtain critical information that can influence military operations or destabilize an area of operations. The goal of police engagement is to develop a routine and reliable network through which police information can flow to military police and USACIDC personnel and into the operations process. Based on the tactical situation and designated intelligence requirements, police engagement can be formal or informal.

3-18. Police engagement is an activity with two distinct purposes. Police engagement is used to inform the populace or other agencies and organizations of specific data points and themes in an effort to persuade the population to cooperate with civil and military authorities; mitigate potential or occurring discontent or animosity; provide advanced notification of program, policy, or procedural changes to mitigate potential problems; or gain support and develop a sense of community involvement. Police engagement is also a means to interact with, and gain valuable information from, the population or other agencies and organizations. It is enhanced by regular contact and the subsequent development of trust.

3-19. Formal police engagement is generally conducted as part of deliberate information engagement strategies to gain support or information or to convey a message. This function requires preparation, coordination, and proper reporting after a police engagement activity. Through formal police engagements, military police and USACIDC personnel interact with and influence a wide range of personnel and organizations, to include indigenous or multinational police, civil leadership, governmental agencies, and nongovernmental organizations. It is essential that the information and data exchanged are accurate and consistent with the informational themes and operations they represent.

3-20. Informal police engagement is widespread and less directive in nature; however, it is no less important to the overall success of the mission. Every interaction between military police forces and personnel outside their military police unit has the potential to be an informal police engagement. This level of engagement can occur dozens of times in a single shift. It is not constrained by location, prior coordination, or resources. Building rapport with the community establishes avenues for military police forces to obtain police information. Commanders set the priorities and strategic goals for police engagement and resource police engagement activities. Individual military police Soldiers and teams interacting with the population conduct the bulk of police engagement activities.

3-21. During formal and informal police engagement, military police leaders and Soldiers maintain a deliberate focus and commitment to identifying criminal actors, crime-conducive conditions, and other criminal or policing factors that could destabilize an area or threaten the short- or long-term mission success. Police engagement should be reported through established reporting methods at the conclusion of the mission. This can be done through verbal backbriefs, written patrol reports, automated databases, or other reporting mediums. The information can then be evaluated for further dissemination, analysis, and action as required. If valuable information is identified, an informal police engagement can quickly transition to a deliberate collection effort. (See chapter 5 for additional information on the production and dissemination of police information and intelligence.)

Community Leaders

3-22. Community leaders can be valuable sources of information specific to their areas of influence. They will typically have historic knowledge of persons and activities in their cities, towns, neighborhoods, or bases. While all information received should be confirmed and vetted, community leaders can provide military police personnel, USACIDC personnel, and police intelligence analysts with valuable information regarding the criminal history (persons or groups, new individuals or groups, activities and observations that are out of the norm) in their area. These leaders can also provide insight into the opinions of the population on the police in the area (animosity, levels of trust, perceptions).

3-23. Community leaders in another culture may require time and effort by military police and USACIDC personnel to build a level of trust that will facilitate the open sharing of information. Care must be exercised to ensure that interactions with local leaders are initiated at the appropriate level. Failure to do so may result in individuals feeling slighted or developing an inflated sense and perception of importance among other community members. These assessments should be made early in an operation to determine the appropriate level of engagement.

3-24. Community leaders may include—

- Local government officials.
- Installation or base commanders and staff.
- School officials.
- Neighborhood mayors and watch leaders.
- Religious and tribal leaders.
- Informal leaders.

Initial Complaints and Contacts

3-25. Military police and USACIDC personnel can gain a significant amount of information from initial complaints or calls for response due to specific emergencies or incidents. The initial contact with complainants or individuals at the scene of an incident (witnesses, victims, and potential perpetrators) can result in valuable pieces of information that may not be available with the passage of time. These circumstances provide the recent memory of an event or a valuable observation. It is important that this information be captured and documented as quickly, thoroughly, and accurately as possible. The passage of time will result in faded memories, modified recollections based on external inputs, internal rationalizations and thought patterns, and intentional or unintentional corroboration between witnesses, victims, and perpetrators. Accurate and timely information is critical to the development of accurate assessments by military police personnel, USACIDC personnel, and police intelligence analysts.

Unified Action Partners

3-26. Military police and USACIDC personnel regularly interact with representatives of local, state, and federal law enforcement agencies. In a deployed operational environment, this interaction may also expand to other governmental agencies (Department of State, multinational partners, host nation governmental organizations). Nongovernmental organizations may also be present in an area of operations, depending on the type of operation and the security environment. The development of appropriate relationships with these entities can provide a wealth of valuable information to military police and USACIDC activities. (See chapter 5 for more information regarding interagency coordination.) Joint, interagency, intergovernmental, and multinational coordination may include—

- Host nation police.
- Civilian law enforcement agencies (local, state, and federal).
- Multinational police forces.
- U.S. governmental agencies (Department of State, DHS).
- Nongovernmental organizations (American Red Cross, Doctors Without Borders).

Military Police Reconnaissance, Surveillance, and Assessment

3-27. Military police reconnaissance and assessment capabilities cover a wide span. These task capabilities range from tactical reconnaissance requiring relatively little technical capability to technically specific assessments requiring military police or USACIDC elements with specialized technical training and experience. Tactical reconnaissance missions by military police Soldiers still benefit from the basic law enforcement training that separates military police Soldiers from non-military police Soldiers. Military police and USACIDC Soldiers with specific technical capabilities (such as military police investigator) may augment baseline military police patrols or be employed as part of a multifunctional reconnaissance or assessment team. Capabilities in military police and USACIDC units that facilitate the conduct or support of reconnaissance and assessment include—

- Area, zone, and route reconnaissance.
- Detention requirement assessments.
- Police and prison infrastructure assessments.
- Police and prison capability and capacity assessments.
- Investigative capability assessments.
- Police or legal system assessments.

- Criminal activity threat assessments.
- Personal security vulnerability assessments.
- Terrorism threat assessments.
- Forensic capability assessments.

3-28. Commanders and staffs must fully understand the capabilities and limitations of available military police assets. This prevents collection asset tasking that does not possess the requisite equipment, training, or expertise to complete the mission successfully. Some reconnaissance and assessment requirements require the collection of technical information with capabilities not present in baseline military police elements. Military police reconnaissance efforts may be focused on technical assessments of police and criminal environments, infrastructure, systems, persons, or specific incidents. These assessments may be in support of police or detention missions or in defense support of civil authorities. (See FM 3-39 for a full listing of military police and USACIDC elements and additional information on their specific technical capabilities.) Military police technical expertise may also be integrated with other types of reconnaissance capabilities to achieve a more holistic reconnaissance effort. Teaming or task organization during infrastructure reconnaissance is an example. (See FM 3-34.170.)

3-29. Military police reconnaissance and assessment assist in collecting police information and subsequently developing police intelligence that is required to enhance situational understanding; plan, execute, and assess missions in defense support of civil authorities; and compile the critical information and evidence required for establishing cases for criminal prosecutions (if necessary). Military police reconnaissance efforts conducted early in an operation establish the baseline knowledge and understanding required to influence stability tasks or defense support of civil authorities operations and success in attaining U.S. objectives to assist the host nation or civilian law enforcement in establishing a criminal justice system and governance under the rule of law. In support of decisive action, military police reconnaissance is primarily used to determine the presence of criminal, terrorist, or irregular threats in the area of operations. While conducting route, area, and zone reconnaissance and security missions, military police patrols collect and report information specific to main supply route trafficability, threat presence, key terrain, and other mission variables. Military police patrols also collect information regarding the security environment, locations of host nation police stations, locations of host nation prison facilities, and general population disposition. Military police reconnaissance patrols are capable of satisfying multiple CCIRs for an area of operations and intelligence requirements specific to policing and criminal environments.

3-30. In any operational area, military police may be tasked to conduct surveillance on specific populations, locations, or facilities to satisfy CCIR that have been identified and disseminated through the operations process. Military police units may conduct surveillance and countersurveillance to gain information to help guard against unexpected threat attacks in the area of operations or to gain information critical to understanding, planning, and executing missions in defense support of civil authorities. When surveillance is required in populated areas, military police Soldiers may be a more acceptable asset due to the perception of military police as a law enforcement organization rather than a combat element.

3-31. Military police and USACIDC personnel may be required to conduct surveillance focused on observing specific criminal or threat targets and gathering required information. Law enforcement surveillance may be required to confirm suspected criminal activity; establish association of a suspected criminal in terms of time and place; and confirm association between persons, groups, or entities. Surveillance may be the physical observation of a person or location, visual observation by remote video equipment, or audio observation via technologies employed to intercept audio evidence. Law enforcement surveillance is typically associated with specific criminal investigations. However, law enforcement surveillance may also be performed to conduct assessments (traffic studies, physical security assessments, other security and protection requirements).

Law Enforcement Investigations

3-32. Military law enforcement investigations are official inquiries into crimes involving the military community. A law enforcement investigation is the process of searching, collecting, preparing, identifying, and presenting evidence to prove an issue of the law true or false. (See ATP 3-39.12.) Law enforcement investigations involve activities to collect pertinent information related to a criminal or suspected criminal

activity. These activities determine if a crime has been committed, identify the perpetrators, and collect and organize evidence for enabling a successful prosecution.

3-33. Military police investigate a wide range of crimes, incidents, and accidents in environments where military personnel, assets, and interests are found. These investigations range from simple investigations completed quickly by Soldiers on routine patrols to extremely complicated fraud investigations spanning several years. Investigations may result from information gathered and police intelligence developed during operations that point to a person, network, or location that could be associated with threat forces. At other times, investigations may result from known criminal events or incidents.

3-34. All military police Soldiers are trained to conduct initial investigations. Specially trained military police investigators and USACIDC special agents conduct most formal criminal investigations in the Army. These investigators are trained in technical investigation techniques, to include evidence identification, processing, and preservation critical to successful criminal investigations. Typically, USACIDC maintains purview over criminal cases as outlined in AR 195-2. Military police investigate incidents by identifying, collecting, and preserving potential evidence; observing physical characteristics of locations and items; and conducting interviews with witnesses, victims, suspects, and technical experts.

3-35. Police intelligence analysts support investigators through the collection, collation, and analysis of investigative information from case files that involve allegations and testimony from witnesses, suspects, and victims. Information drawn from these case files can benefit from the inherent analytical framework and scrutiny performed by investigators. Information can also be derived through testimonial evidence or from quality information that has been vetted through the rigor of the criminal investigative process and can result in timely and relevant information and police intelligence in support of criminal investigators. Information gained via criminal investigative files can result in an accelerated generation of police intelligence. In complex cases involving criminal networks or criminal activity crossing jurisdictional boundaries, analysis can be a laborious and time-consuming process.

3-36. Typically, police information and police intelligence associated with criminal investigations are law enforcement-sensitive and remain within law enforcement channels; however, depending on the environment and mission, this police intelligence may be directly integrated into the operations process as discussed in chapter 2. Police intelligence can provide significant, relevant, and timely police intelligence derived from U.S. and host nation criminal investigative efforts focused on active criminal, terrorist, and irregular threats against U.S. and host nation assets and interests. (See ATP 3-39.12 for additional information on law enforcement investigations.)

Interviews and Law Enforcement Interrogations

3-37. Although physical evidence, records, and recordings can often provide critical bits of information about an incident, there is usually a significant benefit in asking questions of persons who have some knowledge of an incident (including preparation and aftermath activity). There are three categories of question-and-answer sessions. The first two are interviews and law enforcement interrogations. The third type is intelligence interrogations. Interviews are conducted with persons who may or may not have information important to an incident and are, by general definition, nonconfrontational. Law enforcement personnel use interviews during the initial-response phase to determine facts regarding an incident. Military police or USACIDC personnel also conduct interviews in an effort to gain background or corroborative information. Law enforcement interrogations are conducted by military police investigators, USACIDC special agents, or host nation security forces with individuals suspected of a crime in which some type of prosecutorial outcome is expected. Law enforcement interrogations are generally more confrontational than interviews. Intelligence interrogations are only conducted by DOD trained and certified interrogators when the status of a person is identified as a detainee and the circumstances of the incident indicate that the matter will not likely be part of a criminal prosecution.

Note. Law enforcement interrogations are separate from intelligence interrogations. Intelligence interrogations are covered by FM 2-22.3. Law enforcement interrogations are covered by AR 190-30 and AR 195-2.

3-38. Some devices (such as polygraphs) are useful in determining a subject's truthfulness. However, no device exists that determines truthfulness with complete accuracy. A polygraph is useful to criminal investigators, but it has limited use across the Army and in routine military police operations or intelligence due to training and certification requirements and the level of expertise required to accurately use the equipment and interpret the data. The USACIDC and the U.S. Army Intelligence and Security Command maintain the only polygraph capability in the Army. The Commanding General, USACIDC, in coordination with the Army Deputy Chief of Staff for Operations and Plans, exercises overall Army staff responsibility for the DA polygraph program and the policy with respect to using polygraphs in criminal investigations. The Army Deputy Chief of Staff for Intelligence provides policy guidance for use of polygraphs in intelligence and counterintelligence applications. (See AR 381-10.)

Law Enforcement Interviews

3-39. The difference between a suspect interview and a law enforcement interrogation is the level of certainty that the investigator has regarding the guilt of the subject and the ability that the subject has to leave at will. An interview is generally unstructured and takes place in a variety of locations (residences, workplaces, police stations). It is conducted in a dialogue format in which investigators are seeking answers to typically open-ended questions, and the guilt or innocence of the person being interviewed is generally unknown.

3-40. There are four main interview categories that investigators use to learn more about crimes, attacks, and incidents. (See ATP 3-39.12 for additional information on law enforcement interviews.) These categories include—

- **Canvass.** Canvass interviews offer the opportunity to talk to large numbers of people quickly to determine if they are aware of the incident and have information that may prove useful to the investigation. Canvass interviews are normally conducted immediately after an incident to determine if someone saw or heard anything that may be important to an investigation or to obtain necessary contact information.
- **Victim.** Victim interviews are question-and-answer sessions with victims of crimes or incidents. The interviewer will often work to establish rapport with the victim by expressing sympathy or understanding as a way of eliciting their support. It is imperative that investigators remain objective at all times during victim interviews.
- **Witness.** Witness interviews seek to obtain information from people who saw, heard, or know information of value about an incident. Many of the same factors that make victim interviews unreliable are also present during witness interviews.
- **Suspect.** Suspect and subject interviews are conducted with persons who are suspected of having committed a crime or caused an incident or with persons who are charged with a criminal offense. All of the factors for obtaining accurate reports from witnesses and victims apply in interviews with suspects; however, the suspect's fear may be magnified.

Law Enforcement Interrogations

3-41. An interrogation is planned and structured. Generally, an interrogation is conducted in a controlled environment that is free from interruption or distraction. An interrogation is monologue-based and progresses with the subject under threat of detention if they attempt to end the interrogation. Based on these factors, the investigator must be reasonably certain of the suspect's guilt before initiating an interrogation. ATP 3-39.12 contains more information regarding interviews and law enforcement interrogations.

EVIDENCE

3-42. Evidence encompasses a wide array of physical objects, testimony, electronic data, and analyses; it is a key source of police information. Evidence consists of objects, material, or data that can provide proof or a high probability of proof that an incident, association, or pattern will lead to a conclusion or judgment. The thoughts, intuition, and opinions of an analyst or investigator are not evidence; however, they can be critical in forming a conclusion or judgment. Effective evidence collection requires planning, preparation, execution, and training. Evidence collection teams can be selected ahead of time to focus training and resources. Digital cameras, rubber gloves, paper bags, boxes, tape, and marking supplies are all tools

required to collect evidence properly. Evidence collection should be performed as a deliberate and methodical process, unless the tactical situation requires a hasty collection effort. Evidence should be handled by as few personnel as possible to avoid contamination and the risk of breaking the legal chain of custody.

3-43. The most recognizable evidence consists of physical items that are related to crimes or incidents, including firearms, illegal drugs, and blood-spattered clothing. Although these items have obvious evidentiary value, their value is increased when placed in the hands of police intelligence and forensic analysts. For example, when properly handled and analyzed, weapons confiscated at the scene of an attack on U.S. forces may provide—through the discovery of fingerprints or deoxyribonucleic acid (DNA) evidence—information on the individuals who last handled the firearms. The barrel and firing pin of a weapon may be an exact match to a weapon used in previous attacks against U.S. or multinational partners. The evaluation of drugs and associated materials may also provide fingerprints or DNA evidence; a chemical analysis may specify where the drug was grown or how it was processed.

3-44. The continuous growth in electronic devices (cellular telephones, digital cameras, laptop computers, global positioning systems) has expanded the types of evidence that can be collected. Photographs, video and audio recordings, recording equipment, computers, and portable data storage (diskettes, thumb drives, memory cards, media players) can provide a wealth of information about a criminal or terrorist organization. The information may include identities, training techniques, weapons capabilities, targets, and locations. Photographic evidence may come from U.S. or host nation security forces, including manned or unmanned aircraft.

Note. Information extracted from electronic devices, photographs, video and audio recordings, and written or printed (hardcopy) documents can be exploited by document and media exploitation teams. If the information contained within these items does not have applicability to military police investigations, forwarding them to document and media exploitation teams for processing could be of great value. (See TC 2-91.8 for additional information.)

3-45. Hardcopy documents are valuable sources of police information. Fingerprints and DNA can be lifted from sheets of paper or envelopes. The type of paper or print used may provide clues as to the system used or the age of the document. Word choices and spelling may provide clues as to a person's background and education. A handwriting analysis may give investigators another means of identifying a specific individual. Lists kept near the computer may be valuable as they may contain passwords, Web site addresses, access codes, e-mail addresses, and aliases. This category of evidence also includes identity papers (passports, visas, licenses, property ownership, shipping documents). An analysis of written and printed documentation may identify locations that an individual has visited, suppliers used, funding sources, and associates. (See ATP 3-39.12 for more information on evidence collection.)

3-46. The forensic analysis of evidence and biometrics identification through numerous modalities (fingerprints, DNA, facial photographs, iris images, firearms and toolmark analyses, forensic examinations) has significantly increased the ability of investigators and police intelligence analysts to add clarity and understanding of events and the involvement of individuals in those events. Forensic collection capabilities require—

- Military police personnel, law enforcement investigators, or trained Soldiers who can recognize, preserve, and collect potential forensic evidence.
- Forensic laboratory examiners who can extract usable information from the collected evidence.

3-47. Biometrics collection capabilities require—

- Personnel who are trained on how to operate the biometrics collection device being used.
- Approved biometrics collection device that is capable of collecting fingerprints, iris images, and facial photographs to DOD standards.
- Biometrics collection and storage capability and manipulation software for the comparison and analysis of biometrics samples.

3-48. Biometrics and forensic identification tools and capabilities can be significant assets to distinguish between friendly, neutral, and threat forces and to establish identity dominance in the area of operations.

Biometrics and forensic identification tools are also critical in criminal investigations to identify an individual, establish an individual's presence at a specific location in relation to time and space, establish a suspect's physical contact with material related to an investigation, or identify an indicator of deception. Military police and USACIDC organizations extensively employ the use of biometrics and forensic capabilities while conducting law enforcement in bases, base camps, or decisive action.

Biometrics Data

3-49. *Biometrics* is the process of recognizing an individual based on measurable anatomical, physiological, and behavioral characteristics (JP 2-0). Biometrics applications measure biological characteristics, which are stored in databases for future comparisons. In addition to the biological data stored in databases, biographic data and personal behavioral traits are also collected for future comparison.

3-50. These characteristics and traits can be useful for tracking individuals, making positive identifications, establishing security procedures, or detecting deception based on measurable biological responses to stimulus. Biometrics data can be used for protection and security efforts and as evidence in investigations and criminal prosecutions. Identification data is combined with claimed biographic data to match an individual to the DOD authoritative databases. During screening, police compare the claimed identity of the subject with the database to verify the identity, discover the identity, or enroll as a new identity. This data includes biometrics data (fingerprints, voiceprints, facial photographs, iris images, DNA).

3-51. Military police and USACIDC personnel and investigators or police intelligence analysts can leverage biometrics data to develop trends, patterns, and associations between individuals. Biometrics data that results in identification, confirmation of an individual's presence at specific times and locations, and determination of truthfulness or deception can be extremely useful in building singular associations to linking groups, cells, or organizations. Linking biometrics data with forensic evidence analysis collected at the scene of a crime or attack can assist law enforcement personnel in criminal investigations or directly feed the targeting process for commanders conducting decisive action in an area of operations.

Note. Biometrics data that is collected during the course of military police operations can be extremely useful to military intelligence personnel in the development of biometrics-enabled intelligence. When not restricted by military police investigations, every effort should be made to forward this data to military intelligence. (See TC 2-22.82 for more information.)

Forensic Evidence

3-52. Forensics is the deliberate collection and methodical analysis of evidence that establishes facts that can be used to identify connections between persons, objects, or data. It is most commonly associated with evidence collected at crime scenes or incident sites; but it also includes methodologies for the analysis of computers and networks, accounting, psychiatry, and other specialized fields. Forensics is typically employed to support legal proceedings that lead to criminal prosecution.

Note. Forensics is used during analysis and subsequent targeting in support of decisive action.

3-53. The USACIDC supports Army forensics requirements through the U.S. Army Criminal Investigations Laboratory. Its facility is stationary due to the nature of the equipment required and other operational requirements.

3-54. Operational requirements for a forward-deployed forensic capability have resulted in the development, deployment, and operation of expeditionary forensics laboratories in the supported area of operations. The USACIDC provides limited deployable forensics laboratories to support commanders as far forward as possible. This expeditionary capability enables timely forensic analyses across a broad range of forensic capabilities, to include latent fingerprints, toolmarks, firearms, and DNA. USACIDC laboratory capabilities may be operated in conjunction with forensic laboratory capabilities resident in sister Services, capitalizing on complementary capabilities to support the operational commander.

3-55. Forensic analysis expands the ability of police intelligence analysts to establish trends, patterns, and associations by providing scientific documentation of relationships between persons, objects, or data. Criminals, terrorists, or other threat elements tend to operate in predictable ways. The analyses and comparisons of fragments left at the scenes of improvised explosive device bombings or sites in an area of operations can identify similarities in the materials used, the construct of the trigger device, and other variables. This can lead to the development of patterns in which events can be associated with the same bomb maker. Information derived from the analyses of the materials used, to include the identification of chemical characteristics, can enable police intelligence analysts to develop associations leading to specific suppliers of those materials. These efforts can lead investigators to the resolution of criminal investigations and assist operational commanders to develop targeting strategies, as appropriate.

3-56. The proper handling of material from crime scenes or incident sites is critical to the success of forensic examination by forensic scientists and technicians. Military police are trained to properly identify, preserve, and collect material, whether in the context of crime scene processing, collecting, or protecting material at an incident or sensitive site. ATP 3-39.12 provides detailed information on evidence collection and preservation.

INFORMANTS AND LAW ENFORCEMENT SOURCES

3-57. In some circumstances, investigators may attempt to gain recurring access and insight into the workings of a criminal or terrorist network. At other times, they will seek similar access to an organization that may knowingly or unknowingly provide support to criminals or terrorists. Army law enforcement personnel frequently obtain information from informants or law enforcement sources. Informants or law enforcement sources may be insiders who are willing to provide such information for a variety of reasons. At times, these persons may be anonymous and available only once or twice. At other times, they will be known to the investigator and may be willing to provide additional information, including information that they obtain specifically at the request of an investigator or analyst.

3-58. Informants are informal contacts that are willing to provide information to law enforcement personnel; there is no formal relationship established between an informant and law enforcement personnel. They can be repetitive sources of information or may provide information only once. Law enforcement sources are managed formally, include strict controls to protect the source, and control contact and information flow. Army law enforcement sources are registered and managed by USACIDC source managers.

Note. Personnel involved with selecting, recruiting, and managing a registered source will normally coordinate and deconflict their sources with other source managers operating in the area of operations. This coordination occurs between USACIDC source managers, HUMINT, and the counterintelligence staff element responsible for counterintelligence and HUMINT operations in the area of operations.

3-59. Individuals may be motivated to serve as informants or law enforcement sources for a variety of reasons. They may be motivated by money, through the assumed protection of their assets, or through payments from investigators. Other informants or law enforcement sources may cooperate with U.S. and law enforcement authorities to prevent prosecution or attack or to direct prosecution or attacks against their rivals. Still others are motivated by feelings of patriotism or justice, or they may simply support U.S. ideals. Some informants and law enforcement sources will be motivated by feelings or revenge toward the organization they are reporting against. It is important for police investigators and police intelligence analysts and staff to understand these motives. At a minimum, this understanding may provide insight into biases and potential areas of informant or law enforcement source unreliability that may make information suspect or warrant deliberate corroboration.

DETAINEE OPERATIONS

3-60. Detained persons are frequently sources of information pertaining to other investigations and trials due to their direct or indirect connections with crime or criminal activity or personnel internal or external to the detention facility. Only trained law enforcement interrogators or investigators are authorized to

interview or interrogate detained or imprisoned individuals for law enforcement purposes. Intelligence interrogations are not law enforcement-related collection activities and, therefore, are executed only by DOD trained and certified personnel. Military police Soldiers are prohibited from conducting or participating in intelligence interrogations of detainees. Trained police personnel, usually military police investigators or USACIDC special agents, may interview or conduct law enforcement interrogations of individuals for specific law enforcement investigation purposes.

3-61. Military police responsible for guarding detained personnel continuously employ passive collection techniques to gather information about the population of U.S. military corrections facilities and detention facilities in support of unified land operations. This passive collection stems from observing the activities, routines, and interactions of detainees in detention facilities. Military police personnel conducting detainee operations use observation and listening techniques to gain and maintain situational awareness critical to protection of the guard force and population in the facility. This passive collection requires attention to detail and significant and continuous attention on the part of the military police forces. Information collected by guard personnel is passed through the chain of command to the echelon S-2 or G-2 using established debriefing procedures.

3-62. Information collected in a detainee environment assists the staff in determining potential security issues. Criminal groups may organize and exert their influence or act out in a violent manner, often targeting detainee facility guard forces or other members of the population. These associations can be critical to law enforcement investigators as they develop criminal cases for crimes committed external and internal to a facility. Regular debriefings for guard personnel operating in close proximity to the facility population can provide the military police staff and police intelligence analysts with the pieces of information necessary to develop and identify the formation of disruptive trends, patterns, and associations in the facility.

3-63. Persons in a facility may provide information relevant to criminal or threat activity outside the facility. This information should be immediately reported to the military police staff for dissemination to the appropriate external element for action. In detainee facilities, the appropriate external element will be the chain of command and the S-2 or G-2 in a deployed operational environment. The external element may also require additional HUMINT or law enforcement interviews or interrogations. FM 3-63 contains additional information concerning detainee operations and associated PIO.

OPEN-SOURCE AND PUBLIC INFORMATION

3-64. Open-source and public information can provide a significant amount of information that may be useful to police intelligence analysts. Trends, patterns, and associations can be determined from open sources (newspapers, press releases, other publications). With the proliferation of data in the public domain via the Internet, police intelligence analysts can find significant information for integration and fusion with existing police information and police intelligence. Individuals, groups, and organizations regularly populate public sites, providing valuable information about their associations, organizations, motivations, and other aspects of their operations and activities.

CONTRACTORS

3-65. A contractor is a person or business that provides products or services for monetary compensation. A contractor furnishes supplies and services or performs work at a certain price or rate based on the terms of a contract. (See ATTP 4-10.) Contractor support in the modern era has expanded significantly. Contracted support often includes traditional goods and services; but it may include interpreter communications, infrastructure, security, and other technical support.

3-66. The integration of contractor information as an element of unified action falls into two categories:

- Passively collected information provided by contractors.
- Contracted personnel directly integrated into operations to fill capability gaps.

3-67. Military police and USACIDC personnel may gain valuable information from contractors. Contractors perform functions throughout an area of operations and may witness events firsthand or through interaction with host nation, U.S. military, multinational, intergovernmental, or nongovernmental

personnel. Military police and USACIDC personnel should not overlook contractors as a possible source of information. Policing capabilities may be contracted and integrated into U.S. military operations to enhance existing capabilities; however, these actions are typically short-term solutions.

INFORMATION REPORTING

3-68. Collected information is useless unless it is provided to the appropriate personnel in a timely manner. Following any collection activity, reports must be compiled for the staff, investigator, or commander requiring the information. The location of physical evidence must also be preserved and reported to maintain chain-of-custody requirements and to allow the timely reexamination of other evidence. Appropriate data should be provided to police intelligence analysts supporting law enforcement and investigative operations. Collection efforts during the conduct of military police operations in support of decisive action (military police reconnaissance, technical assessment, police engagement activities, or data mining) must be documented and provided to the military police or USACIDC personnel and police intelligence analysts for further assessment and analysis.

3-69. Immediate assessment of collected information may lead to the determination that the information has completely or partially answered an intelligence requirement or a PIR. This information should be reported to the appropriate staff, commander, investigator, or provost marshal. Investigators, staffs, and analysts must monitor the CCIR of their higher, subordinate, and adjacent units to support this immediate recognition of CCIR. Time-sensitive information identified as exceptional should be immediately reported through the appropriate staff and command channels for action. (See ADRP 6-0.)

3-70. While it is important to produce police intelligence, it is equally important to share raw information when appropriate. The value of raw information should not be overlooked; an item of information that is not of particular value to one investigation may later be important to an adjacent law enforcement organization, unit, or replacement unit. Terrorists and criminal enterprises have robust information sharing capabilities. Tactics used successfully in one location may be used elsewhere in a matter of hours or days. Information sharing allows staffs and analysts to see a broader picture of the conflict. However, police information or police intelligence may be so important that its existence cannot be immediately shared. In some instances, it may be possible to develop a synopsis of information that conceals the method, technique, or source. When sharing such synopsized information, it is also important to provide contact information so that the receiving element can ask further questions and possibly receive additional information.

3-71. If there is no operational requirement to withhold information after coordination with the supporting judge advocate, efforts should be made to disseminate the information to other law enforcement agencies or other U.S. forces for inclusion into the intelligence process or targeting process depending on the current operational phase. Information dissemination may be in a verbal, written, interactive, or graphic format and may be pushed directly to a cooperating organization. (See chapter 5 for a more in-depth discussion of PIO dissemination.)

3-72. Before the release of police information and police intelligence, it is important to ensure that the release is according to U.S. laws and Army regulations. Sharing information on U.S. persons is generally subject to more restrictions than sharing information on non-U.S. persons. Additionally, individuals detained outside of U.S. territories during military operations typically have fewer protections than those detained within U.S. territories during law enforcement activities. It is very important to coordinate with the supporting judge advocate or higher headquarters regarding legal restrictions on the release of information.

This page intentionally left blank.

Chapter 4

Police Information Analysis

PIO is conducted across the range of military operations. The ability of military police and USACIDC personnel to provide timely and relevant information is enhanced through the integration of police intelligence into military police operations. The results gained from the collection and analysis of police information and the subsequent production of police intelligence drive military police operations. Police intelligence enables law enforcement personnel to proactively identify criminal threats and their capabilities. Military police personnel (enabled by the dedicated analyses of police information and production by military police and USACIDC personnel and police intelligence analysts) provide proactive policing activities and support the interdiction and prosecution of criminals and terrorists who threaten U.S. citizens. Police intelligence products produced through the analyses of police information greatly enhance a commander's situational understanding for supporting elements of decisive action. Critical thinking and predictive analysis techniques applied by trained police intelligence analysts support the formation of a holistic common operational picture and continuously feed the operations process and its supporting integrating processes of intelligence preparation of the battlefield, targeting, and risk management.

RESPONSIBILITIES

4-1. The commander and staff, provost marshal, and law enforcement investigators play a critical role in the analysis process. They determine information requirements needed to plan and execute an operation. The commander provides guidance to the staff to ensure that the analysis effort is integrated with other capabilities of the command (biometrics, forensics, site exploitation) and that it is focused on the CCIRs and priorities. The commander approves or modifies the recommended PIR.

4-2. During the analysis of police information, stakeholders (commanders, provost marshals, law enforcement investigators) must deconflict their priorities to ensure that their limited analysis assets are synchronized and focused in a manner that best supports operational and investigative requirements. Military police and USACIDC personnel and police intelligence analysts must understand the priorities of commanders, provost marshals, and investigators so that decisions regarding analysis priorities are consistent with stakeholder requirements.

4-3. Provost marshals responsible for law enforcement in support bases and base camps, military police commanders, or USACIDC commanders are responsible for PIO in their assigned areas of operation. PIO is an operational function; the S-3, G-3, or provost marshal operations officer is typically responsible for planning and directing PIO. An integral element of PIO is the analysis of police information enabling the subsequent production of police intelligence. The operations element responsible for PIO will typically have a trained Soldier or DA civilian police intelligence analyst assigned. An analyst's skill set includes—

- Technical expertise.
- Knowledge of targets.
- Analytical-technique expertise and experience.
- Research and organizational abilities.
- Inductive reasoning and data-synthesizing abilities.
- Report writing and briefing abilities.

4-4. The Crime and Criminal Intelligence Analysts Course at the U.S. Army Military Police School is the approved course to train police intelligence analysts for military police and USACIDC units. In support of unified land operations outside the United States or its territories, military police and USACIDC personnel conducting PIO coordinate closely with the S-2 or G-2 to ensure that PIO is synchronized and integrated in the intelligence process. In support of bases or base camps, police information and police intelligence typically remain in law enforcement channels due to legal restrictions placed on the intelligence collection of U.S. citizens. See appendix C for more information on legal authorities pertaining to PIO.

4-5. PIO conducted in support bases and base camps in the United States and its territories must be conducted within legal and policy restrictions regarding the collection and maintenance of information on persons in the United States. In these operational environments, law enforcement personnel may collect information and maintain police information and police intelligence on specific individuals and groups if a military nexus exists (an offense that has been committed or evidence that exists indicating that a crime may be committed that has a military connection). Typically, intelligence personnel are restricted from collecting or storing information or intelligence on U.S. persons. The restrictions on collecting and maintaining information and intelligence are typically less restrictive on operations outside the continental United States that deal with non-U.S. persons.

4-6. In support of unified land operations, police information and police intelligence fed into the operations process is fused with other information and intelligence. Police information and police intelligence is integrated within the overall common operational picture to enable commanders to take effective actions against threat forces. Police intelligence analysts, military intelligence analysts and, in selected cases, other law enforcement and intelligence agency analysts provide mutual support to each other. Close coordination and interaction between these elements enhance the effectiveness of PIO. Analysts at all echelons exchange requirements, information, and intelligence products horizontally and vertically throughout the system. (See chapter 2 for more detailed discussion of PIO as part of the operations process.)

4-7. Regardless of the environment, police intelligence analysts analyze information and produce police intelligence products with the objective of supporting commanders, provost marshals, and investigators. The ultimate goal for police intelligence analysts and staff performing PIO is to develop useable intelligence. The trained police intelligence analyst provides the following capabilities to the unit commander, provost marshal, or law enforcement investigator:

- Development of initial background data and knowledge relative to police operations and the criminal environment for a specific area of operations or police investigation.
- Compilation and integration of collected police information for subsequent analysis and dissemination.
- Information and police intelligence on crime and criminal trends, patterns, associations, and other police-related statistics and information that increase understanding of—
  - Offenders, groups, and criminal networks.
  - Criminal funding sources.
  - Specific individuals and groups (supporter, financier, corrupt official, supplier, trafficker, smuggler, recruiter, or other categorization) activities.
  - Geographic relationships of crime and criminals.
  - Population from the perspective of policing and the criminal domain.
- Identification of police information gaps and recommendations of information requirements and collection strategies.
- Identification of systemic issues in police organizations.
- Predictive analyses of crime and criminal activity.
- Recommendations regarding policing and investigative strategies to address crime and criminal threat trends.
- Liaison and information exchange with other military police, law enforcement, civilian, and military elements operating in the area of operations.
- Analysis and police intelligence products tailored to the specific missions or audiences.

- Support to the targeting process.
  - Production of police intelligence.
  - Recommendations for targeting strategies.
- Support to law enforcement and law enforcement investigators in case developments.
  - Identification of background information.
  - Identification of gaps in information and police intelligence relevant to specific investigations.
  - Recommendations for additional law enforcement and investigation efforts.

ANALYSIS OF POLICE INFORMATION

4-8. The purpose of police intelligence analysis is to answer PIR and other supporting intelligence requirements and to produce police intelligence in support of decisive action and law enforcement missions. Analysis in the context of PIO is conducted from a policing and law enforcement investigative viewpoint and is focused on policing activities, systems, capabilities, and criminal dimension in the operational environment.

4-9. Analysis is one of the two continuing activities in the intelligence process and PIO that involves integrating, evaluating, analyzing, and interpreting information from single or multiple sources into a finished product (police intelligence). Police intelligence products must include the needs of the commander, provost marshal, or investigator and be timely, accurate, usable, complete, precise, reliable, relevant, predictive, and tailored.

4-10. Analysis enables the development and recognition of patterns and relationships. Tools and techniques for analysis provide methods to manage or manipulate those relationships and patterns to draw relevant and accurate conclusions. More simply, analysis is a structured process through which collected information is compared to all other available and relevant information to—

- Develop theories and form and test hypotheses to prove or disprove accuracy.
- Differentiate between the actual problem and the symptoms of the problem.
- Enable the analyst to draw conclusions.
- Develop threat courses of action.

4-11. Analysis requires manipulating and organizing data into categories that facilitate further study. Patterns, connections, anomalies, and information gaps are assessed during the analysis of police information. The initial hypothesis and data comparison is accomplished by—

- Observing similarities or regularities.
- Asking what is significant.
- Categorizing relationships.
- Ascertaining the meaning of relationships or lack of correlation.
- Identifying requests for information and the need for additional subject matter expert analyses.
- Making recommendations for additional collections, to include locations and time constraints, for the reconnaissance and surveillance matrix.

4-12. There are many categories of analyses used to organize and guide the analytic process. Analysis is a very broad term without consistent nomenclature, especially across analytical disciplines. Military police and USACIDC personnel apply a policing and investigative focus in the use of analytic methods.

ANALYTICAL FOCUS AREAS

4-13. Military police and USACIDC personnel analyze, synthesize, and develop analytical products based on available information. Analytical techniques use cognitive thought and require analysts to deduce, induce, and infer while working toward conclusions that answer specific information or intelligence requirements. Depending on specific requirements and missions, categorizing the effort helps to focus the analyst's efforts toward specific data, considerations, and results.

COMMUNICATION ANALYSIS

4-14. Communication analysis (formerly referred to as toll analysis) depicts telephone records, to include the analytical review of records reflecting communications (telephone, e-mail, pager, text messaging) among entities that may be reflective of criminal associations or activity. It may result in the identification of the steps required to continue or expand the investigation or study.

4-15. While communication analysis has been a key element in law enforcement investigations, advances in technology have elevated the importance, capability, and scope of tracking communications activities of individuals and organizations during investigations. Communications analysis can enable an analyst to document incoming and outgoing calls, telephone locations, date and time of calls, call duration, and other communications data. This facilitates the identification of communication patterns and associations relative to specific communications equipment.

CRIME AND CRIMINAL TARGET ANALYSIS

4-16. Crime and criminal target analysis enables staffs and analysts to identify potential criminal targets and crime-conducive conditions, including vulnerability assessments and the relative importance or priority for targeting. A key aspect to performing a crime and criminal target analysis is the determination of the effect desired and the optimal method of targeting.

4-17. Military police and USACIDC personnel use crime and criminal target analysis to identify criminal targets and crime-conducive conditions and to make recommendations on appropriate engagement methods. Targeting could range from police (information) engagements to the application of nonlethal and lethal force, depending on mission and operational variables.

CRIME AND CRIMINAL THREAT ANALYSIS

4-18. Crime and criminal threat analysis is a continuous process of compiling and examining available information concerning potential criminal threat activities. Criminal and terrorist threat groups or individuals may target U.S. military organizations, elements, installations, or personnel. A criminal threat analysis reviews the operational capabilities, intentions, and activities of the threat group and the operational environment in which friendly forces operate. Criminal threat analysis is an essential step in identifying and describing the threat posed by specific groups or individuals.

4-19. Criminal threat analysis techniques are regularly applied to antiterrorism, physical security, and conventional criminal activities. Threats operating against U.S. interests may use criminal and terrorist tactics, techniques, and procedures that make them viable targets for friendly criminal threat analysis. Crime and criminal threat analysis supports the production of the crime prevention survey and other threat assessments.

CRIME PATTERN ANALYSIS

4-20. Pattern analysis is the process of identifying patterns of activity, association, and events. A basic premise is followed when using this technique. Activities, associations, and events are identifiable, characteristic patterns. (See ATP 2-33.4 for additional information on pattern analysis.) Crime pattern analysis looks at the components of crimes to discern similarities in the areas of time, geography, personnel, victims, and method of operation. Crime pattern analysis is critical when facing a threat in which doctrine or the method of operation is undeveloped or unknown, but it is necessary to create a viable threat model. Crime pattern analysis is particularly applicable in law enforcement and investigative applications and against threats.

4-21. Crime pattern analysis can be employed using several different analytical methods. These methods include—

- Crime and criminal trend analysis.
- Pattern analysis.
- Link, association, and network analysis.

- Flowcharts.
- Time, event, and theme line charts.

FUNCTIONAL ANALYSIS

4-22. Functional analysis is focused on assessing a threat disposition and action for a particular type of operation. Functional analysis is based on the concept that certain operations or tasks are explicitly unique; certain actions or functions must be implicitly performed to accomplish those operations or tasks. The functional analysis provides a framework for understanding how specific threats make use of their capabilities. Functional analysis is applicable regardless of how the threat is characterized. Specific knowledge and training enable analysts to apply the functional analysis process, which effectively addresses specific threat types. (See ATP 2-01.3 for additional information on the functional analysis.) Functional analysis graphically depicts the threat use of each capability and typically—

- Determines the threat objective.
- Determines the functions to be performed to accomplish the identified threat objective.
- Determines the capabilities available to perform each function.

4-23. In the context of the functional analysis, military police staff and police intelligence analysts also conduct a criminal threat risk analysis. The purpose of the criminal threat risk analysis is to determine the relative risk that a specific criminal threat poses to military forces, assets, or the population in general. A heightened criminal threat probability typically drives a more rapid and focused action on the part of military police, investigators, and other police agencies working in concert.

FINANCIAL CRIME ANALYSIS

4-24. The purpose of a financial crime analysis is to determine the extent to which a person, group, or organization is receiving or benefiting from money obtained from sources that are not legitimate. Financial crime analysis is applicable to many criminal investigations (including organized crime, drug trafficking, human trafficking, and property crime) particularly those involving crimes where money is a motivating factor. This type of analysis focuses on financial and bank records, the development of financial profiles (through net worth analyses, identifications of sources, and applications of funds), and business records. Examples of crimes in which financial crime analysis is relevant include—

- Fraud.
  - Insurance fraud.
  - Contract fraud.
- Bribery.
- Embezzlement.
- Theft.
  - Deception.
  - Product substitution.
- Racketeering.
- Other economic crimes.

TERRAIN AND GEOGRAPHIC DISTRIBUTION ANALYSIS

4-25. Terrain analysis is conducted to understand the effects of terrain on operations. A terrain analysis in policing operations has the same primary objective as conventional operations—to reduce the commander's operational uncertainties as they relate to terrain. Terrain analysis is used heavily for specific police activities (special-reaction team operations, protective services, large-scale crime scene or search operations). Terrain analysis is also critical in the context of physical security applications and in antiterrorism and other protection operations. Typically, the factors of observation and fields of fire, avenues of approach, key terrain, obstacles and movement, and cover and concealment are used in terrain analysis efforts; however, the application of each aspect is significantly different from conventional operations due to the policing and protection focus. Geospatial products may enhance terrain analysis and geographic distribution analysis. (See ATP 3-34.80.)

4-26. Geographic distribution analysis seeks to identify and map the occurrence of a specific activity or incident over a particular geographic area and emphasizes the use of graphics to depict the activity and emerging patterns. This further enables the analyst to identify hot spots and facilitates geographic profiling to predict potential occurrences. Geographic distribution analysis can also display locations of connected crime series, enabling the determination of probable bases of operation, offender residences, or other key locations.

4-27. Geographic distribution analysis tools vary from incident pin mapping (using a physical map and colored pins, stickers, or other methods to identify specific occurrences in an effort to recognize a pattern) to geographic information system software technology. Police intelligence analysts use geographic information system software to conduct geographic distribution analysis, allowing the use of layered graphics and blending geographic data and descriptive information to map places, events, and criminal incidents for analysis to identify patterns and associations.

POLICE INFRASTRUCTURE AND CIVIL CONSIDERATIONS ANALYSIS

4-28. Infrastructure analysis generally focuses on two types of civil information (basic infrastructure data and the actions of local populations). Performing the analyses of infrastructure and populations is especially important when conducting stability or defense support of civil authorities, to include operations in support of police and prisons, the establishment of the rule of law, and antiterrorism operations. The defining areas, structures, capabilities, organizations, people, and events elements are used by the Army to guide the assessment of the six characteristics or variables affecting the tactical variable of civil considerations. ATP 2-01.3 contains additional information on the analysis of infrastructure and civil considerations.

4-29. Military police have developed the POLICE memory aid to guide the assessment of civil considerations that is focused on police activities and systems and the criminal dimension. In the context of PIO, the overall goal of infrastructure analysis is the identification and analysis of issues that affect police and prison infrastructure and the population. This identification enables commanders to identify criminal threats, potential disruptive events, and law enforcement operations.

POLICE OPERATIONS ANALYSIS

4-30. Operations analysis refers to the study of activities necessary for the day-to-day functions of a specified organization. It is a management tool used to identify problem areas and improve operations. In PIO, these activities cover a range of possible activities (patrol and resource allocation, administrative functions, logistic support, training, investigations, and other critical policing activities). Operations analysis can be focused internally or externally. Military police may conduct an operations analysis to assess and improve their own operations. In the context of PIO, military police conduct assessments of host nation policing and prison capabilities. This mission is typically conducted during, but is not limited to, stability operations.

PREDICTIVE ANALYSIS

4-31. Predictive analysis employs multiple analytical techniques to analyze current and historical information and intelligence to predict future activities, behaviors, trends, or events. It captures statistical and historical data and, through the analyses of previous and current associations, uses patterns and trends to enable the analyst to predict potential incidents or activities. Predictive analysis is not guessing; it is based on reasoning, deliberate analysis, and appropriate analytical tools and methodologies. It may focus on specific criminal or disruptive individuals, groups, or organizations to determine their capabilities, vulnerabilities, intent, and probable courses of action. Predictive analysis can also be valuable in identifying crime trends and extrapolating future patterns. The value in predictive analysis lies in enabling commanders and provost marshals to make informed decisions regarding threat mitigation and interdiction. It also enables them to make adjustments in task organization and asset distribution to counter negative or disruptive trends.

CRIME PATTERN ANALYSIS

4-32. There are many tools and techniques available to staffs and police intelligence analysts to focus efforts and maximize the effectiveness of the analyses. These tools and techniques are used to recognize trends, patterns, and associations. These techniques are not used as singular methods but, rather, are sometimes concurrent and often consecutive activities that complement and enhance each other. Qualitative and quantitative data are used in these techniques. Qualitative data refers to nonnumerical data. This type of data lends itself to content analysis and the identification of historical trends, patterns, and associations. Quantitative data is typically numerical, and the analysis of quantitative data is typically statistical in nature.

4-33. Military police and USACIDC personnel and police intelligence analysts use these tools and techniques to fuse disparate information in police intelligence products. They are also used to help in developing crime trends and patterns and performing predictive analysis. These tools and techniques help military police and USACIDC personnel determine what crimes or events are taking place, where they will be located, what time they will occur and, oftentimes, what future activities may occur. When coupled with S-2 or G-2 efforts supporting decisive action, these tools may link crimes to threat group activities that may impact the common operational picture, intelligence preparation of the battlefield, and CCIR. Throughout the analysis of police information and the production of police intelligence, relevant information and intelligence is provided to the operations and integrating processes.

TREND ANALYSIS

4-34. Trend analysis refers to the gathering, sorting, prioritizing, and plotting of historical information. It provides analysts and supported commanders, provost marshals, and investigators with a view of how events, elements, and conditions have affected police operations and criminal dimensions in the past. Statistical analysis allows an analyst to extrapolate data to predict future actions or occurrences. This historical perspective provides continuous insights for developing coherent possible or probable courses of action for the criminal threat and the ability to predict specific occurrences. The results of trend analysis are sometimes referred to as statistical intelligence. For PIO, statistical intelligence refers to data collected from police reports, raw data files, and other historical data assembled into useable maps (or other geospatial products), charts, and graphs. This information is used to indicate past crimes and trends, patterns, or associations. This information must be maintained and updated to be effective.

4-35. Police intelligence resulting from trend analysis is the baseline that analysts and units should use as a statistical point of reference for future analyses. Trends can be depicted in many different formats, to include—

- Graphs.
- Maps (or other geospatial products).
- Narrative summaries.

4-36. Ideally, trend analysis products should be depicted visually and in a report format. A trend analysis is extremely useful for—

- Specific occurrences.
  - Traffic collisions.
  - Driving while intoxicated and other alcohol-related incidents.
  - Juvenile crimes.
  - Assaults (simple, aggravated, domestic incidents).
  - Sex crimes.
  - Suicide.
  - Drug offenses.
  - Homicide.
  - Larcenies.

- Gang activities.
- Security-related incidents (perimeter breaches, unauthorized entry, exclusion area violations).

- Offenses by specific persons (persons with a criminal history).
- Locations and times of specific offenses.
- Complaints against the police.
- Number and type of citations.
  - DD Form 1408 (*Armed Forces Traffic Ticket*).
  - Other locally used forms.
- Calls for assistance.
- Response times.
- Special-event attendance statistics.
- Traffic flow.
  - Specific intersections or roadways.
  - Entry control points and traffic control points.
  - Traffic peaks (including daily, seasonal, holiday and special events).

4-37. Comparisons of recorded historical police and criminal events and associated trends derived through statistical trend analysis can provide clues to criminal and threat capabilities, modes of operation, and activities in relation to time and location. Police intelligence derived from trend analysis enables the redistribution of police assets to address specific policing problems. Trend analysis can also determine organizational problem areas and facilitate organizational adjustments or changes to improve operations.

PATTERN ANALYSIS

4-38. Pattern analysis helps an analyst identify indicators of threat activity. A pattern analysis is based on the premise that activities conducted by individuals, groups, or organizations tend to be replicated in identifiable ways. A thorough analysis of seemingly random events can result in the identification of certain characteristic patterns. Pattern recognition defines the ability of an analyst to detect and impose patterns on random events, allowing for the separation of relevant information from irrelevant information. Pattern recognition can enable an analyst to make assumptions and predictions based on previous historical patterns of activity. See ATP 2-33.4 for details in pattern analysis. During PIO, pattern analysis looks for links between crimes and other incidents to reveal similarities and differences that can be used to help predict and prevent future criminal, disruptive, or other threat activities.

4-39. Numerous tools and techniques can be used to display data and establish patterns for the analyses. These tools and techniques include—

- **Incident maps and overlays.** Incident maps and overlays are sometimes referred to as a coordinate register. They document cumulative events that have occurred in the area of operations. This technique focuses on where specific events occur. Incident maps and overlays are a critical tool in geographic distribution analysis. Geographic information system tools can be helpful in producing incident maps with overlay data. Figure 4-1 provides an example of a basic incident map.
- **Pattern analysis plotting.** This tool focuses on identifying patterns based on the time and date of occurrences.

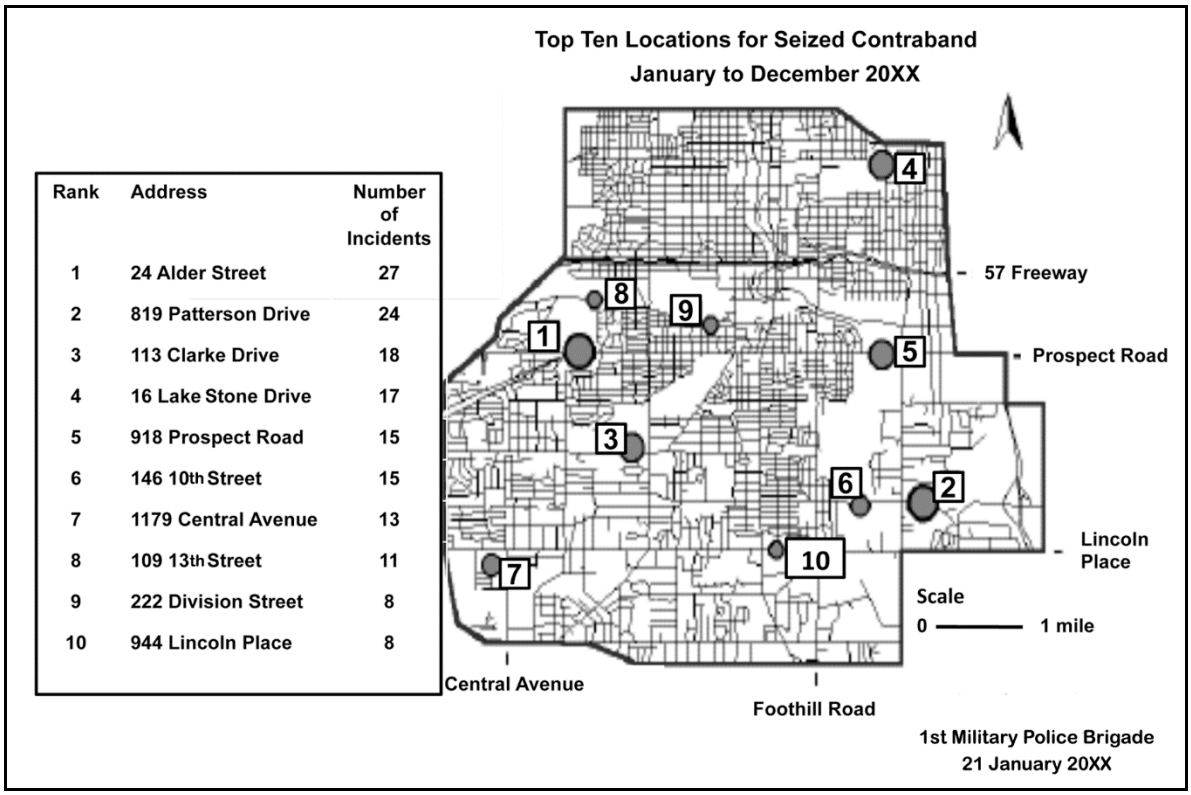


Figure 4-1. Example of an incident map

LINK AND NETWORK ANALYSIS

4-40. Link analysis is a technique used to depict relationships or associations between two or more entities of interest graphically. These relationships or associations may be between persons, contacts, associations, events, activities, locations, organizations, or networks. Link analysis is sometimes referred to as an association or network analysis. Police intelligence analysts use link analysis to find and filter data that will locate people; identify ownership of assets; and determine who is involved, how they are involved, and the significance of their association. Link analysis can be especially valuable to active, complex investigations. It provides avenues for further investigation by highlighting associations with known or unknown suspects. Link analysis is normally tailored to a specific investigation; therefore, dissemination is generally restricted to other law enforcement or military personnel acting as part of the same investigation.

4-41. The main reason for using link analysis is to provide a visual depiction of the activities and relationships relevant to the investigation or operation being conducted. The visual depiction of the network gives meaning to data absent from a written depiction because it would be too confusing to comprehend. Link analysis is a good tool for generating inferences based on what is known about the current relationships of the known individuals being targeted. The network charting tool can depict the ever-changing alliances and relationships relevant to the investigation or operation.

4-42. The results of link analysis are typically depicted on a chart, matrix, link diagram, or other graphic medium (to include geospatial products). An effective link analysis should depict the existence and strength of relationships between two or more entities of interest (individuals, organizations, businesses, locations, property). Figure 4-2, page 4-10, shows an example of standard link analysis symbology; and figure 4-3, page 4-10, shows an example of a link diagram. ATP 2-33.4 provides additional information on link analysis and other analytical tools.

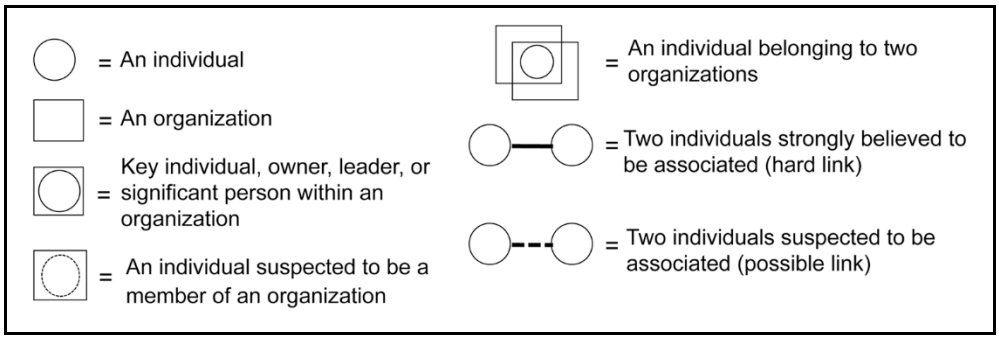


Figure 4-2. Example of a standard link analysis symbology

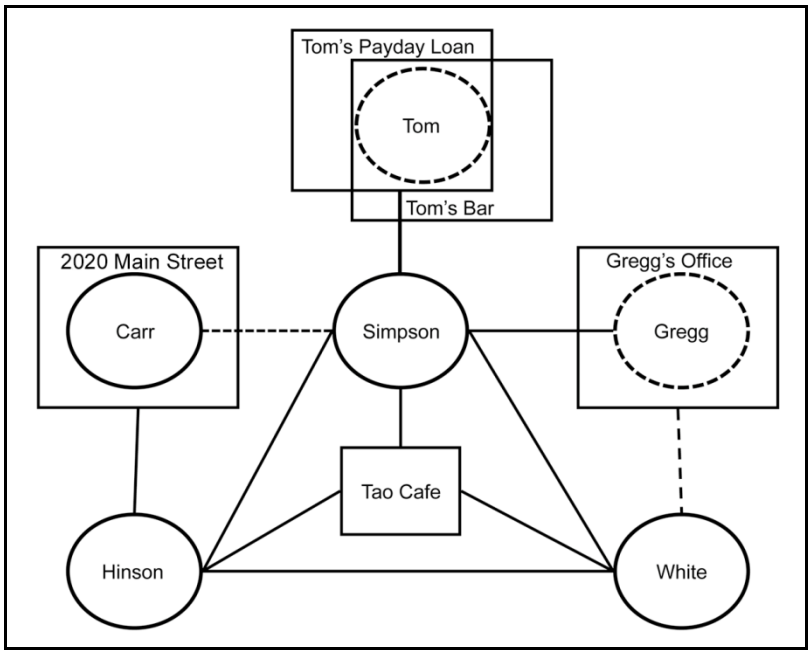


Figure 4-3. Example of a link diagram

4-43. A link analysis assists an analyst with—

- **Determining the focus of the analysis.** The focus may be on an individual, organization, business, location, or other entity. The analysis will attempt to answer if—
  - Possible associations or relationships exist among the entities of interest.
  - Patterns or trends are apparent.
  - Information can be inferred from the gathered data.
- **Gathering or assembling information.** The collection of information during Army law enforcement operations in the United States or its territories must have a military nexus and support a law enforcement activity. These restrictions may not apply when supporting operations outside the United States or its territories, depending on the phase of the operation and SOFAs in the host nation This information may include—
  - Field interview cards or reports.
  - Pawnshop databases.
  - Vehicle records.
  - Traffic citation reports.

- Patrol reports.
- Initial investigative reports and statements.
- Crime scene or incident narratives, photographs, and sketches.
- Communication and computer records.
- Collected evidence and laboratory analyses (biometrics data, forensic evidence).
- National Crime Information Center data, be-on-the-lookout (BOLO) alerts, calls for service, or other police data.
- Case files.
- Surveillance reports.
- Financial reports.
- Public records.
- Local or regional databases.
- Other agency reports.
- Intelligence reports (open source intelligence, HUMINT, electronic intelligence, imagery intelligence).

- **Determining the type of diagram or matrix to be used.** A link diagram graphically displays connections between individuals, organizations, and activities. Link diagrams can clarify what is known and what may be missing about the network being charted. To remain relevant and effective, link diagrams must be continually updated to include relevant reported information. Association matrices establish the existence of known or suspected connections between individuals. An association matrix may be reflected as an array of numbers or symbols in which information is stored in columns and rows. Figure 4-4, page 4-12, provides an example of a basic association matrix. Activity matrices are used to determine connections between an individual and organizations, events, locations, or activities (excluding other individuals). The appropriate association or activity matrices reveal who knows whom, who participated in what, who went where, and who belongs to what group.
  - **Rough draft.** This graphic may depict associations (such as weak or unconfirmed, strong or confirmed, or a significant member of an entity or group).
  - **Link analysis graphic and depicting associations.** See figure 4-2 for an example of analysis symbology.

4-44. Flowcharting is a series of analytical techniques that describes and isolates the distribution pattern of a criminal organization, their method of operation, and the chronology of crime-related activities. Flowcharting allows an analyst to isolate associations and patterns identified through previous analysis techniques to depict a specific person, organization, entity association, or activity without the extraneous information that may be present in earlier analysis techniques. The flowchart may also show gaps in time that need to be accounted for. When combined with ventures and link analysis charts, a flow chart can assist personnel in understanding relationships and where the involved associates fit into the scheme of the criminal or terrorist enterprise. Some flowcharting techniques include—

- **Activity.** This technique depicts the key activities and modes of operation of an individual, organization, or group. Activity flow analysis is used to view criminal actions and identify methods of operations to determine likely suspects. Most criminals will leave unique indicators when committing a crime. These indicators are specific details, common to the specific criminal or organization, and may include details regarding weapons, notes, vehicles, targets, or the number of people involved.
- **Time event and theme line.** These tools establish chronological records of activities or related events. The charts may reflect activities of individuals or groups and depict large-scale patterns of activity. Figure 4-5, page 4-12, shows an example standard symbology used in time-event charts, and figure 4-6, page 4-13, shows a basic example of a time-event chart.
- **Commodity.** This technique displays a graphic representation of the movement of materials or products (weapons, materials, drugs, money, goods, services) in a criminal or other network, enabling an analyst to discern the organization hierarchy.

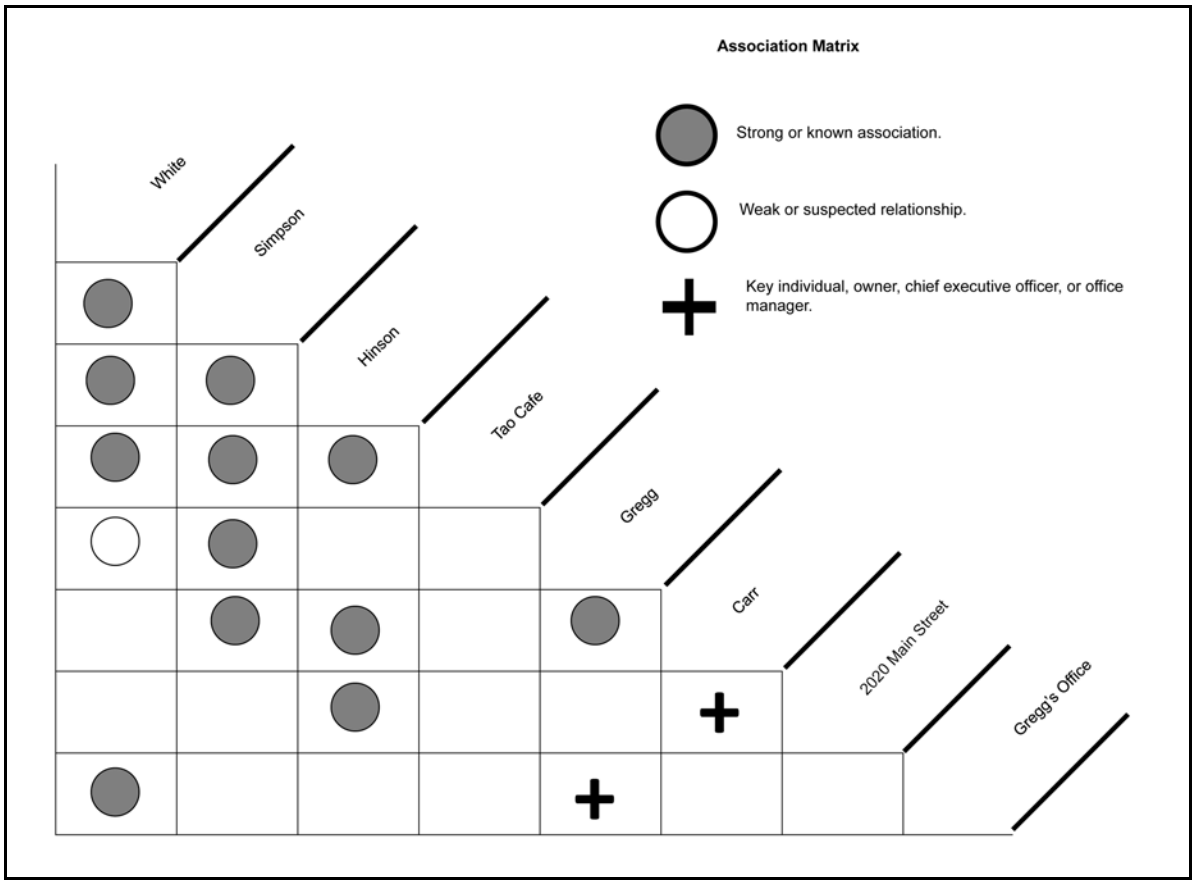


Figure 4-4. Example of an association matrix flowchart

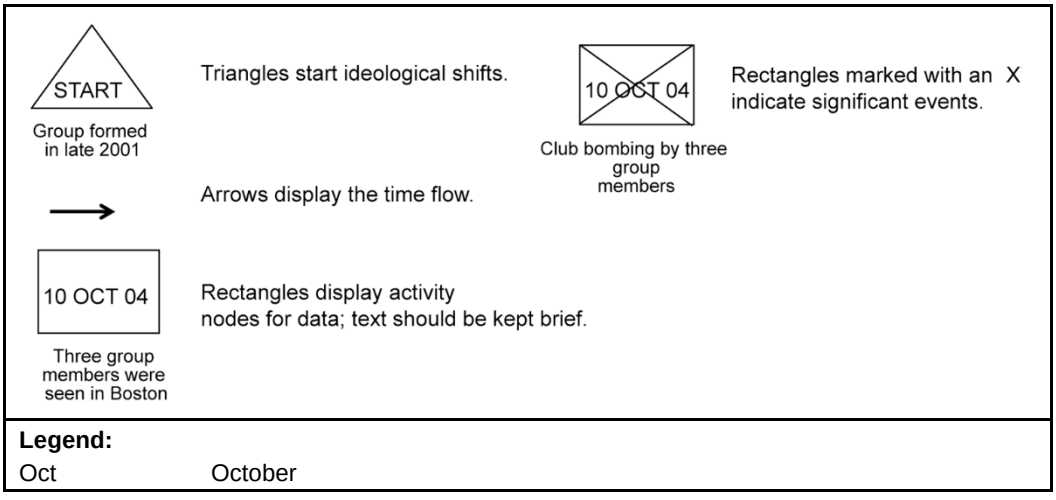
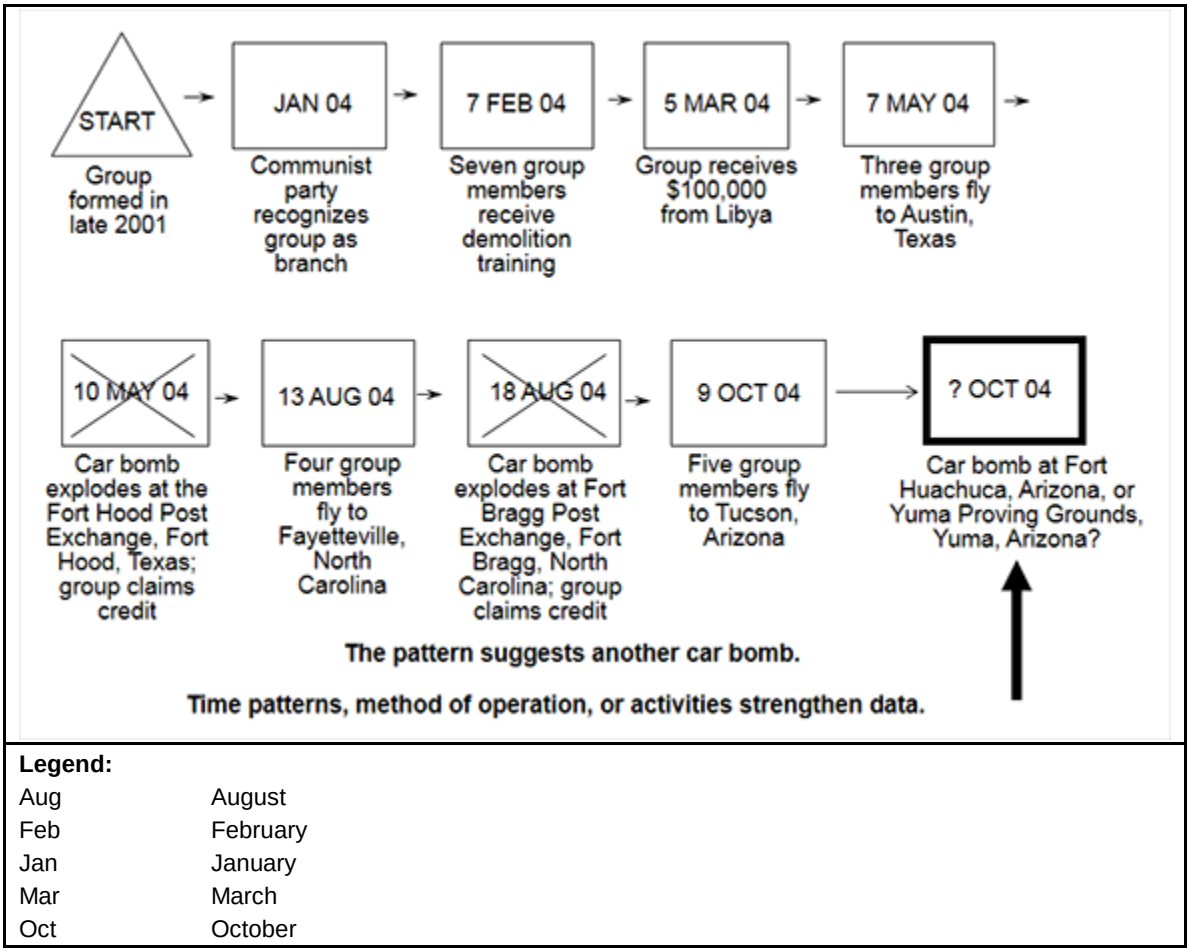


Figure 4-5. Example of standard time-event symbology



Legend:

Aug	August
Feb	February
Jan	January
Mar	March
Oct	October

Figure 4-6. Example of a time-event chart

STATISTICAL DATA

4-45. Statistical data can be drawn from diverse sources and depicted in numerous manners. Statistical data can be very useful in determining frequencies, trends, and distributions; however, the data also has limitations. Analysts and statistical data users must be aware of the limitations and resist the desire to infer more than the presented data can accurately portray. Statistical data may be presented in charts displaying—

- Frequencies (using bar, pie, and Pareto charts).
- Trends (using bar and line charts).
- Distributions (using geographic information system, trend lines, or other formats).

4-46. Data requires different types of statistical tools to present effective information in a clear and understandable manner. For example, an analyst is required to depict the number of reported incidents by the host nation population of contraband markets or movement of contraband material within a specific area of operations, quantifiable data, or data that can be counted or put into a particular category would be required. The staff or analyst may depict these statistics on a frequency chart. A frequency chart may also be used to identify traffic accidents, fatalities, or injuries and pinpoint specific offenses (aggravated assaults, sexual assaults, larcenies, juvenile offenses). However, if an analyst wanted to portray how long this activity has been occurring, they could depict the data on a trend chart (such as a line graph). The data presented in graphic form should also be tabulated so that the information is readily available to back up the chart and show how data was tabulated. Supporting geospatial products may enhance the presentation.

POLICE INTELLIGENCE COLLECTION FOLDERS

4-47. Extensive working files should be created and maintained on persons, groups, or organizations that are the subject of law enforcement investigations in support bases or base camps or are targeted by the U.S. military and its partners. Collection folders contain background information, analysis, spot reports, bulletins, or any other information required by an analyst to develop an understanding of the current problem. The analyst compiles the data needed to conduct the analysis and produce police intelligence products. These collection folders are created to establish and maintain graphic and documentary reference material and record analyses. These folders should be maintained separately from law enforcement investigative files; access to the folders should be controlled.

4-48. The baseline content of police intelligence analysis record holdings should include—

- Names.
- Locations.
- Threat indicators of criminal behavior.
- Threat signs and symbols.
- Threat effects.
- Source identification and where the specified information can most likely be obtained.

4-49. Critical information associated with a given threat includes (at a minimum)—

- Patterns.
- Method of operation.
- Equipment or supplies used in the commission of a crime or terrorist act and how those items were used.
- Known and suspected associations.
- Areas of operation.

4-50. Many ideological threat groups place great emphasis and importance on symbolism. This is also true of the gang culture in the United States. Unique characteristics related to specific threat groups should be included in the working files—

- Important dates.
- Times.
- Symbolism.
- Method of operation.
- Signatures.

CRIME AND CRIMINAL THREAT ANALYSIS

4-51. Compiling, examining, and reexamining the available information concerning potential threat activities is a continuous process. Threat analysis is conducted by intelligence and law enforcement organizations to determine and monitor current and potential threats. It is an integral element in the production of a threat assessment. The relevancy of a threat assessment depends on how current the threat assessment is.

4-52. Intelligence and criminal information, threat information, and asset vulnerabilities are considered when conducting a criminal threat analysis. Intelligence and criminal information provide data on the goals, method of operation, techniques, strategies, tactics, and targets of individuals and groups. Threat information can lead to the identification of criminals and criminal groups. A criminal threat analysis must be a continuous activity to account for inevitable changes in the operational environment. As vulnerabilities are reduced in some areas, they may increase in others. Threat elements assess their targets in relation to one another. An increase in the security posture of one asset may increase the attractiveness of another asset as a target, even though the asset has not reduced its security. Changes in missions, tasks, and personnel may have an impact on the status of the current criminal threat analysis.

4-53. Criminal and terrorist threat groups or individuals may target DOD organizations, elements, installations, or personnel. A criminal threat analysis reviews the factors of operational capabilities,

intentions, and activities of a threat group and the operational environment in which friendly and threat forces operate. Criminal threat analysis is an essential step in identifying and describing the threat posed by specific groups or individuals. Criminal threat analysis is most typically associated with terrorist activity, but the same techniques are applied to conventional criminal activities.

4-54. A threat assessment integrates a criminal threat analysis with criticality and vulnerability assessments that are required for prioritization of assets by commanders and provost marshals to counter threat activities and associated risks. Vulnerability and criticality information helps the analyst to identify security weaknesses and potential high-risk targets. Several factors are considered during a criminal threat analysis to determine the level of threat posed against specific U.S. interests (material, structure, organization, installation, unit, population). Threats may be direct threats against specific targets or interests or indirect threats that can disrupt operations. Threat analyses and threat assessments enable commanders and provost marshals to prioritize their efforts and assets to counter criminal, terrorist, or irregular threats posing the greatest risks to critical and vulnerable assets. The factors considered in a criminal threat analysis address the following areas:

- **Existence.** Existence refers to the determination that a threat group is known to be present, assessed to be present, or able to gain access to the area of operations. The existence of a threat is not dependent on the actual intent or history of threat activity against U.S. interests.
- **Capability.** Capability refers to the determination that a specified threat is known to have acquired, believed to have acquired, or has demonstrated a specific capability.
- **Intent.** Intent refers to a stated desire by threat elements or an actual credible history of threat actions against U.S. interests.
- **History.** History refers to a demonstrated pattern of past activity.
- **Targeting.** Targeting refers to the assessment or additional assessment of threats. It applies if there are known plans, preparations, or activities that indicate a threat of attacks on U.S. interests.
- **Security environment.** Security environment refers to assessing political and security considerations affecting threat capability. This may include—
  - Host nation security cooperation.
  - U.S. and friendly multinational presence. Some considerations include the type and size of the presence and the location, duration, and perception of the local population and threat elements.
  - Geopolitical factors (war, instability, economic turmoil, status of local government, environmental stress).

CRIME PROBABILITY

4-55. Based on the factors of existence, capability, intent, history, targeting, and security environment, the criminal or terrorist threat can be assigned a level of probability and credibility. The probability of criminal or terrorist action against U.S. interests is established as—

- **High.**
  - Threat elements are operationally active.
  - There is potential for significant attacks.
  - The operational environment favors the criminal or terrorist element.
- **Significant.**
  - Criminal or terrorist elements are present in the area of operations.
  - There is operational activity.
  - The elements possess the capability to conduct significant attacks.
  - The operational environment does not favor U.S., host nation, or criminal and terrorist elements.

- **Moderate.**
  - Criminal or terrorist elements are present in the area of operations.
  - There are no current indications of threat activity.
  - The environment favors U.S. or host nation elements.
- **Low.**
  - There are no indications of a threat presence.
  - There is no threatening activity present in the area of operations.

SOURCE RELIABILITY AND CREDIBILITY

4-56. Information and information sources used during analysis should be evaluated for reliability and credibility. Staffs and analysts conducting PIO must conduct continuous evaluations to ensure that information used in their analyses do not lead to false assumptions and conclusions due to problems with the initial source or the information itself. Military police staffs, USACIDC personnel, and police intelligence analysts use a source reliability scale to establish the level of reliability of an information source. (See table 4-1.) Information is further evaluated for credibility using the information credibility scale in table 4-2.

Table 4-1. Source reliability scale

Rating	*Reliability Criteria*
A = Reliable	• No doubt of authenticity, trustworthiness, or competency • History of complete reliability
B = Usually reliable	• Minor doubt about authenticity, trustworthiness, or competency • History of valid information most of the time
C = Fairly reliable	• Doubt of authenticity and trustworthiness • History of reliability information some of the time
D = Not usually reliable	• Significant doubt about authenticity, trustworthiness, and competency • History of occasional reliability
E = Unreliable	• Lacking in authenticity, trustworthiness, and competency • History of unreliable information
F = Cannot be judged	• No basis exists for evaluating the reliability of the source

Table 4-2. Information credibility scale

Rating	*Credibility Criteria*
1 = Confirmed	• Confirmed by other sources and logical in itself
2 = Probably true	• Not yet confirmed, but is logical in itself
3 = Possibly true	• Not yet confirmed, but seems more likely than not • Logical and agrees with other information
4 = Doubtful	• Not confirmed • Possible but not logical • No other information is available
5 = Improbable	• Unconfirmed • Not logical in itself • Contradicted by other information
6 = Cannot be judged	• No basis exists to evaluate the information

4-57. An integral part of a threat assessment is the criticality and vulnerability assessment. The purpose of criticality and vulnerability assessments is to identify the importance and relative susceptibility of unit, base, or base camp assets to criminal or terrorist actions. (See ATP 3-37.2 and ATP 3-39.32 for additional information on criticality and vulnerability assessments.) The process helps the staff prioritize identified assets for command protection efforts. Assets may include personnel, equipment, stockpiles, buildings, recreation areas, communication, or transportation systems that are deemed critical.

4-58. The criticality of an asset typically considers the—

- Value of an asset to a mission or population.
  - **Importance.** Importance measures the value of the area or asset located in the area, taking into consideration the function, inherent nature, and monetary value.
  - **Effect.** Effect measures the ramification of a criminal or terrorist incident in the area, taking into consideration psychological, economic, sociological, and military impacts.
  - **Recoverability.** Recoverability measures the time required to restore function to an area (if the asset is disabled or destroyed), taking into consideration the availability of resources, parts, expertise and manpower, and available redundant assets or systems.
- Ability to replace an asset or function.
  - **Mission functionality.** Mission functionality identifies key positions, special facilities, specialized equipment, and other assets required to fulfill assigned missions.
  - **Substitutability.** Substitutability identifies if there are suitable substitutes available for personnel, facilities, or materiel; if missions can be performed using substitutes; and if the substitutes will produce less-than-successful missions.
  - **Repairability.** Repairability identifies whether an injured or damaged DOD asset can be repaired and rendered operable, how much time will be required for repairs, how much the repairs will cost, and if the repairs will degrade asset performance or if the mission can be accomplished in the degraded condition of the asset.

CRITICALITY AND VULNERABILITY

4-59. There are numerous tools available to military police, USACIDC, or provost marshal staffs to assess the criticality and vulnerability of a particular asset. Each of these tools has unique inherent strengths and weaknesses. Most of the tools used were developed as targeting tools, and they are used to analyze and assess the criticality and vulnerability of specific targets. Their use is based on the premise that, by conducting analyses and assessments of assets as potential targets, the relative criticality and vulnerabilities may become apparent. The value in these types of assessments is that it is likely that threat elements use similar analysis tools to assess their targets. For military police and USACIDC personnel using these tools, the results can be used to develop protection strategies and defeat threat tactics.

4-60. Task-organizing teams are set up by specific function, and they are typically the optimum approach when conducting vulnerability assessments. These teams may include expertise in engineering, signal and communications, network automations, medical operations, special operations, and legal operations, along with the security and law enforcement expertise resident in the military police and USACIDC force structure. This multifunctional approach ensures a comprehensive assessment across a wide spectrum of technical specialties and ensures a holistic and layered approach.

4-61. The most commonly used analytical tools or approaches are the mission (sometimes demography), symbolism, history, accessibility, recognizability, population, and proximity. A second analytical tool is the criticality, accessibility, recuperability, vulnerability, effect, and recognizability model. ATP 2-33.4 and ATP 3-37.2 provide details on how to use these analytical tools.

ECONOMIC CRIME AND LOGISTICS SECURITY THREAT ANALYSIS

4-62. The Army crime prevention program consists of the economic crime threat assessment (ECTA) and logistics security threat assessment (LSTA) critical elements. The USACIDC elements typically focus on these threat areas. These two assessments are a basic analysis of bases or base camps, and the assessments are focused on ascertaining economic crime potential and vulnerabilities. The USACIDC works closely

with logistics unit commanders to identify and mitigate vulnerabilities. The USACIDC criminal intelligence analyst and military police intelligence analyst in the area of operations should communicate with each other and collaborate on significant items in the ECTA and LSTA. This collaboration will result in proactive police intelligence analysis in the area of operations. The following describes the critical elements:

- **ECTA.** An ECTA is an assessment of the overall economic posture of an installation or activity in a USACIDC field element area of operations. It is an important element of the USACIDC crime prevention program and is critical to maintaining a proactive effort and relating to economic crime and logistic security operations.
- **LSTA.** An LSTA is an assessment of logistic storage, transfer and shipping areas and systems, modes of transportation, or aerial ports of debarkation and seaports of debarkation for criminal threat vulnerabilities and terrorist threats directed at logistic pipelines, the security of U.S. government assets, and the safety of DOD personnel. LSTAs can serve as substantial internal and external operational planning tools.

CRIME AND CRIMINAL TARGET ANALYSIS

4-63. Targeting methodology is designed to facilitate the engagement of the right target, at the right time, and with the most appropriate assets to achieve effects consistent with the commander's intent. Persons, groups, infrastructure, and activities can be targeted by many means (lethal and nonlethal). Police intelligence supports the targeting process, enabling the selection and prioritization of crime and criminal targets and the subsequent selection of the appropriate response to them, taking into account operational requirements and capabilities. Targeting entails the analysis of adversary situations relative to the mission objectives. Crime and criminal target analysis enables staff and police intelligence analysts to identify potential targets, including assessments of their vulnerability and relative importance. Key objectives of crime and criminal targeting analysis is the determination of timing and synchronization of operations and the prioritization of targets to be engaged, the desired effect, and the optimal method of targeting.

4-64. The police intelligence analyst creates police intelligence through evaluations and the analyses of collected data. Collected data comes from many sources and methods. These methods range from military police reconnaissance and assessment operations in a tactical environment to covert operations conducted by USACIDC drug suppression teams, with many in-between activities. Relevant police information and police intelligence can be exploited to gain an advantage over the threat.

4-65. Evaluation, analysis, and exploitation may occur simultaneously. New information may be obtained; recognized as relevant, credible, and time-sensitive; and disseminated quickly to maximize exploitation. Further analysis continues to ensure fusion with other information and intelligence while staff and commanders simultaneously use the targeting process to actively exploit the data. For example, information from a reliable source may indicate that an enemy element is about to launch a major attack or that a criminal element is imminently threatening U.S. interests. In this case, the report that an attack is imminent is disseminated as soon as possible after receipt.

4-66. Police intelligence that results from crime and criminal target analyses conducted during PIO and fused into the operations process and common operational picture can provide valuable information to commanders and enable effective targeting. The results of police intelligence analyses may contribute to the development of tactical threat targets for commanders. These results may also target criminals and criminal threat systems that threaten the commander's mission or the safety and security of installations, personnel, and resources. Police intelligence provides information to the commander and provost marshal, with a related situational understanding of the capabilities and challenges associated with operating within the rule of law in a given area of operations. This is extremely important in an expeditionary environment that is transitioning from major combat and instability to supporting a host nation in establishing a criminal justice system under the rule of law. As the environment transitions, due process requirements increase, and targeting activities require a higher level of specificity and probable cause to justify warrants or other legal mechanisms to authorize targeting on individuals or organizations.

4-67. Crime and criminal target analyses and subsequent support to operations occur in all environments. The ultimate goal of a crime and criminal target analysis, as it relates to PIO, is to—

- Identify criminal and threat persons, groups, or organizations.
- Identify historic and current crime trends and predict future trends and activities that enable targeting decisions.
- Develop investigative leads through the identification of trends, patterns, and associations.
- Make target recommendations.

4-68. PIO supports the targeting process through—

- **Target identification.**
  - Using the criminal information gathered and stored in the data files to identify threats (crimes, criminals, and other threat elements and activities) and locations of threat activity.
  - Identifying the organizations involved in the threat activity. This may be criminal enterprises affecting U.S. interests or irregular threat groups (terrorists, insurgents, or groups engaging in criminal activity that disrupt or endanger U.S. operations, including threats from corrupt officials or infiltrators internal to host nation organizations).
- **Analysis of police, criminal, and threat data.** Data analysis can determine trends, patterns, and associations that might otherwise go unnoticed. Analysis enables ongoing crime and crime trend tracking in support of force protection and antiterrorism programs.
  - At locations in the United States and its territories, these analyses aid provost marshals and investigators in focusing their resources at the appropriate places and times to deter or interdict criminal and disruptive activity.
  - In support of unified land operations, military police and USACIDC personnel use this police intelligence to guide their actions and to enhance the commander's common operational picture. This can be done as a U.S. operation or in concert with the host nation or multinational forces, depending on the mission and operational variables.
- **Corroboration of source and informant information.** Due to their dispersion and presence, military police and USACIDC personnel are well equipped to obtain corroborating information for otherwise unsubstantiated source data.
  - During law enforcement operations conducted in the United States and its territories, this corroboration can be accomplished through data mining, witness interviews, surveillance, or other source contacts. (See ATP 3-39.10.)
  - In support of decisive action, similar techniques can also be applied to corroborate witness statements or evidence obtained at an incident site. This corroborated information can then be used in the legal system for prosecution or acted on by the appropriate geographic combatant commander for military action, depending on mission and operational variables.
- **Information sharing and support to active police investigations.**
  - Regardless of the agency, ongoing investigations can be solved using information that is collected and documented by law enforcement officers. One law enforcement officer may have an informant who knows the perpetrator of a burglary that another officer is investigating. Aggressive and proactive analyses and information sharing can contribute to the resolution of specific investigations or criminal activity across organizational lines.
  - In operational environments outside the continental United States, this support can assist commanders and staffs by identifying key threat players, organizations, or cells that may be operating across or within unit boundaries or areas of operations. Police intelligence may identify weapons caches, facilities for the production of improvised explosive devices, or personnel involved in threat activities that are being conducted in another area of operations. The fusion of ongoing police information and police intelligence into the operations process and the common operational picture may provide critical information to commanders and staffs to enable effective targeting.

- **Analysis of threat information.** The analysis function is the hub of PIO. Police intelligence analysis converts information into police intelligence and contributes to other intelligence products.
  - In law enforcement terms, the data or information collected is analyzed to develop additional leads in ongoing investigations, provide hypotheses about who committed a crime or how they committed it, predict future crime patterns, and assess the threat that a crime group or activity might pose to a jurisdiction.
  - In unified land operations, police intelligence resulting from an analysis of threat information enhances the operations process and aids in the maintenance of a holistic common operational picture. Police intelligence may identify threat, operational, or logistic networks; individual operators or sympathizers; and low-level criminals that can disrupt U.S. operations, including threats from corrupt officials or infiltrators internal to host nation organizations. Police intelligence is injected into the targeting process for assessment and exploitation.

ADDITIONAL CONSIDERATIONS AND TECHNIQUES

4-69. There are numerous tools available to the military police and USACIDC personnel and police intelligence analysts. Likewise, there are also pitfalls that can hinder the objectives and accurate and timely assessments of valuable police information. The following paragraphs discuss some of these analytical technique pitfalls.

Evaluation Criteria

4-70. The police intelligence analyst must be able to weigh data use and decide what data is credible. Five aspects determine the value of police information. These aspects include—

- **Validity.** Is the information actually a correct representative of what it is believed to signify? Do not produce police intelligence before validity is confirmed.
- **Relevance.** Is the information actually relevant to the mission or investigation? Is the data a logical connection to the priority of effort?
- **Timeliness.** Is the information or intelligence tied to a specific event or decision point or required in a hard time frame? New information is processed as it is received, but the staff must be aware of time considerations.
- **Corroboration.** Ideally, two independent sources are used to corroborate data. Failure to corroborate information can produce a flawed product. Normally, uncorroborated information is suspect and of limited usefulness. However, uncorroborated information may be useful when balanced against contextual and historical factors. An example may be information received from a confidential source that has a history of reliable and credible reporting. See source reliability and information credibility scales in table 4-1, page 4-16, and table 4-2, page 4-16.
- **Legality.** Information that is not legally obtained will risk tainting all work and expended resources. An analyst must ensure that information is obtained within legal guidelines.

Scanning, Analysis, Response, and Assessment Model

4-71. The scanning, analysis, response, and assessment model is a problem-solving approach developed and used in the law enforcement community. In simple terms, once a problem is identified and its characteristics are analyzed, a response is developed and deployed to combat the problem. After a determined period, the response is evaluated.

4-72. The following is a brief discussion of each aspect of the model:

- **Scanning.** Scanning is the first problem-solving step. Scanning involves the identification of a cluster of similar, related, or recurring incidents identified in the course of a preliminary review of information. It enables the analyst to select and focus on specific crime or disorder problems from among many disparate items of information.
- **Analysis.** Analysis is the use of available sources of information to determine why a problem is occurring, who is responsible, who is affected, where the problem is located, when it occurred, and what form it takes.
- **Response.** Response is the execution of a tailored set of actions that addresses the most important findings of the analysis phase.
- **Assessment.** Assessment is the measurement of the impact of responses on a targeted problem. Assessment uses information collected from multiple sources, before and after the responses have been implemented.

DATABASE AND AUTOMATION REQUIREMENTS

4-73. The increased proliferation of digital technology has greatly increased the amount of information that must be assessed by commanders, provost marshals, staffs, and investigators. Concurrently, the expansion and use of automated systems for data storage and manipulation has become a reality and a necessity to effectively manage the volume and types of data that are available. Databases serve as repositories for raw police information and analyzed police intelligence products. This data may be maintained by a local provost marshal office, a combat unit, or an Army or DOD command. Databases can be used during active investigations and as final storage locations for complete information on closed investigations and reports. It is imperative that investigators become familiar with the full host of available databases for data entry and retrieval.

4-74. Advances in database technology, combined with an explosion in information sharing and networking among police agencies, has resulted in the development and expansion of these robust information repositories. Army law enforcement personnel continue to access the National Crime Information Center database, but can also turn to databases containing fugitive information from corrections systems and terrorist threat information from DHS and the Federal Bureau of Investigation systems. The DOD proprietary automation systems (COPS, ACI2) greatly improve interoperability and eliminate seams that criminal and other threats might otherwise exploit.

4-75. Access to local, theater, DOD, non-DOD, and commercial databases allows analysts to leverage stored knowledge on topics ranging from basic demographics to threat characteristics. A validated Defense Intelligence Agency customer number (acquired by the intelligence directorate of an echelon intelligence staff section S-2 or G-2), in combination with SIPRNET and Joint Worldwide Intelligence Communication System connectivity, can establish access to most online databases. The challenge for an analyst is to gain an understanding of the structure, contents, strengths, and weaknesses of the database, regardless of the database type. Additionally, the procedures are often difficult for extracting portions of data or downloading and transferring data to unit automated information systems. Database access is typically accomplished through unit or agency homepages via SIPRNET and the Joint Worldwide Intelligence Communication System.

4-76. Automation increases the capability to correlate large volumes of information from many sources and assist in the analysis process. Interpretation of the information requires an analyst to develop search and file parameters. Analysis continues to be a human function—cognitive functions that manifest in reflective thinking. Information is converted into police intelligence products through a structured series of actions that, although set out sequentially, may also take place concurrently. Production includes the integration, evaluation, analysis, and interpretation of information in response to known or anticipated intelligence product requirements.

ARMY CRIMINAL INVESTIGATION INFORMATION SYSTEM

4-77. The ACI2 supports Army criminal investigation operations; is accredited for unclassified law enforcement-sensitive operations; and uses private, network-based software applications. USACIDC

personnel have local office and global access to most data in ACI2. Scheduled reports and ad hoc queries provide powerful data mining capabilities. ACI2 supports numerous USACIDC operations and reports that include—

- Investigation reports.
- Forensic laboratory reports.
- Crime prevention surveys.
- Criminal activity threat assessments.
- Criminal intelligence reports.
- LSTAs.
- ECTAs.
- Port vulnerability assessments.
- Terrorist information and threat reports.
- Regional criminal intelligence summaries.
- Registered source reports.
- Criminal alert notices.
- Drug suppression surveys.

4-78. These software programs help analysts and investigators by revealing the structure and content of a body of information by storing, organizing, and analyzing intelligence and presenting it in an easily understood graphic format. Civilian law enforcement partners cannot access many DOD proprietary automation systems (COPS, ACI2). By using commercial products with appropriate information release policies, information gaps can be bridged between Army and civilian law enforcement. Common crime analysis databases, automation, templates, and data formats improve interoperability and eliminate seams for criminals and other threat forces to exploit.

CENTRALIZED OPERATIONS POLICE SUITE

4-79. A significant tool used by the provost marshal today is COPS. COPS is an information management system supporting worldwide military police operations. It combines all facets of law enforcement reporting. The current applications found in COPS are the Vehicle Registration System, Military Police Reporting System, Army Correctional Information System, Detainee Reporting System, and a self-registration feature. The COPS applications include daily activity law enforcement (blotter) reports, military police reports, and other automated entries. It is accredited for unclassified law enforcement-sensitive operations and uses a virtual private network and Web-based operations.

4-80. Typically, COPS provides military police access to automated police records from a centralized database. It allows users, with appropriate permissions, to conduct queries expeditiously from a centralized database. Name queries return limited criminal arrest history data from Army-wide military police records. A major component of the COPS database is the ability to provide real-time information. This centralized database also eliminates natural borders and barriers that normally hamper the law enforcement community. The capabilities afforded by COPS allow for a quick compilation of statistics, based on the query input.

4-81. The COPS is capable of supplying a significant amount of statistical data to police intelligence analysts and provost marshal staffs. This data can be manipulated to identify trends, patterns, and associations that enable provost marshals and staffs to effectively allocate resources, address specific crime problems or other areas of concern, and forecast future requirements.

DISTRIBUTED COMMON GROUND SYSTEM–ARMY

4-82. DCGS-A is the Army reconnaissance and surveillance ground processing system for signal intelligence, imagery intelligence, measurement and signature intelligence, and HUMINT sensors. It also provides weather and terrain analysis. DCGS-A is the primary intelligence processor for the intelligence warfighting function. It is critical that police information and police intelligence reports that reside on DCGS-A abide by legal and regulatory restrictions on the collection against U.S. persons by intelligence

personnel. DCGS-A provides Web-based communications and interactive analytical capability. The platform, with integrated analytical tools, allows analysts to participate and collaborate in the development of products geared to mission planning, targeting, and information analysis at all echelons. DCGS-A integrates existing and new reconnaissance and surveillance system hardware and software to produce a common, net-centric, modular, scalable, multisecurity, multi-intelligence, and interoperable reconnaissance and surveillance architecture. DCGS-A provides the ability to access data, from tactical to national sensors, across the intelligence enterprise, and facilitates reach with collaboration capabilities for deployed elements. DCGS-A enables the rapid input of analytical products, increasing responsiveness to the needs of commanders and staffs.

4-83. DCGS-A facilitates the rapid conduct of operations and synchronization of warfighting functions. This enables commanders to operate in the threat decision cycle and shape the environment for successful follow-on operations. The DCGS-A provides the following capabilities:

- Receives and processes select reconnaissance and surveillance sensor data.
- Facilitates the control of selected Army sensor systems.
- Facilitates the reconnaissance and surveillance synchronization and integration.
- Facilitates the fusion of information from multiple sensors.
- Enables the distribution of friendly, threat, and environmental (weather and terrain) data.

ADDITIONAL ANALYTICAL AND DATABASE CONSIDERATIONS

4-84. Many commercial database and analytical applications are useful for police intelligence analysis and data management. Some of these applications may be costly and require a significant up-front training investment. These applications will typically be used by dedicated police intelligence analysts. Other applications may be more readily available as standard database applications that can be used for more low-level analysis and statistical manipulation; these applications may also be used by dedicated police intelligence analysts, but are also readily and easily available to the staff in general.

Automated Databases

4-85. A database is a tool for collecting and organizing information. A database can store information about people, types of events, or just about anything. Many databases start as a list in a word-processing program or spreadsheet. Without databases, information is difficult or impossible to retrieve quickly, especially under adverse conditions. Depending on the capability of the individual database software, databases can support many complex analytical functions and requirements.

4-86. Military police staff and police intelligence analysts may use databases to—

- Deconflict and synchronize collection missions.
- Track requests for information.
- Track intelligence requirements.
- Prepare reports and assessments.
- Track threat and friendly events or situations.
- Develop targeting recommendations and priorities.

4-87. Many analytical software applications are compatible with various databases. This enables databases to interact with other tools to support predictive analysis, prepare graphic analytical products, and provide situational awareness to the unit commander. These databases can—

- Support time-event charts, association matrices, link analysis, and other analytical tools.
- Allow operators, staff, and analysts to—
  - Protect source-sensitive, operational database segments, files, records, and fields.
  - Create, update, and maintain databases from locally generated information.
  - Import complete or partial databases from larger or peer databases.
  - Export complete or partial databases to peer or larger databases.
  - Share database information with personnel possessing appropriate access authorization (peers, subordinates, higher commanders).

- Allow data queries for decisionmaking and operational and analytical support.
- Interact with analytical programs able to correlate data and facilitate information retrieval from data repositories.
- Allow for information retrieval functions (browsing, Boolean functions, key word searches, concepts).

Automated Analytical Tools

4-88. The automation of analytical tools (time-event charts, association matrices, activity matrices, link analysis diagrams) can significantly enhance the predictive analysis capability and pace of production. Automation enables rapid access to information. When properly evaluated, this allows the critical analysis of a greater pool of information, which produces a more accurate and timely product.

4-89. Automated analysis software includes computer-assisted analytical programs that reduce the time required for analysis. These programs help the analyst develop predictions and identify information gaps to support targeting and collection. Automation and Web-based tools allow an analyst to—

- Track, integrate, and catalog information and reports.
- Expedite data retrieval, data organization, content analysis, and visualization.
- Share analyses and information with other units and analytical elements, as appropriate.
- Take advantage of Web-based collaborations.
- Provide analytical results and view operations in real time.
- Share resources (models, queries, visualizations, map overlays, tool outputs through a common interface).
- Apply clustering (a nonlinear search that compiles the results based on search parameters) and rapid spatial graphical and geographic visualization tools to determine the meaning of large informational streams.
- Discover links, patterns, relationships, and trends in text to use in predictive analyses rapidly.
- Capture analytical conclusions and automatically transfer them to intelligence databases and systems.

Note. There are strict legal and regulatory constraints on the collection, storing, and dissemination of information on U.S. persons. The supporting judge advocate should be consulted to ensure that data storage complies with applicable laws and regulations.

Geographic Information Systems

4-90. There are several automated geographic information systems to help military police staff and police intelligence analysts with organizing, analyzing, and producing geographic data and products. A geographic information system can provide a graphic depiction of data as it relates to the geography of a specific area. Geographic information system software uses database data to display maps and data, as required by the system operator. These tools are useful and have the capability of providing layered, three-dimensional images of specific areas of interest. Typically, data will be imported from an existing database or input manually into the geographic information system. Data should be continuously updated to ensure that current and accurate data is available. Once loaded, the analyst can manipulate the data to produce specific analytical products, as required.

4-91. Geographic information systems enable the analyst to layer informational data on top of terrain to provide a more accurate picture of the area of operations or a specific target. These capabilities are most useful in the analyses of dense urban areas. These systems are used to track and analyze specific criminal activity and associated structures and locations, allowing the development and identification of patterns and linkages that might otherwise go unnoticed. Geographic information systems can also be used as a platform to portray the effects of terrain on operations. For example, in a crisis response scenario, a geographic information system can provide a three-dimensional image of a target building for rapid analysis and decisionmaking where a law enforcement raid or special-reaction team mission is planned.

Chapter 5
Production and Dissemination

PIO support military police activities and Army operations by producing relevant, accurate, and usable police intelligence products. The goal of PIO is achieved when police information is collected, analyzed, produced, and disseminated to military police and USACIDC units, maneuver commanders, other Service forces, host nation security forces, or the local population. Close coordination with police intelligence analysts ensures that products are tailored to meet specific requirements. The military police staff and police intelligence analysts must be proficient in packaging relevant police intelligence into usable products that are clear, concise, and targeted to the needs of the stakeholder. Police intelligence products may range from simple, free-formatted alerts to complex briefings and assessments. This chapter provides a brief description of some of the more common products that may be produced by the military police or USACIDC personnel and their associated analysts.

OPERATIONS

5-1. Police intelligence products answer intelligence requirements and enable commanders and law enforcement investigators to make informed decisions. These products may assist law enforcement personnel in capturing a wanted felon, gaining information to assist in an investigation, or closing an investigation. When police intelligence products are fused with other police intelligence, it greatly enhances the effectiveness of law enforcement investigations and police operations. When supporting decisive action, police intelligence can provide critical understanding to commanders regarding police and prison organizations, systems, structures, and the criminal environment in the area of operations. When fused with Army intelligence, police intelligence can greatly enhance the commander's situational understanding and update the common operational picture.

5-2. Police intelligence products will generally contain basic information and analyzed intelligence. It is important to keep the intended recipient and purpose at the forefront during the planning and production phases. Failure to do so may result in the production of multiple documents, each with a specific audience and purpose. Regardless of the format employed, producers of police intelligence products must take extreme care to ensure the accuracy of the products and the protection of classified or sensitive information. Information or police intelligence that must be retained in law enforcement channels to protect information, sources, or ongoing investigations is characterized as law enforcement-sensitive. The term law enforcement-sensitive is used to classify information or intelligence that is obtained for, processed through, or managed by law enforcement organizations. It is essential that the data is restricted to law enforcement channels, unless otherwise directed by a competent authority.

5-3. The producers and recipients of disseminated police information or police intelligence must understand distribution restrictions. At times, products may contain data drawn from multiple unclassified sources. These police intelligence products may—

- Remain unclassified.
- Receive a distribution caveat of law enforcement-sensitive or sensitive but unclassified.
- Receive a classified restriction when the results of the analyses warrant.

5-4. The classification of a document or data may be required to protect an informant or law enforcement source; a monitoring capability; a tactics, techniques, and procedure for gathering police information; or other classification criteria. It may be possible to prevent the creation of a classified product simply by protecting the manner in which the information was collected or processed. In the event that a product

requires classification, immediate action should be taken to ensure that the classified data or document is properly stored to prevent unauthorized access or compromise information or intelligence. Coordination with the local offices responsible for computer network defense and security issues should be maintained to ensure that security requirements are maintained.

PRODUCTION

5-5. Intelligence production includes analyzing information and intelligence and presenting intelligence products, conclusions, or projections regarding the operational environment and enemy forces in a format that enables the commander to achieve situational understanding. (See ADRP 2-0.) Police intelligence products produced by police intelligence analysts, military police, and USACIDC personnel and law enforcement investigators should enable the stakeholder to gain a greater understanding of the operational environment and enable operational objectives. Police intelligence products and reports should provide commanders, provost marshals, and law enforcement investigators with useful tools to augment a holistic assessment of the security and criminal environment across the area of operations. Effective police intelligence products have several characteristics. These characteristics are—

- **Distinct.** The product can support or enhance other intelligence products but should provide an analysis that stands on its own merit.
- **Tailored.** The product should be tailored to a specific commander, provost marshal, or law enforcement investigator mission, objective, or area of operations.
- **Actionable.** The product provides commanders, provost marshals, and law enforcement investigators with situational understanding to support effective decisionmaking.
- **Accessible.** To the greatest extent possible and within mission, legal, and policy constraints on information sharing, products must be accessible to stakeholders requiring the information.
- **Timely.** The products support the commander, provost marshal, or law enforcement investigator objectives and intent for operations or effects.

5-6. Police intelligence products produced by military police and USACIDC personnel and police intelligence analysts are sometimes in standardized formats to ensure consistency in reporting and content. Most products are dependent on the target audience; the mission; and the specifics of the event, material, person, or organization that is the subject of the product. At the tactical level, the level of detail and type of intelligence required is much different from the operational or strategic level. The staff and analyst must fully understand the information, intelligence requirements, and specific needs of the target audience and provide a product that enables decisionmaking appropriate to the level of the recipient.

5-7. The following sections include examples of various police intelligence products. These examples are baseline products; they will change with command and host nation requirements, technological advances, and legal restrictions. Formats may vary; however, the accuracy, timeliness, and relevancy of the product is critical to the targeted audience.

BE-ON-THE-LOOKOUT ALERT

5-8. A BOLO alert is routinely sent out by Army and civilian law enforcement agencies. A BOLO alert is used to provide information to, and request assistance from, military and civilian law enforcement organizations, military units and, at times, the public about specific individuals, vehicles, events, or equipment. Typically, these alerts are used when the subject matter is time-sensitive and a heightened awareness by all available personnel is requested to facilitate the appropriate action. A BOLO alert may be distributed in a printed format, distributed over appropriate information networks, or transmitted over radio nets depending on the breadth of distribution, time sensitivity, or other mission and environmental factors.

5-9. A BOLO alert may be general or very specific; but it should contain, when possible, enough information to prevent numerous false positive reports and should provide reporting and disposition instructions. These instructions should include any known dangers associated with the subject of the BOLO alert. For example, a BOLO alert for a grey BMW® automobile to all military police units operating in Germany or an orange and white taxi in Iraq would be ineffective and would likely result in an extremely high number of sightings. This type of general information might also be ignored by military police personnel for the same reason. Additional information about the driver, body damage to the vehicle, or

other specific details would reduce the false positives and increase the value of what is reported. In some instances, the amount of known information is limited to one or more identifying data points. This is common in expeditionary environments where a list of names may be the only data available or immediately following a crime or incident when only rough descriptions of suspects or few witnesses are available. Figure 5-1 and figure 5-2, page 5-4, show examples of BOLO alerts.

For Immediate Release
20 March 20XX, Washington DC
FBI National Press Office
(Subject Name) Poster

Insert Photo

THE FBI IS SEEKING THE PUBLIC'S ASSISTANCE IN LOCATING AN INDIVIDUAL THAT IS SUSPECTED OF PLANNING TERRORIST ACTIVITIES.

The FBI has issued a BOLO alert for (subject) in connection with possible threats against the United States. In the BOLO alert, the FBI expresses interest in locating and questioning (subject) and asks law enforcement personnel to notify the FBI immediately if the subject is located. The subject's current whereabouts are unknown.

The subject is possibly involved with al-Qaeda terrorist activities and, if true, poses a serious threat to U.S. citizens worldwide.

The subject is 27 years old, and he was born in Saudi Arabia. He is approximately 132 pounds (but may be heavier) and 5'3" to 5'5" tall; he has a Mediterranean complexion, black hair, brown eyes, and occasionally grows a beard. A photograph of this individual is available on the FBI Web site.

The subject carries a Guyana passport; however, he may attempt to enter the United States with a Saudi Arabia, Trinidad, or Canadian passport. The subject is also known by the following aliases:

Alias #1, Alias #2, Alias #3, Alias #4

Legend:

BOLO	be on the lookout
DC	District of Columbia
FBI	Federal Bureau of Investigation
U.S.	United States

Figure 5-1. Example of a Federal Bureau of Investigation BOLO alert

[CLASSIFICATION] Be-On-the-Lookout List		
Date	***Individual/Vehicle***	***Threat Summary***
4 Sep XX	1970s Chevrolet® Impala®, white, host nation plate 283AC2	Vehicle was used to transport explosive materials for IED production and target U.S. and host nation police forces.
5 Sep XX	Late model Mercedes® panel truck, dark blue with white bumpers, host nation plate 853DJC	Vehicle was possibly used to transport contraband weapons, stolen merchandise, and funds used in support of organized criminal networks operating in the area of operations. It has also reportedly used different plates, to include GE65ART and UK19873.
15 Sep XX	John Doe 	Individual is wanted for questioning by host nation and U.S. military police personnel in connection with the murder on 4 Sep XX of a host nation police chief. He also has possible connections to at least three additional assassinations of host nation police officials. This individual has been previously detained and subsequently released; biometrics data is uploaded to the area of operations biometrics equipment.
[CLASSIFICATION]		
Legend:		
IED	improvised explosive device	
Sep	September	
U.S.	United States	

Figure 5-2. Example of an Army BOLO alert

CRIMINAL INTELLIGENCE BULLETIN

5-10. Criminal intelligence bulletins are documents produced by USACIDC and disseminated internally to USACIDC and Army law enforcement. These bulletins are forwarded to all USACIDC field elements by the USACIDC chain of command and shared with other Army law enforcement to alert them of conditions, techniques, or situations that could be significant factors in present or future investigations or crime prevention surveys. Local units, organizations, and entities may be provided with pertinent information that affects their organizations via a crime prevention flyer (see paragraph 5-13).

CRIME PREVENTION SURVEY

5-11. Crime prevention surveys are conducted, within resource and mission constraints, by USACIDC to support commanders in the context of the Army Crime Prevention Program. The survey is a formally recorded review and analysis of existing conditions in a specified facility, activity, or area for the purpose of detecting crime, identifying conditions or procedures conducive to criminal activity, and minimizing or eliminating the opportunity to commit a criminal offense or engage in criminal activity. The crime prevention survey is the result of a crime and criminal threat assessment and analysis. The crime prevention survey seeks to determine the nature, extent, and underlying causes of crime, and it provides the commander with information that is used in the crime prevention program. (See AR 10-87 and AR 195-2.)

5-12. A crime prevention survey may be initiated by USACIDC or at the request of the supported commander. The USACIDC conducts crime prevention surveys and crime and criminal activity threat assessments of facilities, activities, events, and areas that are under Army control or that directly affect the Army community. The USACIDC may also conduct crime prevention surveys of other DOD facilities and activities when requested (if resources are available). The crime prevention survey will identify situations that are not procedural deficiencies but could, if left unchecked, result in the loss of Army assets through negligence, systemic weakness, or failures and erosion of established internal controls. The crime

prevention survey is provided to the local commander responsible for the area of operations in question, typically commanders of posts, base camps, stations, or other mature bases. A crime prevention survey identifies—

- Criminal activity in a specific location.
- Regulatory deficiencies.
- Economic threats to installations or activities.
- Domestic and international terrorist threats.
- Likely theft, diversion, sabotage, or destruction of U.S. government property or assets.
- Vulnerability of Army automated systems.

CRIME PREVENTION FLYER

5-13. The crime prevention flyer is an external document prepared by USACIDC or provost marshal office personnel for local agencies and entities. It is produced and disseminated to notify organizations of identified conditions that could result in another criminal incident or future loss of government funds, property, or personnel. The flyer is formatted for external distribution, with the intent to share pertinent information and facilitate cooperation and assistance in crime prevention activities. Figure 5-3, page 5-6, displays an example crime prevention flyer.

ECONOMIC CRIME THREAT ASSESSMENT AND LOGISTICS SECURITY THREAT ASSESSMENT

5-14. The ECTA report is a USACIDC assessment of the overall economic posture of an installation or activity. The ECTA process is one of the most important aspects of the USACIDC crime prevention program. ECTAs provide valuable information and police intelligence to enable the effective employment of limited USACIDC and other law enforcement assets. An ECTA is an important element for a proactive effort that relates to economic crimes and logistic security operations.

5-15. The LSTA report is produced by USACIDC special agents looking specifically at key logistic bases and infrastructure. The LSTA is prepared to assess logistic systems, modes of transportation, or port (air and sea) criminal threat vulnerabilities and terrorist threats targeting the integrity of the logistic lines of communications, the security of U.S. government assets, and the safety of DOD personnel. An LSTA can serve as a substantial internal and external operational planning tool. Distribution is normally restricted to the commander of the facility, supporting law enforcement and security elements, and higher headquarters. Due to the specifics of the report, LSTAs are normally classified.

FORENSIC ANALYSIS REPORT

5-16. Forensic analysis reports are produced at laboratories that conduct forensic examinations of collected materials and potential evidence. These reports are usually produced according to the standards of the laboratory conducting the analysis. When supporting law enforcement investigations, the reports will usually have controlled distribution in law enforcement and judicial channels. Although technical in nature, the reports may contain summaries that provide the basic data information in a more readable format. Law enforcement investigators who are reviewing forensic reports should directly contact serving laboratories for clarification or explanation of evidence or to correlate the results of other investigative findings.

5-17. In support of decisive action, forensics reports developed in expeditionary forensics laboratories are passed to the National Ground Intelligence Center. The National Ground Intelligence Center plays an important role in providing forensics analysis reports to the intelligence community. The National Ground Intelligence Center maintains a biometrics management analysis team that is responsible for providing finished intelligence products to the intelligence community regarding biometrics information.

Office Symbol 12 November 20XX

MEMORANDUM FOR Commander, 10th Sustainment Command, Port of Entry, Country
SUBJECT: Crime Prevention Flyer, Regarding: Larceny of Government Property

1. PURPOSE: This crime prevention flyer addresses the larceny reported on 21 October 20XX and the immediate actions recommended to deter future criminal activity and loss of property.

2. BACKGROUND: Investigators have expended a significant amount of resources investigating the stated crime that occurred on 21 October 20XX. Due to the conditions outlined below, the investigation has produced negative results. Losses to date have been valued at about $8,200. During the investigation, several conditions were discovered that produce conditions conducive to criminal activity. Most of these conditions are basic physical security deficiencies. Actions that correct the identified deficiencies can contribute to making the 10th Sustainment Command and associated warehouse areas a hard target for thieves and deter future break-ins. The investigation into this incident is not complete; however, the items shown below are of time-sensitive interest:

a. The rear door to the unit warehouse did not have a security cover over the doorframe area where the locking mechanism was located. This facilitated the insertion of a pry bar to force open the door.
b. The rear floodlights were burned out or missing. Operational floodlights would illuminate the rear entry, forcing potential criminals to operate in an illuminated area rather than in darkness.
c. A security camera was present and functional, but not serviced (taping medium was full); therefore, the security cameras were rendered useless. Interviews revealed that the camera has not been used during the assignment of any current Soldier or civilian.
d. The gate at the rear entrance to the warehouse area was not properly secured, and security checks on that area were not conducted.

3. RECOMMENDATIONS: Standard physical security measures, according to AR 190-53, should be followed. These measures include—

a. Ensuring that security lights are operational.
b. Ensuring that security camera tapes or disks are changed in a timely manner and the camera system is employed.
c. Modifying the rear door of the warehouse to ensure that a security cover is in place.
d. Securing the rear gate entrance to the warehouse area and adding security checks to existing standard operating procedures.

4. The point of contact for additional information is the undersigned, at [telephone number] or [e-mail address].

John Q. Agent
Special Agent in Charge

Figure 5-3. Example of a crime prevention flyer

WARNING INTELLIGENCE

5-18. *Warning intelligence* are those intelligence activities intended to detect and report time-sensitive intelligence information on foreign developments that forewarn of hostile actions or intention against United States entities, partners, or interests (JP 2-0). The S-2 or G-2 has primary staff responsibility for producing warning intelligence; however, all functional elements contribute to warning intelligence through awareness of the CCIR and by reporting related information. The PIO is planned and executed by the S-3 in functional units and the provost marshal staff in multifunctional units; warning intelligence related to police intelligence will be produced by the S-3, G-3, or provost marshal staff and coordinated with the S-2 or G-2 as required.

5-19. Military police and USACIDC elements, by virtue of their mission and their dispersion across the area of operations, are often the first to see indications of an imminent threat. When this information is reported through normal reporting channels, it is disseminated rapidly to alert affected organizations, units, and adjacent law enforcement agencies. Military police produce warning intelligence to provide police information or analyzed intelligence for timely notification that a possible criminal threat or attack on U.S. interests has been identified and is imminent.

5-20. The nature of a threat indicator will generally dictate the distribution list and the method used. The speed, positive acknowledgement, and sensitivity of the information may be critical. At a minimum, military police, other security forces, the S-2, and the commander are normally notified of incoming warning intelligence. As with other police intelligence products, a decision must be made about how much information to release and whether sources of information must be protected in the warning.

LINK ANALYSIS PRODUCTS

5-21. Link analysis products (charts, maps, and graphs) provide a visual link between persons, organizations, locations, crimes, and evidence. These products may be automated with commercially available programs or produced by hand using maps, overlays, matrices, or graphs. Law enforcement investigators conducting criminal investigations typically use link analysis products extensively. Link analysis products can also be designed and produced specifically for the legal community involved in judicial proceedings to assist with understanding the connection between known criminals, criminal activities, and other persons suspected of involvement in a crime or criminal enterprise.

5-22. Some commanders and provost marshals may require presentations of the entire link analysis chart; however, the complexity of these products limits their use for personnel not intimately familiar with the events and subjects portrayed. Oftentimes, the staff or analyst that constructed the data may need to build a separate briefing or other presentation for the commander or provost marshal that provides a synopsis of key linkages.

PERSONAL SECURITY VULNERABILITY ASSESSMENT

5-23. Personal security vulnerability assessments are conducted and produced by USACIDC special agents on high-risk personnel, based on the duty position, the level of threat, and the geographic location (when directed by the Secretary of the Army or the Chief of Staff of the Army). The personal security vulnerability assessment is conducted to enhance the personal security posture of high-risk personnel. At a minimum, a personal security vulnerability assessment will include a review of the procedures and measures employed at the residence and workplace of the high-risk personnel and for travel between the two locations. The personal security vulnerability assessment scrutinizes all aspects of the physical security of the principal's residence, workplace, and mode of travel. A review and analysis of the principal's routine habits and social and personal commitments are conducted. These activities are performed to determine where the principal would be most vulnerable and to reduce the likelihood of becoming a target of an individual or group.

5-24. All supporting documentation (blueprints, schematic drawings, still photographs, videos, written documents) will be available for review or as attachments during the final personal security vulnerability assessment. The final report is typically made available to high-risk personnel for review. Due to the nature of these reports, distribution is normally severely restricted and is provided only to the individual covered in the assessment, their immediate staff, the security team, and USACIDC headquarters. A copy of the final report is kept in the high-risk person's file; a second copy is provided to the USACIDC Crime Records Center, Fort Belvoir, Virginia. The conduct of a personal security vulnerability assessment is directed in AR 10-87, AR 190-58, and AR 525-13.

5-25. The personal security vulnerability assessment final report includes—

- The date the high-risk personnel briefing was held.
- A list of personnel who received the exit briefing.
- The reaction of high-risk personnel receiving the briefing.
- A list of noted problem areas and recommended solutions.
- A list of security recommendations.

POLICE INTELLIGENCE ADVISORIES

5-26. Police intelligence advisories are produced to transmit information related to criminal activity in the area of operations of other law enforcement organizations. The document can be used to relay information and police intelligence on crime patterns, methods of operation, organized crime networks, technology used by criminal threat elements, and intelligence requirements and concerns involving criminal organizations and activities. Figure 5-4 shows an example of a police intelligence advisory.

5-27. Police intelligence advisories produced by USACIDC are referred to as criminal intelligence reports, but they follow the same format as the police intelligence advisory. Other law enforcement organizations may have slightly different titles and format variations. The report is an informative document prepared for another USACIDC or military police element and includes the following information:

- Heading.
- Date prepared.
- Preparing office.
- Sequence number.
- Offense or additional types of information.
- Synopsis.
- Signature blocks.
- Warning and distribution statements.

POLICE INTELLIGENCE ALERT NOTICES

5-28. The police intelligence alert notice is a document prepared by Army law enforcement elements. It expedites the reporting of perishable, time-sensitive, and crime-related information. A police intelligence alert notice is prepared and disseminated to attack the offender's capability of victimizing others. The notice alerts persons, organizations, or entities identified as high risk for criminal activity (logistics bases, units operating within the threat area of operations, high-payoff targets [hospitals, financial organizations, supply depots]) in an effort to prevent victimization by an identified threat. See figure 5-5, page 5-10, for an example police intelligence alert notice.

[CLASSIFICATION]

POLICE INTELLIGENCE ADVISORY

Date Prepared: 1 January 20XX

Preparing Office: 11th MP Detachment, FOB Bulldog, Country

Sequence Number: 444-09-MPR992, First PIA

1. Subject 1; Specialist; [social security number]; male; white; 6'2"; 180 pounds; brown hair; brown eyes; 345th Maintenance Company, Fort Sunny, California (formerly 123d Maintenance Battalion, FOB Bulldog, Country).

2. Subject 2; Specialist; [social security number]; female; white; 5'4"; 110 pounds; blonde hair; blue eyes; 123d Maintenance Battalion, FOB Bulldog, Country.

3. Subject 3; Sergeant; [social security number], male; white; 5'8"; 143 pounds; blonde hair; brown eyes; 123d Maintenance Battalion, FOB Bulldog, Country.

Offense: Wrongful appropriation/larceny of government property.

Reference is made to this office MPR 0443-09-MPR992.

Source of Information: The information contained in this PIA was developed during the referenced MPR and is considered reliable.

Narrative: At about 2300 hours on 1 May 20XX, the 11th MP Detachment, MP Investigations Section, FOB Bulldog, Country, while conducting an investigation of possible larceny of government property in the 123d Maintenance Battalion supply room, discovered evidence linking Subject 2 and Subject 3 to stolen government property. The stolen property includes bayonets, commercially procured personal hydration units, and laser sights. During subsequent interviews, Subject 2 admitted that, in addition to being a friend to Subject 3 and Subject 1, she conspired with them to take government property with intent to mail the items back to the United States for resale by Subject 1. Several stolen items were later found in the possession of Subject 3 and recovered. Court-martial actions are being taken against Subject 2 and Subject 3. Subject 1 has been allegedly quoted by his roommate (not considered a suspect) as saying that he had a “sweet business deal waiting for him stateside.” The supporting judge advocate has reported that there is insufficient evidence to take action against Subject 1. This is a terminal report; no further reports are contemplated pending receipt of additional police intelligence.

Warning Statement: This document is intended for law enforcement personnel, police intelligence analysts, military personnel, and other officials with a need to know. Further dissemination of this report should be limited to a minimum, consistent with the purpose for which the record has been furnished (such as the effective enforcement of civil and criminal law). Additional release requires approval from the originator.

Report prepared by:	Report approved by:
Staff Sergeant Joe Smith	Major John Surname
MP Investigator	MP Operations

Distribution:
Provost Marshal, FOB Bulldog, Country
Commander, 345th Maintenance Company, Fort Sunny, California
Provost Marshal, Fort Sunny, California

[CLASSIFICATION]

Legend:

FOB	forward operating base
MP	military police
MPR	military police report
PIA	police intelligence advisory

Figure 5-4. Example of a police intelligence advisory

POLICE INTELLIGENCE ALERT NOTICE
TERRORIST ACTIVITY
(MANUFACTURE AND EMPLACEMENT OF IMPROVISED EXPLOSIVE DEVICES)

Date Prepared: 1 January 20XX

Preparing Office: 50th Military Police Brigade, Province, Country.

Source: Information was obtained from a local national informant that has supplied credible and accurate information in the past; the information is considered reliable.

Credible information has been received that Subject 1, Subject 2, and Subject 3 have been assembling improvised explosive devices and hiring third-party individuals to emplace the devices, targeting U.S. military and host nation convoys throughout Hostile Province.

Subject 1 has been known to use the aliases Alias 1 and Alias 2.

Subject 2 has been known to use the aliases Alias 1 and Alias 2.

Subject 3 has been known to use the aliases Alias 1 and Alias 2.

Police intelligence indicates that Subject 1, Subject 2, and Subject 3 have been manufacturing improvised explosive devices in a mobile facility, most likely a modified panel van. Police intelligence further indicates that they consistently use electronic triggers supplied by a foreign source and that their devices are consistently radio frequency-detonated using components from a single source supplier. When on the move, Subject 3 typically drives while Subject 1 and Subject 2 work in the back of the van. Subject 3 is described as 6'6" tall, weighing more than 300 pounds, with a large, heart-shaped tattoo with the word “MOM” on his left forearm. There are currently no descriptions for Subject 1 and Subject 2.

Units operating in the area should be alert for suspicious activity, particularly at vehicle checkpoints and when involving paneled vans transiting the area of operations. If the suspects are encountered, detain them if possible. However, exercise extreme caution. Additional intelligence indicates that the van is often booby-trapped. If Subject 1, Subject 2, or Subject 3 is detained, notify the 50th Military Police Brigade as soon as possible to facilitate law enforcement apprehension of the suspects. Incident sites should be searched for remnants of trigger devices and other material to be collected for forensic evaluation.

The point of contact for this alert is Major Jane Surname, Military Police Operations Officer, 50th Military Police Brigade, [telephone number], [e-mail].

This alert is intended for dissemination to all units operating in Hostile Province.

Figure 5-5. Example of a police intelligence alert notice

5-29. The police intelligence alert notice informs the recipients of criminal activity, the specific actions required to interdict or mitigate the stated activity, and specific evidence collection and preservation priorities. The police intelligence alert notice is an action document, not an informational report. Police intelligence alert notices produced by USACIDC are referred to as criminal alert notices.

5-30. Police intelligence alert notices and criminal alert notices follow the same basic format. They will typically include—

- Source and reliability of the information.
- Entities involved.
- Known aliases.

- Known personal identification numbers (social security number, driver's license number).
- A summary of pertinent information developed to date on the subject or suspect.
- Actions that the recommending unit wishes to be taken by the activities and agencies receiving the bulletin (detain subject or suspect, notify law enforcement authority).
- Points of contact, to include names and contact numbers from the issuing unit.
- Distribution and dissemination instructions and restrictions.

STATISTICAL DATA

5-31. Statistical data can be drawn from diverse sources and can be depicted in numerous manners. Statistical data may be presented in charts displaying—

- Frequencies (using bar, pie, and Pareto charts).
- Trends (using bar and line charts).
- Distributions (using geographic information systems, trend lines, or other formats).

5-32. Different audiences and types of data require different types of statistical tools to present data in a manner that is clear and concise. Data placed into a table or other database can be rapidly retrieved and manipulated into a presentation. The ways in which statistical data can be displayed are numerous. The next three figures show examples of statistical data in different formats and related to crimes in an area of operations.

5-33. Figure 5-6 displays the number of burglaries, robberies, and larcenies for each quarter of a given year. Figure 5-7, page 5-12, shows the trend for larceny with a run or line chart. Figure 5-8, page 5-12, displays a pie chart showing the percentage of occurrences for each crime depicted on the chart.

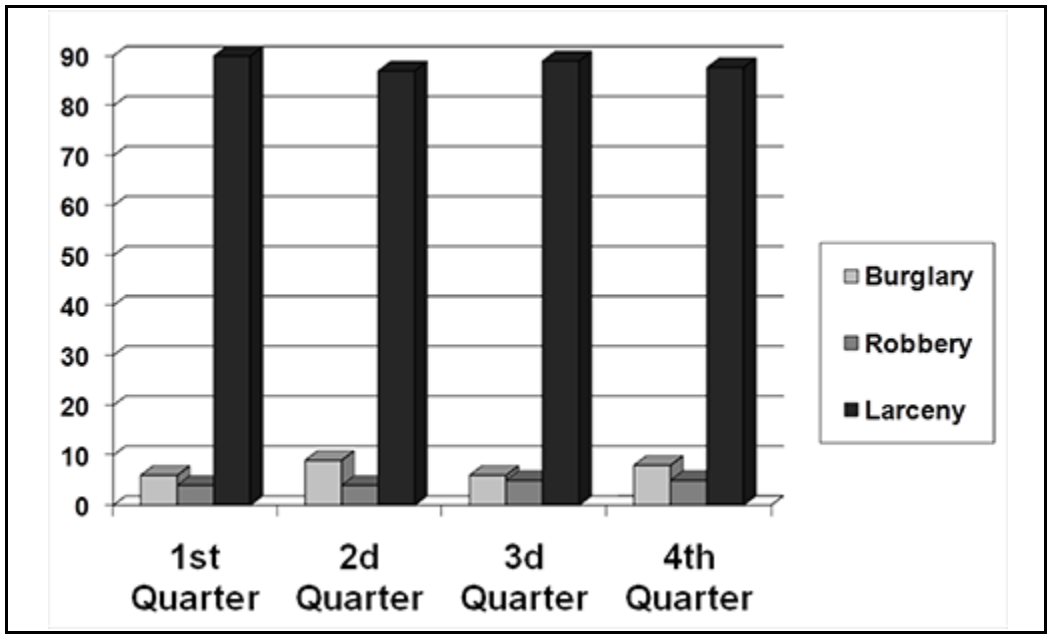


Figure 5-6. Example of a bar graph showing the rate of select quarterly offenses

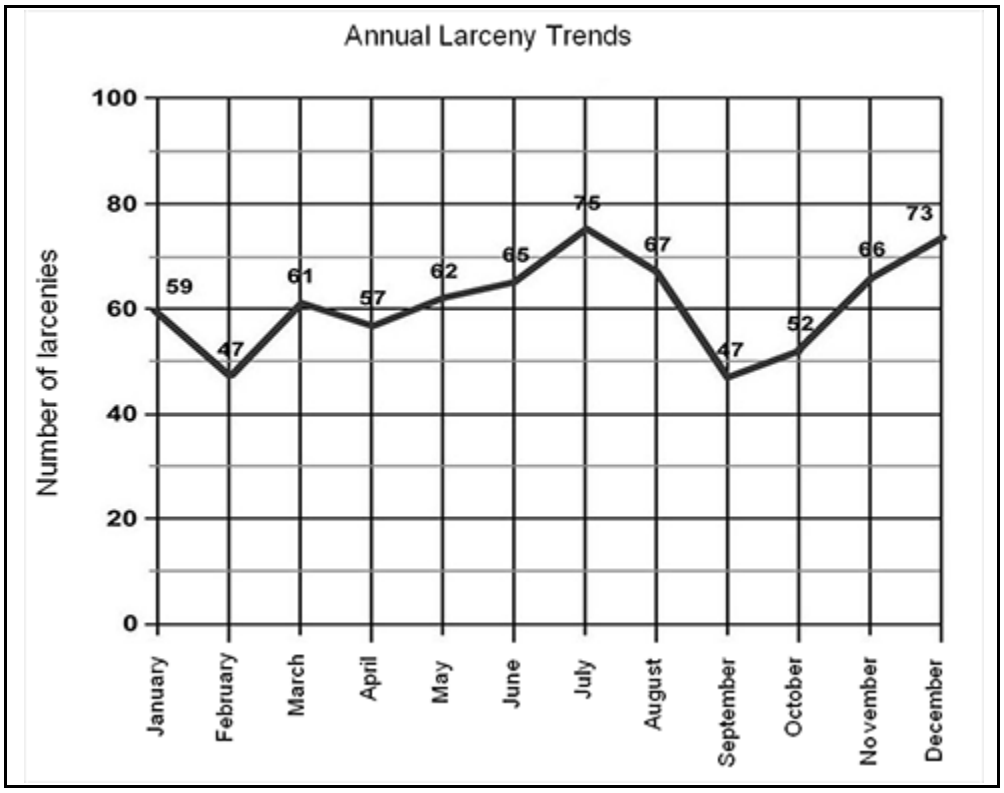


Figure 5-7. Example of a line chart showing annual larceny trends

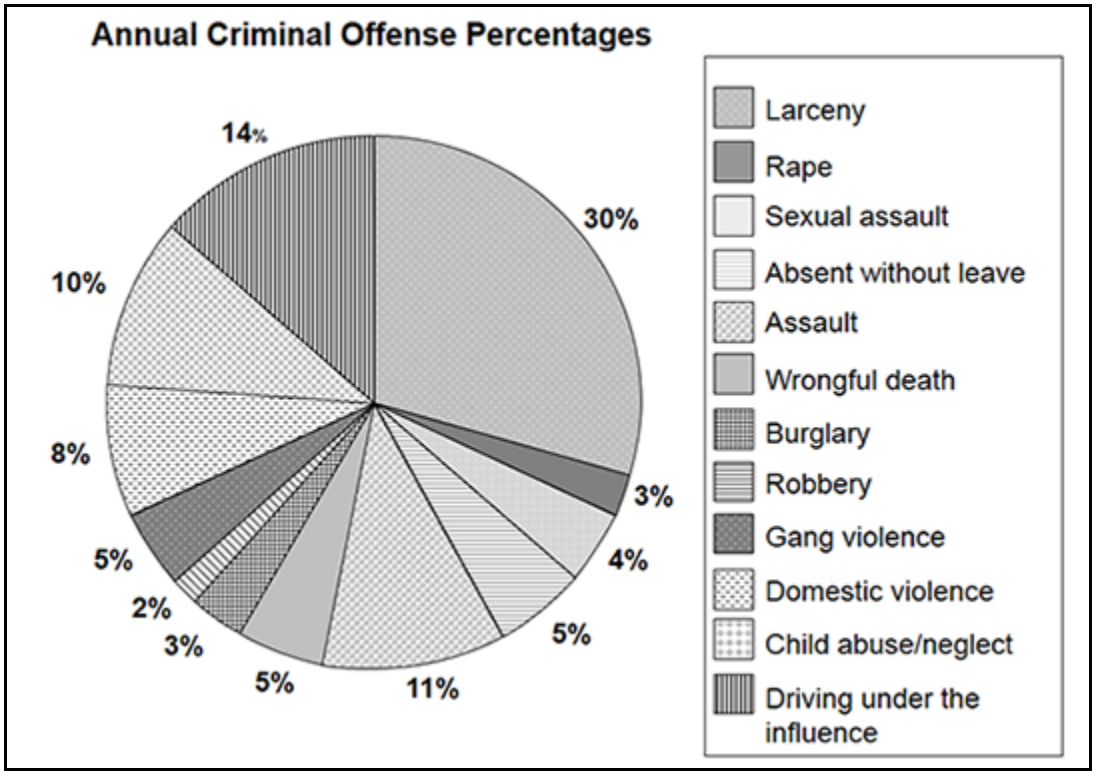


Figure 5-8. Example of a pie chart showing annual crime percentages

WANTED AND REWARD POSTERS

5-34. Wanted posters are clearly intended for public distribution and viewing. Formats typically vary depending on the amount of information known, the specific information sought, and the law enforcement agency producing the wanted poster. Wanted posters are posted by local, state, and federal agencies (to include Army law enforcement). The law enforcement agency or military unit that has the investigative lead for the incident should be the final approval on the wanted poster. This allows the lead investigative agency an opportunity to review the poster to ensure that information about an individual or crime that police are withholding for investigative purposes is not inadvertently released.

5-35. Wanted posters may contain the names, descriptions, and pictures of one or more individuals known to law enforcement. A picture can be an artist's sketch (a rendering of the suspect through the eyes of a witness) or a photograph. The photograph should be as recent as possible. Typically, there will be a short history of the criminal below the sketch or photograph. The wanted poster may include the following information:

- Age, date of birth, and place of birth.
- Sex, height, weight, and hair and eye color.
- Known identifying scars or marks.
- Occupation.
- Nationality.
- Known aliases.

5-36. In some cases, little is known about the individual being sought. In these cases, the wanted poster may simply provide information about a specific crime or an unknown perpetrator and request additional information. Wanted posters may contain instructions on what to do when an individual observes the wanted person. If a reward is offered, the wanted poster should state the reward offered and the individual or agency providing the reward. Wanted posters will also provide points of contact for persons with potential information.

5-37. Wanted posters used in support of decisive action in environments outside the continental United States or in areas within the United States where English is not the primary language must have the information released and the translation carefully screened. It is important to have a native speaker review the wanted poster for the accuracy of the translation and the cultural context of the wanted poster for unintended word use or messages. Figure 5-9, page 5-14, and Figure 5-10, page 5-15, provide examples of wanted posters.

5-38. Reward posters are generated to notify the public that a reward may be available for information specific to a crime or criminal. They are a variant of the wanted poster. Like the wanted poster, reward posters are used to solicit information from the public, but they may also include a tangible incentive in return for information that is provided under specified conditions. (See figure 5-11, page 5-15, for an example of a reward poster.) Reward posters typically contain specific details, to include—

- Reward amounts.
- Specifics about the crime or criminal for which information is sought.
- Pictures (if available) pertinent to the crime or criminal.
- Specific requirements that must be met (such as information leading to recovery or prosecution).
- A point of contact for the reward.
- A confidentiality statement from the provider reference information received.
- Any applicable expirations of the reward offer.

Wanted

ARMED AND EXTREMELY DANGEROUS

PHOTOGRAPH:

Insert photo (if available)

NAME: SUBJECT NAME

DOB: NOVEMBER 29, 1985

SEX: MALE

HEIGHT: 6'1"

WEIGHT: 195 POUNDS

HAIR: BROWN

EYES: BROWN

RACE: WHITE

SCARS OR MARKS: BULLET WOUND ON THE LOWER THIGH AND ON THE RIGHT ARM; SCAR ON THE RIGHT WRIST, LEFT THIGH, AND LEFT ANKLE; AND TRACK MARKS ON THE RIGHT ARM AND BETWEEN THE TOES.

OCCUPATION: CONSTRUCTION

SSN USED: XXX-XX-XXXX

NATIONALITY: AMERICAN

PLACE OF BIRTH: MIAMI, FLORIDA

ALIAS: ALIAS #1; ALIAS #2

IF YOU HAVE ANY INFORMATION CONCERNING THIS CASE, CONTACT YOUR LOCAL FBI FIELD OFFICE.

THE CRIME: UNLAWFUL FLIGHT TO AVOID PROSECUTION–ATTEMPTED MURDER. SUBJECT IS BELIEVED TO BE CONNECTED WITH THE ATTEMPTED MURDER OF A STATE TROOPER WHEREIN A .357-CALIBER PISTOL WAS USED.

REWARD: THE LOCAL FBI FIELD OFFICE IS OFFERING UP TO $50,000 FOR THE APPREHENSION OF THE SUBJECT.

REMARKS: THE SUBJECT HAS BEEN KNOWN TO BE ASSOCIATED WITH THE KLU KLUX KLAN AND OTHER RACIST GROUPS.

SOURCES: JEFFERSON COUNTY SHERIFF DEPARTMENT

FBI HOMEPAGE: <http://www.fbi.gov>

WRITTEN BY: INVESTIGATOR DOE

Legend:

DOB	date of birth
FBI	Federal Bureau of Investigation
SSN	social security number

Figure 5-9. Example of a Federal Bureau of Investigation wanted poster

WANTED
BY CID

Information concerning the offense of larceny of government property from the 29th Sustainment Brigade, Camp Bulldog, Country, APO AE 09090.

USACIDC Report of Investigation 0092-96-CID987-20973-7F9A.

On 1 April XXXX, the USACIDC initiated an investigation into the larceny of government property from the 29th Sustainment Brigade. Between 1800, 29 March XXXX and 0530, 30 March XXXX, person(s) unknown stole one M998 HMMWV, bumper number SVC 4 29TH SB, serial number 044308, from the parking lot adjacent to Building 1013A (Headquarters, 29th Sustainment Brigade), Camp Bulldog, Country.

If you have information about this incident, please contact the CID office at DSN [telephone number] or commercial [telephone number] or call the local military police station.

Legend:

APO	Army post office
CID	criminal investigation division
DSN	Defense Switched Network
HMMWV	high-mobility, multipurpose, wheeled vehicle
USACIDC	United States Army Criminal Investigation Command

Figure 5-10. Example of a USACIDC wanted poster

$10,000.00 REWARD

For information leading to the recovery of a 5-ton wrecker (M936WW), stolen at 1217, 6 March XXXX from the 50th Military Police motor pool, Forward Operating Base Bulldog. All information provided will be kept confidential. If you have information, contact your local military police at DSN [telephone number] or commercial [telephone number] or the Criminal Investigation Division element at DSN [telephone number] or commercial [telephone number].

Legend:

DSN	Defense Switched Network

Figure 5-11. Example of a reward poster

DISSEMINATION

5-39. Dissemination is the activity that delivers an analyzed product into the hands of commanders, provost marshals, staffs, and law enforcement investigators to answer intelligence requirements, enabling decisionmaking and action. It is critical that dissemination occur as early in the process as practical and possible. The need to balance speed with thoroughness should be weighed throughout the process. Commanders and analysts should consider interim reports to provide key data to end users as it becomes available. Oftentimes, waiting for complete information may delay product dissemination so long that the product, although accurate, is too late to be useful to the Soldiers and law enforcement investigators who need it.

COMMAND AND STAFF CHANNELS

5-40. In support of decisive action, PIO leverages command and staff channels to ensure timely and accurate reporting of police intelligence that answers intelligence requirements, CCIRs, or exceptional information identified by the staff or commander that is unforecasted but of immediate value to the command. Command and staff channels will also likely be used to distribute other products (wanted posters, spot reports, BOLOs). This is likely the most efficient method to provide information to every member of a unit or organization. Products disseminated through command and staff channels should clearly articulate the purpose for distributing the product and the action required or requested.

FUNCTIONAL CHANNELS

5-41. Functional channels include military police and law enforcement channels and other groups that operate along functional lines. The law enforcement and intelligence networks are examples of functional channels. Oftentimes, police intelligence is maintained in law enforcement functional channels. This is done to maintain control over sensitive information (as mandated by law) and protect information and intelligence critical to ongoing law enforcement investigations.

COLLABORATION AND FUSION

5-42. Police intelligence networks in support of bases, base camps, and decisive action are developed with the same overarching objective—to enhance police information and police intelligence sharing. Regardless of the operational environment, subtle influences will create variations in network memberships. Influences (availability of agencies in the local area of operations, varied personalities of organizational leaders, cultural or operational differences between agencies) may influence membership participation and team dynamics. For example, military police and USACIDC personnel may not have a local Federal Bureau of Investigation or Bureau of Alcohol, Tobacco, and Firearms field office in their immediate area of operations or United Nations civilian police may be operating in the immediate area of operations with the headquarters and support elements hundreds or thousands of miles away. Despite local variations, general guidelines for developing, managing, and participating in police intelligence networks can be established.

5-43. Military police and USACIDC personnel may develop police intelligence networks anywhere in support of missions in any operational environment. Standardization provides a platform for tailoring staff, providing institutional training, and selecting the most appropriate resources (automation, other emerging technologies). The successful development of police intelligence networks may help enhance coordination and cooperation between local agencies and provide a springboard for developing vast regional, national, or international police intelligence networks.

NETWORK PARTICIPANTS

5-44. A police intelligence network should be tailored to meet the requirements of the operational environment and the specific area of operations. Participation is influenced by threat assessments, intelligence requirements, and specific needs of participating agencies. Police intelligence collaboration and networking can occur in predetermined working groups with relatively set membership, structure, and function or in ad hoc methods created for a specific mission or event. A police intelligence network will typically consist of agencies located in the immediate area of operations; however, with the expansion of

communications and internet technology, participation from outside the immediate area of operations is possible. This allows participation and sharing to occur between agencies located across the state, country, or world. Such arrangements may fill essential capability gaps in the police intelligence network. If particular agencies are not represented in the local environment (Federal Bureau of Investigation, Drug Enforcement Administration field offices, military intelligence, host nation law enforcement), military police and USACIDC personnel can add them to their network by leveraging another police network or making direct contact with the agency using Web-based intelligence services.

NETWORKS IN SUPPORT OF BASES AND BASE CAMPS

5-45. Police intelligence networks established to support law enforcement and security efforts at bases and base camps can provide significant capability to address the complexities of the criminal threat to military assets and personnel. Cooperation between local, state, federal, and military agencies enhances law enforcement and security operations for the military and local civilian community. Typically, networks in support of bases and base camps are more static than those supporting decisive action, and they provide continuity that builds institutional knowledge of crime and criminal threats; physical and social conditions; and long-term relationships with local, state, and federal law enforcement agencies in the area of operations. Most police intelligence networks will typically have a core of constant participants and the flexibility to expand to form focused ad hoc, threat-specific cells to address, prevent, or react to a specific hazard, condition, or event.

5-46. Figure 5-12 provides an example of a police intelligence network supporting a typical base or base camp. Specific networks will differ slightly, based on available participants. Military police and USACIDC personnel are located in the center, post agencies are on the right, and agencies located off base are on the left. Typical law enforcement agencies may include international, federal, state, and local law enforcement, depending on whether the base is in the continental United States or outside the continental United States. Relationships between Army law enforcement personnel and other police intelligence network members will differ. Some network members will require day-to-day working relationships, while others will be based on mutually supporting relationships for selected routine activities or occasional collaboration.

Legend:	
DA	Department of the Army
MP	military police
USACIDC	United States Army Criminal Investigation Command

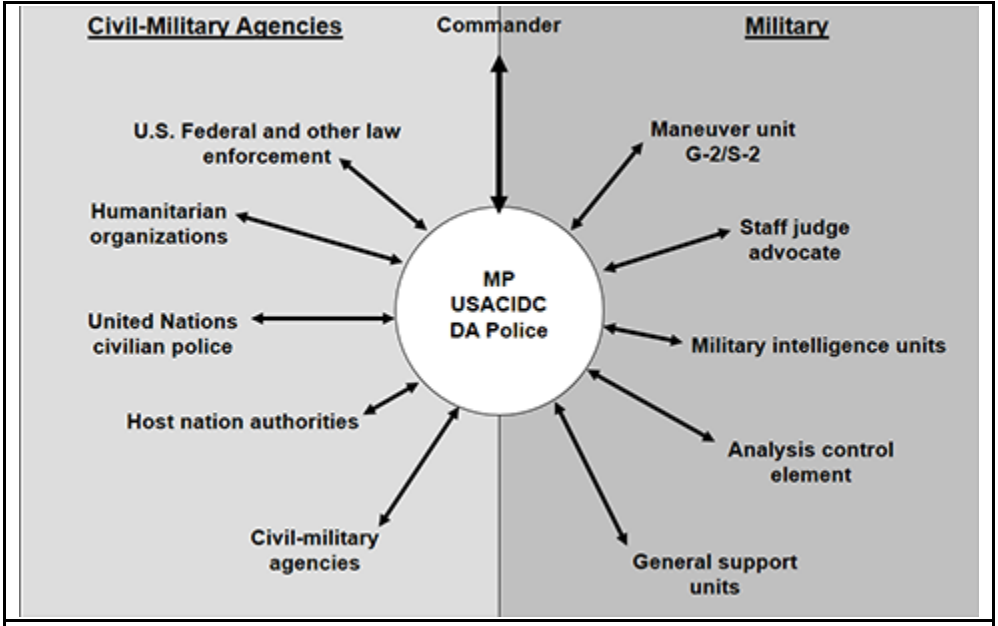
Figure 5-12. Typical police intelligence network in support of a base or base camp

5-47. Police intelligence network relationships between agencies will fluctuate based on numerous factors in the operational environment. Relationships will also continue to develop as bonds are strengthened through joint ventures and as agencies expand their own operating networks. Missions and priorities of individual organizations will greatly affect participation and the level of sharing conducted.

NETWORKS IN SUPPORT OF DECISIVE ACTION

5-48. Police intelligence networks are formed to support specific missions or operations during decisive action. These networks are affected by unit deployments and rotations, governmental and civilian organizations operating in the area of operations, mission changes, and threat changes. These factors equal continuity that builds institutional knowledge of crime and criminal threats, improved physical and social conditions, and additional long-term relationships (often difficult to attain). Specific conditions or threats may bring additional resources and expertise to the area of operations and increase participation in the network. Similarly, mission changes and force reductions in the area of operations may reduce or shift the number of participating elements.

5-49. Figure 5-13 shows a typical PIO network in a deployed operational environment. Like the previous example, these police intelligence networks will vary in composition based on mission and operational variables. Civil-military agencies are located on the left, and military organizations are located on the right.



Legend:	
DA	Department of the Army
G-2	assistant chief of staff, intelligence
MP	military police
S-2	battalion or brigade intelligence staff officer
U.S.	United States
USACIDC	United States Army Criminal Investigation Command

Figure 5-13. Typical PIO network in a deployed operational environment

5-50. The success of the police intelligence network depends on the mutual exchange of timely, relevant, and accurate police intelligence products prepared according to established laws and regulations. To accomplish this, military police and USACIDC personnel should work closely with other agencies to thoroughly understand the strengths and weaknesses of each organization. This enables the organizations to capitalize on their respective strengths and compensate for organizational weaknesses, enabling organizational capabilities to complement each other. The respective staffs should understand each

organization's vision, mission, goals, and objectives and identify and develop strategies to overcome cultural, organizational, and operational barriers.

APPROPRIATE COMMAND AND STAFF ALIGNMENT

5-51. Military police and USACIDC personnel and commanders should identify and properly correlate their personnel with those of other organizations. This is important to ensure that coordination between staff and commanders from different organizations is conducted with counterparts operating at a similar level and span of control in other organizations. It is important to nest similar command and staff, levels of authority, and intelligence functions appropriately between agencies to increase interoperability. Similar terms for ranks or titles between organizations do not necessarily translate to the same management level. For example, a lieutenant with the state police may be the equivalent of a military police colonel. A full understanding of the counterpart structure and appropriate staff alignment can avoid embarrassment and help build personal working relationships with more effective interagency cooperation and intelligence sharing. Using a modified organizational chart, managers can identify comparable staff positions and existing gaps between organizations.

COMMUNICATIONS

5-52. A comprehensive communications system to support the police intelligence network will ensure uninterrupted contact between elements when necessary. Contact lists for all agencies should be disseminated throughout the network and routinely checked to validate less frequent contacts and maintain personal working relationships. It is desirable that agencies have compatible communication methods and networks for support. Communication methods and networks may include—

- Communication methods.
  - Telephones.
  - Radios.
  - Facsimile machines.
  - E-mail.
  - Web sites.
  - Video teleconferencing.
  - Computer databases.
- Communication networks.
  - SIPRNET.
  - Nonsecure Internet Protocol Router Network.
  - Electronic intelligence interface.
  - Law enforcement-specific information exchange networks.

POLICE INTELLIGENCE FUSION CELLS

5-53. Fusion is a collaborative effort between two or more organizations working together and sharing resources, expertise, and information to enhance the ability of participating elements to detect, investigate, and respond to prevent or mitigate crime and criminal activity. It involves the processing of information from multiple systems, assets, and sources and translating that information into refined information and police intelligence products that increase situational understanding and knowledge. Fusion enables commanders and Army law enforcement to have a significant observe, orient, decide, and act advantage over criminal networks and terrorist groups, cells, and individuals. This effort enables commanders, provost marshals, and law enforcement investigators to guide and direct actions that achieve desired effects. The combination of trained and experienced staff, law enforcement personnel, and police intelligence analysts, coupled with open information sharing agreements and advances in technology, allows the elements participating in the fusion process to analyze a variety of information from different organizations, collection assets, and systems to more effectively produce police intelligence for personnel making decisions.

5-54. In some cases, a police intelligence fusion cell may be formed to facilitate the collaboration, integration, and fusion of police information and police intelligence with other law enforcement and intelligence agencies and organizations. The primary purpose of a police intelligence fusion cell is the collation, correlation, and fusion of data from multiple sources, enabling further analysis to produce police intelligence and increased knowledge concerning police, crime, and criminal activities. This enables the military police and USACIDC personnel and police intelligence analyst to build a coherent picture of the environment to increase situational understanding and enable informed decisionmaking by commanders, provost marshals, and law enforcement investigators regarding policing and investigative activities. The collaboration of law enforcement and military intelligence information and intelligence in a police intelligence fusion cell enhances the overall police intelligence effort.

5-55. Fusion cells are typically formed to support specific investigations, missions, and operations. Fusion cells are more focused and meet more frequently than working groups. These cells may be required to work continuously to support their assigned mission and purpose. Police intelligence fusion can provide police information and police intelligence to the operations process and supporting integrating processes. The Criminal Investigation Task Force (see paragraph 1-20) is an example of a fusion cell. In the United States, these cells may include local, county, state, federal, tribal, and the source intelligence agencies operating in or supporting policing and law enforcement operations in the area of operations. Outside the United States, this agency interaction and coordination may include other military units, military and civilian U.S. and multinational organizations, host nation law enforcement elements, and other governmental organizations. The composition of the fusion cell in any environment depends on the specific mission of the organizations and agencies involved. Table 5-1 shows an example of the composition for a police intelligence fusion cell.

Table 5-1. Example of police intelligence fusion cell composition

In Support of Bases or Base Camps and Defense Support of Civil Authorities	***In Support of Unified Land Operations Outside the United States or its Territories***
Military police (to include DA civilian police)	Military police (to include DA civilian police)
USACIDC	USACIDC
Local, state, and federal law enforcement	Civilian police
902d Military Intelligence	902d Military Intelligence
	S-2 or G-2
	HN police and security forces
Legend:	
DA	Department of the Army
G-2	assistant chief of staff, intelligence
HN	host nation
S-2	battalion or brigade intelligence staff officer
USACIDC	United States Army Criminal Investigation Command

5-56. The employment of police intelligence fusion activities is applicable across the range of military operations. Fusion activities work well for analyzing complex criminal organizations and establishing trends, patterns, and associations from information gathered across a large area of operations and multiple organizational areas and jurisdictions. These activities can identify duplications of effort and enable participating elements to eliminate unnecessary duplications of collection and analysis activities. The effective application of fusion activities can facilitate the coordination and synchronization of local, state, national, international, service intelligence, and private sector organization capabilities while simultaneously enhancing the commander's common operational picture.

Appendix A

Legal Requirements and Authorities

The number of agencies involved in police intelligence and the array of applicable laws, regulations, and directives can make negotiating the various authorities and restrictions complex. Military police and USACIDC personnel leverage the expertise and advice of a judge advocate to ensure compliance with all legal parameters in which military police and USACIDC personnel must operate. This is especially true when planning and conducting PIO in support of domestic antiterrorism, defense support of civil authorities, and homeland defense programs or foreign stability operations where the rule of law is established and enforced. Military police, DOD police, and USACIDC personnel collect, manage, analyze, produce, and disseminate police information and police intelligence under the legal instruments of national and international laws, federal statutes, DOD and DA directives and regulations, and SOFAs. Military law enforcement personnel are governed by information acquisition regulations (most notably DODD 5200.27) not by intelligence regulations. This appendix addresses those documents most relevant to the PIO collection efforts. A summary of each document (with respect to its relevancy and applicability to the PIO function) and its restrictions and provisions to Army law enforcement conduct of PIO are discussed in this appendix.

AUTHORITY TO CONDUCT POLICE INTELLIGENCE OPERATIONS

A-1. While the following authoritative documents do not specifically refer to PIO, they do provide the authority and the premises on which to conduct PIO on installations. It is the police information and police intelligence that results from the activities described in the documents that comprise PIO activities. DODI 2000.12, as implemented by AR 525-13, directs commanders to ensure that they have a capability to collect, receive, evaluate, analyze, and disseminate relevant data on terrorist activities, trends, and indicators of an imminent attack. It also requires commanders to fuse suspicious activity reports from military security, law enforcement, and counterintelligence organizations with national level information collection activities.

A-2. DODI 2000.16 directs commanders to task the appropriate organizations under their command to gather, analyze, and disseminate terrorism threat information, as appropriate. It requires the Army to ensure that forces are trained to maximize the use of information derived from law enforcement liaison and intelligence and counterintelligence processes and procedures. This includes intelligence procedures for handling PIR or in-transit units and the implementation of procedures to conduct intelligence preparation of the battlefield and mission analyses.

A-3. AR 525-13 directs commanders to ensure that the appropriate intelligence and law enforcement organizations in their command collect and analyze criminal threat information and that the collection operations are being conducted according to applicable regulations and directives. It also requires commanders to ensure that threat information prepared by the intelligence community, USACIDC, provost marshals, and other organizations or sources is used when conducting threat assessments.

EO 12333

A-4. EO 12333 provides direction to U.S. intelligence activities and is intended to enhance human and technical collection techniques. While serving that purpose, nothing in the order is to be construed to apply or interfere with authorized civil or criminal law enforcement responsibility of any department or agency. Likewise, PIO does not include the collection, production, and dissemination of military and

military-related foreign intelligence and counterintelligence or information on the foreign aspects of narcotics production and trafficking as contemplated by EO 12333. Only foreign intelligence and counterintelligence elements (S-2) are authorized to conduct such activities on behalf of the U.S. Army.

A-5. This order provides for nonconsensual physical searches in the United States by the Federal Bureau of Investigation and other law enforcement activities in specific situations (such as searches by counterintelligence elements of the military services directed against military personnel in the United States or abroad for intelligence purposes). Nonconsensual physical searches are authorized by a military commander empowered to approve physical searches for law enforcement purposes, based on a probable cause finding (such as the belief that a person is acting as an agent of foreign powers). (See EO 12333.)

A-6. National foreign intelligence collected at locations outside the continental United States is coordinated with the Central Intelligence Agency (if not otherwise obtainable). Collection procedures performed in the continental United States are coordinated with the Federal Bureau of Investigation. EO 12333 allows intelligence agencies to—

- Cooperate with appropriate law enforcement agencies for protecting employees, information, property, and facilities of any agency in the intelligence community.
- Participate in law enforcement activities to investigate or prevent clandestine intelligence activities by foreign powers or international terrorist or narcotics activities, unless otherwise precluded by law or EO 12333.
- Provide specialized equipment, technical knowledge, or assistance from expert personnel for use by any department or agency or, when lives are endangered, to support local law enforcement agencies. The provision of assistance by expert personnel is approved by the general counsel of the providing agency on a case-by-case basis.
- Render any other assistance and cooperation to law enforcement authorities not precluded by applicable law.

DODD 3025.18

A-7. DODD 3025.18 establishes DOD policy and assigns responsibilities for providing military assistance to civilian authorities. It establishes the procedures and reporting requirements for DOD assistance to civilian authorities.

A-8. This directive does not apply to the Inspector General of the DOD, the Defense Criminal Investigative Service, or military criminal investigative organizations (USACIDC, the Naval Criminal Investigations Service, the Air Force Office of Special Investigations) when they are conducting joint investigations with civil law enforcement agencies pertaining to matters in their respective jurisdictions and using their own forces and equipment. It also does not apply to support to authorized inspector general or military criminal investigative organization investigations by elements in the DOD.

DODD 5200.27

A-9. The purpose of DODD 5200.27 is to establish the general policy, limitations, procedures, and operational guidance pertaining to collecting, processing, storing, and disseminating information concerning persons and organizations not affiliated with DOD. This directive pertains to the acquisitioning of information concerning the activities of individuals and organizations (not affiliated with the DOD) in the United States, the Commonwealth of Puerto Rico, and U.S. territories and possessions. It also applies to non-DOD affiliated U.S. citizens anywhere in the world. While serving this purpose, nothing in this directive—

- Prohibits the prompt reporting to law enforcement agencies of any information indicating the existence of a threat to life or property, a violation of law, or the prohibited use of record keeping on such a report.
- Restricts the direct acquisition of information by overt means. Information acquired under this directive will be destroyed in 90 days unless its retention is required by law or is specifically authorized under criteria established by the Secretary of Defense or their designee.

A-10. The DOD policy prohibits the collecting, reporting, processing, or storing of information on individuals or organizations not affiliated with the DOD, except in limited circumstances where such information is essential to the accomplishment of DOD missions. Information-gathering activities will be under overall civilian control, with a high level of general supervision and frequent inspections at the field level. Where collection activities are authorized to meet an essential requirement for information, maximum reliance will be placed on domestic civilian investigative agencies—federal, state, and local. In applying the criteria for the acquisition and retention of information established pursuant to DODD 5200.27, due consideration will be given to the need to protect DOD functions and property in the different circumstances existing in geographic areas outside the continental United States. Relevant factors include the—

- Level of disruptive activity against U.S. forces.
- Competence of host nation investigative agencies.
- Degree to which U.S. military and host nation agencies exchange investigative information.
- Absence of other U.S. investigative capabilities (such as in the unique and vulnerable positions of U.S. forces abroad).

A-11. DODD 5200.27 authorizes Army law enforcement personnel to gather information to accomplish the following missions:

- **Protection of DOD functions and property.** Information may be acquired about activities threatening military and civilian personnel, activities, and installations, to include vessels, aircraft, communications equipment, and supplies. Only the following types of activities justify the acquisition of information under the authority of this paragraph:
  - Subversion of loyalty, discipline, or morale of DOD military or civilian personnel by actively encouraging the violation of law, disobedience of a lawful order or regulation, or disruption of military activities.
  - Theft of arms, ammunition, or equipment or the destruction or sabotage of facilities, equipment, or records belonging to DOD units or installations.
  - Acts jeopardizing the security of DOD elements or operations or compromising classified defense information by unauthorized disclosure or espionage.
  - Unauthorized demonstrations on DOD installations.
  - Direct threats to DOD military or civilian personnel in connection with their official duties or to other persons who have been authorized protection by DOD resources.
  - Activities endangering facilities that have classified defense contracts or that have been officially designated as key defense facilities.
  - Crimes for which the DOD has responsibility for investigating or prosecuting.
- **Personnel security.** Investigations may be conducted in relation to the following categories of personnel:
  - Members of the armed forces, including retired personnel, members of the reserve components, and applicants for commission or enlistment.
  - DOD civilian personnel and applicants for such status.
  - Persons having a need for access to official information requiring protection in the interest of national defense under the DOD Industrial Security Program or being considered for participation in other authorized DOD programs.
- **Civil disturbance operations.** The Attorney General is the chief civilian officer in charge of coordinating federal government activities relating to civil disturbances. Upon specific authorization of the Secretary of Defense or their designee, information may be acquired that is essential to meet operational requirements flowing from the mission assigned to the DOD to assist civil authorities in dealing with civil disturbances. Such authorization will only be granted when there is a distinct threat of a civil disturbance exceeding the law enforcement capabilities of state and local authorities.

A-12. DODD 5200.27 identifies instances in which Army law enforcement personnel are prohibited from collecting information on individuals and organizations. The prohibitions state that—

- The acquisition of information on individuals or organizations not affiliated with the DOD will be restricted to what is essential to the accomplishment of assigned DOD missions under this directive.
- No information will be acquired about a person or organization solely because of lawful advocacy of measures in opposition to government policy.
- There will be no physical or electronic surveillance of federal, state, or local officials or of candidates for such offices.
- There will be no electronic surveillance of any individual or organization, except as authorized by law.
- There will be no covert or otherwise deceptive surveillance or penetration of civilian organizations unless specifically authorized by the Secretary of Defense or their designee.
- No DOD personnel will be assigned to attend public or private meetings, demonstrations, or other similar activities for acquiring information (the collection is authorized by DODD 5200.27) without specific approval by the Secretary of Defense or their designee. An exception to this policy may be made by the local commander or higher authority when, in their judgment, the threat is direct and immediate and time precludes obtaining approval. In each case, a report will be made immediately to the Secretary of Defense or their designee.
- No computerized data banks will be maintained relating to individuals or organizations not affiliated with DOD unless authorized by the Secretary of Defense or their designee.

DODD 5240.01

A-13. According to EO 12333, DOD has established procedures in DODD 5240.01 for the collection, retention, and dissemination of information concerning U.S. persons. Special emphasis is given to the protection of the constitutional rights and privacy of U.S. citizens. DODD 5240.01 applies to DOD intelligence components and activities. It does not apply to authorized law enforcement activities carried out by DOD intelligence components having a law enforcement mission.

AR 190-24

A-14. AR 190-24 establishes policy and procedures for the establishment and operation of armed forces disciplinary control boards. Armed forces disciplinary control boards are established by installation, base, or station commanders to advise and make recommendations to commanders on matters concerning the elimination of conditions that adversely affect the health, safety, welfare, morale, and discipline of armed forces personnel. The armed forces disciplinary control board composition typically includes representatives from the following functional areas—

- Law enforcement agencies. On an armed forces disciplinary control board where an Army installation is the senior service, the provost marshal typically serves as the senior Army armed forces disciplinary control board representative.
- Legal counsel.
- Health.
- Environmental protection.
- Public affairs.
- Equal opportunity programs.
- Fire and safety programs.
- Chaplain.
- Alcohol and drug abuse programs.
- Personnel and community activities.
- Consumer affairs.

A-15. Civil agencies or individuals may be invited to board meetings as observers or witnesses or to provide assistance where they possess knowledge or information pertaining to problem areas in the

jurisdiction of the board. Typically, local law enforcement agencies regularly participate in armed forces disciplinary control board proceedings.

A-16. In support of armed forces disciplinary control board mandates, Soldiers and military or DA civilian police may be required to perform off-installation operations. These law enforcement personnel must be thoroughly familiar with the applicable agreements and constraints of Section 1385, Title 18, United States Code (18 USC 1385) and U.S.-host nation agreements. In the United States or its territories, U.S. military and/or DA civilian police assigned to off-installation operations have the sole purpose of enforcing regulations and orders pertaining to persons subject to their jurisdiction. When accompanying civilian law enforcement officers, these policing forces remain directly responsible to, and under the command of, their military chain of command. Military and DA civilian police may come to the aid of civilian law enforcement officers to prevent the commission of a felony or injury to a civilian law enforcement officer.

A-17. The constraints on the authority of Soldiers or DA civilian police to act on off-installation operations (and the specific scope of off-installation operations) will be clearly delineated in all authorizations for off-installation support. Off-installation operations will be coordinated with the local installation commander through the staff judge advocate or higher authority and the appropriate civilian law enforcement agencies.

A-18. AR 190-24 establishes the primary objectives of off-installation operations as—

- Rendering assistance and providing information to service personnel.
- Preserving the safety and security of service personnel.
- Preserving good order and discipline among service personnel and reducing off-installation incidents and offenses.
- Maintaining effective cooperation with civil authorities and community leaders.

AR 190-45

A-19. This regulation establishes law enforcement reporting requirements for Army law enforcement organizations. It also establishes geographic areas of responsibility for reporting incidents involving Army personnel and assets. The regulation—

- Prescribes policies and procedures for submitting criminal history data (biometrics) to the Criminal Justice Information System.
- Provides policies and procedures for Army participation in the National Crime Information Center, Criminal Justice Information System, and supplements standards and procedures established in the Federal Bureau of Investigation National Crime Information Center Operating Manual and the National Law Enforcement Telecommunications System.
- Mandates the use of COPS and the Military Police Reporting System as the automated reporting systems to standardize law enforcement reporting throughout the Army.
- Prescribes responsibilities and updates policies and procedures for reporting serious incidents in the DA. The Serious Incident Report System—
  - Provides early notice to Headquarters, DA, regarding serious incidents.
  - Provides the chain of command with timely information enabling an informed response to queries from DOD, news media, and others.
  - Meets law enforcement reporting requirements for selected criminal incidents and provides law enforcement personnel (DHS, Transportation Security Administration) the most current information available.

A-20. In referring specifically to PIO, AR 190-45 states that in regard to garrison law enforcement operations, the purpose of gathering police intelligence is to identify individuals or groups of individuals in an effort to anticipate, prevent, or monitor possible criminal activity. Police intelligence that is developed and factually establishes that a criminal offense may have occurred results in the initiation of an investigation by military police and USACIDC or other investigative agencies.

A-21. AR 190-45 affirms the importance of establishing agreements between military law enforcement and civilian law enforcement counterparts to facilitate improved information sharing, especially concerning investigations, arrests, and prosecutions involving military personnel. This regulation provides policy

guidance regarding the establishment of formal memorandums of understanding with civilian law enforcement agencies to establish or improve the flow of information between agencies.

A-22. This regulation establishes policy regarding the—

- Active exchange of police intelligence between DOD law enforcement; military police; USACIDC; and local, state, federal, and international law enforcement agencies.
- Transmission of written law enforcement-related documents. Written extracts from local police intelligence files provided to an authorized investigative agency must have the following statement included on transmittal documents: This document is provided for information and use. Copies of this document, enclosures thereto, and information therefrom, will not be further released without the approval of the installation provost marshal.
- Public dissemination of police intelligence files. Local police intelligence files may be exempt from certain disclosure requirements as outlined in AR 25-55 and the *Freedom of Information Act*.

AR 195-2

A-23. AR 195-2 prescribes responsibilities, missions, objectives, and policies pertaining to USACIDC. This regulation requires commanders to report suspected criminal activity to Army law enforcement personnel and notify investigative services. Criminal incidents in the Army are reported to the military police. Serious criminal incidents, as defined in AR 195-2, are reported to USACIDC personnel. AR 195-2 requires that the focus of the police information program be to detect, analyze, and prevent criminal activity from affecting the Army. In part, the purpose of this program is to conduct criminal investigations, crime prevention, and PIO, which are essential to the effective operations of the Army. This includes personnel security, internal security, and criminal and other law enforcement matters, This regulation, like AR 190-45, requires close coordination between DOD law enforcement agencies; military police; USACIDC; and local, state, federal, and international law enforcement agencies. This regulation also requires that police information and police intelligence be actively exchanged between them. This interaction between different agencies allows for the creation of networks, forums, and fusion cells. These shared, fused systems enhance the ability of Army law enforcement personnel to produce timely, accurate, and relevant intelligence that is crucial to the commander's decisionmaking ability.

AR 380-13

A-24. AR 380-13 implements DODD 5200.27 and establishes policy and procedures governing the acquisition, reporting, processing, and storage of information on persons or organizations not affiliated with DOD. It does not apply to authorized criminal investigations and law enforcement information-gathering activities, which are the responsibilities of military police and the USACIDC Investigation Command. Such activities will continue to be conducted according to applicable regulations. It states that no information will be acquired about a person or organization solely because of lawful advocacy of measures in opposition to U.S. government policy or because of activity in support of racial and civil rights interests. It provides other restrictions on the types of information that may be collected as they apply to the intelligence community. This regulation allows for prompt reporting to Army law enforcement personnel any information that indicates the existence of a threat to life or property and the violation of a law.

AR 381-10

A-25. AR 381-10 is a military intelligence community regulation. The procedures of this regulation do not apply to Army law enforcement personnel. If, during an Army intelligence component investigation, evidence surfaces that provides reasonable belief that a crime has been committed, details of the investigation will be relinquished to the USACIDC or the appropriate military police investigating agency according to AR 190-45 and AR 195-2.

A-26. Agencies within the military intelligence community are authorized to—

- Cooperate with law enforcement agencies for protecting the employees, information, property, and facilities of any agency in the intelligence community.
- Participate in law enforcement activities to investigate or prevent clandestine intelligence activities on foreign equipment or technical knowledge, provide assistance from expert personnel for use by any department or agency, or support local law enforcement agencies when lives are endangered (unless otherwise precluded by law or AR 381-10). The provision of assistance by expert personnel will be approved by general counsel of the providing agency on a case-by-case basis.
- Render other assistance and cooperation (not precluded by applicable law) with law enforcement authorities.

A-27. Army law enforcement personnel can expect cooperation (consistent with DODI 3025.21) from the military intelligence community for the purpose of—

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

A-28. A significant item that AR 381-10 highlights is the definition of collection. In the text of this regulation, its definition is different from the everyday, common definition of assemble or gather. In AR 381-10, collection includes the intent to use or retain information received and includes information received from cooperating sources in the collection effort. The intent of this definition, although not stated in this regulation, is also the intent of information collection efforts by Army law enforcement personnel.

AR 525-13

A-29. AR 525-13 establishes and provides implementation guidance and requirements for the antiterrorism program. The antiterrorism program protects personnel, to include—

- Soldiers.
- Members of other Services.
- DA civilian employees.
- DOD contractors.
- Family members of DOD employees.
- Information.
- Property.
- Facilities (including civil work and similar projects).

A-30. Military police and USACIDC elements hold critical responsibilities due to their law enforcement missions and ability to collect, analyze, disseminate, and manage police intelligence. Specific responsibilities are given to the Provost Marshal General and USACIDC commander for implementation. The Provost Marshal General, acting in direct support to the Headquarters, DA; Deputy Chief of Staff; Operations, Plans, and Training (G-3/5/7) for the management and execution of the Army antiterrorism mission, is responsible for—

- Staffing and providing an antiterrorism branch to serve as the functional proponent and for establishing policy and objectives regarding the antiterrorism program.
- Operating the Army Threat Integration Center in close coordination with the Headquarters, DA; Office of the Deputy Chief of Staff, G-2, to—
  - Issue early warning of criminal and terrorist threats to Army commands, Army Service component commands, direct reporting units, and other senior Army leaders and organizations.
  - Coordinate the analyses and reporting of terrorist-related intelligence with appropriate intelligence and law enforcement agencies to provide warnings and maintain visibility of threats to senior Army leadership; major commands (Army major commands, Army Service

component commands, and direct reporting units); and threatened installations, activities, facilities, and personnel.

- Fuse criminal and terrorist threat information to form a single threat picture.
- Assess terrorist and criminal threats to Army forces and publish an annual comprehensive DA threat statement and daily DA force protection memorandum to disseminate potential and future threats, thereby enhancing threat awareness at all levels.

A-31. AR 525-13 also outlines specific responsibilities for the Commander, USACIDC, as the senior commander responsible for Army criminal investigations. USACIDC is responsible for—

- Ensuring a sufficient USACIDC police intelligence capability to monitor and report on the activities, intentions, and capabilities of domestic threat groups (according to applicable regulations and directives).
- Collecting, analyzing, and disseminating police intelligence to affected commands pertaining to threat activities (in the provisions of applicable statutes and regulations).
- Providing appropriate threat-related police intelligence to Headquarters, DA; the Army Threat Integration Center; the Intelligence and Security Command; and the Army Counterintelligence Center.
- Maintaining a capability to analyze and disseminate collected, time-sensitive information concerning the criminal threat against Army interests.
- Investigating threat incidents of Army interest; monitoring the investigations when conducted by civilian, host nation, military, or other police agencies; and providing applicable results of terrorist-related investigations to the Army Counterintelligence Center, Army Threat Integration Center, and Center for Army Lessons Learned.
- Providing trained hostage negotiators to support Army antiterrorism operations worldwide.
- Planning and coordinating the protection of high-risk personnel for DOD, DA, and foreign officials as directed by Headquarters, DA.
- Serving as the Army primary liaison representative to federal, state, local, and host nation agencies to exchange police intelligence.
- Establishing procedures to ensure appropriate liaison at all levels between USACIDC, the Intelligence and Security Command, and provost marshal elements operating in support of the antiterrorism program.
- Notifying the affected installation provost marshal and Headquarters, DA, upon receipt of time-sensitive threat information immediately.
- Ensuring that criminal activity threat assessments and personal security vulnerability assessments are conducted for Army personnel, installations, systems, operations, and other interests as directed by Headquarters, DA, or based on the Army commander's operational requirements.
- Providing technical personnel support to the Headquarters, DA, Deputy Chief of Staff and designated G-3/5/7 assessment teams, as required.
- Investigating incidents of suspected terrorism as criminal acts, to include safeguarding evidence and collection testimony and preparing investigative reports and presentations for the appropriate judicial officials. Investigations are conducted jointly with federal, state, local, and foreign law enforcement agencies, as appropriate.
- Providing appropriate terrorism analyses and threat assessments to the Army Threat Integration Center in support of Army requirements and the antiterrorism program.

A-32. The regulation also outlines responsibilities for installation and garrison commanders. These commanders are required to—

- Ensure that law enforcement and intelligence organizations in their command collect and analyze criminal and terrorist threat information.
- Develop a system to monitor, report, collect, analyze, and disseminate terrorist threat information.
- Identify a focal point for the integration of operations with local or host nation, intelligence, criminal investigations, police information, and police intelligence.

- Coordinate law enforcement support with higher headquarters in case organic law enforcement is not available.
- Ensure that the command has appropriate connectivity to receive threat-related information and intelligence from classified and unclassified networks, to include products and information from provost marshal offices; local, state and federal law enforcement; and intelligence organizations and fusion centers (Army Threat Integration Center, Federal Bureau of Investigation, USACIDC, Army Counterintelligence Center, Intelink-S, Intelink).
- Ensure that collection operations are being conducted consistent with the requirements and restrictions of AR 380-13, AR 381-10, AR 381-12, DODD 5200.27, and other applicable regulations and directives.
- Establish an antiterrorism program supported by all-source intelligence with PIR; CCIR; and focused collection, analysis, and dissemination to protect personnel and assets in the area of operations.
- Ensure that products and analyses are focused and based on their PIR and CCIR. Review PIR and CCIR for currency, and revalidate them at least annually to update changing threats or requirements.
- Ensure that information and intelligence regarding terrorist activity is developed, collected, analyzed, and disseminated in a timely manner. Current intelligence will be integrated into the antiterrorism training program.

A-33. In reference to terrorist threat assessments, the regulation specifically addresses the law enforcement and intelligence community as follows:

- Threat information prepared by the intelligence community, USACIDC, and the provost marshal's office will be used when conducting threat assessments and collecting technical information from information management.
- Threat assessments will serve as bases and justification for antiterrorism plans, enhancements, program and budget requests, and the establishment of force protection conditions.
- Threat assessments will be part of leader reconnaissance, in conjunction with deployments and follow-on threat and vulnerability assessments (as determined by the commander).
- Consolidated military intelligence and police intelligence data identified in threat assessments (on U.S. personnel) cannot be filed, stored, or maintained as an intelligence product (as directed in AR 381-10). These assessments must be filed, stored, and maintained in operational channels.

STATUS-OF-FORCES AGREEMENT

A-34. A SOFA is typically established when a long-term U.S. presence is required or anticipated. While this is typical, some areas of operations in which U.S. forces operate do not have established SOFA agreements between the United States and host nations. This is common in an area of operations experiencing major combat operations or significant instability. As the theater matures and a stable host nation government establishes control, a SOFA will typically be developed if an enduring U.S. presence is required.

A-35. A SOFA plays a vital role in preserving command authority and the protection of military personnel. The purpose of such an agreement is to set forth rights and responsibilities between the U.S. government and a host nation government on such matters as criminal and civil jurisdictions, uniforms, arms possession, tax and customs relief, entry and exit procedures of personnel and property, and resolutions to damage claims. A SOFA defines the legal status of U.S. personnel and property in the territory of another nation.

A-36. All SOFAs are unique and reflect specific considerations based on the countries entering into the agreement and other factors. A SOFA establishes guidelines for civil and criminal jurisdiction. This process is critical to ensure that the United States and DOD can protect, to the maximum extent possible, the rights of U.S. personnel who may be subject to criminal trials by foreign courts and imprisonment in foreign prisons. Typically, a SOFA will recognize the right of a host nation government to primary jurisdiction, allowing jurisdiction for cases in which U.S. military personnel violate host nation laws. Most SOFAs will

provide two exceptions where the United States may retain primary jurisdiction. These exceptions are for offenses committed—

- By U.S. personnel against U.S. personnel.
- In the performance of official duties.

A-37. In some areas of operations, agreements between the United States and host nation countries may establish legal parameters regarding U.S. authority over host nation personnel. The host nation typically retains jurisdiction over its citizens; however, in some cases, the host nation government may be nonfunctioning or incapable of maintaining security and control over the population. These environments may require U.S. military forces to establish and maintain control over the population until the host nation can assume authority and control. This may be particularly true as operations transition from major combat operations to stability operations and the operational environment becomes stable enough for the host nation to implement the rule of law in dealing with the population and maintaining order. The operational environment that immediately follows a major disaster (natural or man-made) may also cause conditions in which U.S. military forces are required to restore order and maintain control over a host nation population.

A-38. As the operational environment becomes stable and the host nation begins to reestablish the rule of law, U.S. military forces may still be necessary to assist the host nation in policing activities. This is only done pending the full assumption of control by the host nation. During the interim, legal agreements between the host nation and the United States may be established to ensure that the U.S. military and its Soldiers act within the rule of law established by the host nation and that the rights of the local population are maintained.

Appendix B

Briefing and Debriefing Requirements

Successful PIO requires the commander and staff to establish, resource, and conduct mission briefing and debriefing activities. The provost marshal section or S-3 should develop a mission briefing and debriefing plan for preparing mission elements to collect information supporting police intelligence requirements and for gathering postmission information from individual collection assets. Ideally, the mission briefing and postmission debriefing are incorporated as an integrated part of standard mission briefings and synchronized, when appropriate, with S-2 or G-2 intelligence briefing and debriefing requirements.

MISSION BRIEFINGS

B-1. The purpose of a PIO mission briefing is to ensure that personnel conducting missions where the collection of police information is likely or directed are sensitized to specific information and reporting requirements, information gaps, and unique mission requirements. PIO mission briefings may include updated intelligence assessments; a detailed briefing on current mission or investigative information and existing gaps; and specific information, material, or data that may assist police intelligence analysts and staff. These briefings may also include a review of collection objectives and methods to be employed.

B-2. The mission elements briefed may be restricted to a small number of investigative or law enforcement personnel supporting a specific investigation provided to law enforcement personnel operating in an area or include all units operating in an area of operations. In addition, the exact subject matter depends on the nature of the mission, specific requirements, and the sensitivity or classification of known information and police intelligence. The specific content and dissemination decisions are based on operational considerations and classification restrictions that may apply to the information and police intelligence being disseminated.

B-3. A PIO mission briefing may be conducted as a separate presentation or, ideally, integrated in planned mission briefings. Mission briefings are informal briefings that occur during operations. Briefers may be commanders, staffs, or special representatives. The mission briefing format is determined by the nature and content of the information being provided, but it typically follows the operation order format. These briefings are conducted to issue an order; provide detailed instructions or requirements pertaining to the mission; review key points and considerations relevant to the specific mission; and ensure understanding of the mission objective, specific roles in the mission, and potential problems or threats required to overcome or mitigate those problems and threats. (See FM 6-0 for additional information on mission briefings.)

BRIEFING CONSIDERATIONS

B-4. Planning for police intelligence mission briefings requires the consideration of several key elements. First, the identification of the briefing audience is required, consistent with investigative requirements, operational objectives, and information dissemination restrictions. All identified mission elements operating in the area should be thoroughly briefed to ensure that the maximum collection capability is leveraged and synchronized where appropriate. The police intelligence mission briefing should also provide criteria for reporting immediate, time-sensitive information, reporting requirements for nonpriority reporting, and postmission debriefing locations and procedures.

B-5. The PIO brief should include the following:

- Police and criminal environment update.
- Threat update.
  - Route information and current available information and intelligence.
  - Information and intelligence that identifies known and potential high-threat areas and specific threats in the area.
  - Information and intelligence regarding individuals and groups operating in the area that pose threats to U.S. forces and interests.
  - Specific types of criminal and threat activities identified in the area of operations.
- Focus areas for observation.
- Specific collection requirements.
  - Evidence collection priorities.
  - Requirements for the handling and disposition of collected documents.
  - Special requirements for the handling and disposition of captured detainee and enemy materials.
  - Specific requirements for the use of digital photography.
- Specific personnel, activities, materials, data, or evidence that should be reported immediately.
  - Observed conditions inconsistent with normal events (such as an unusually high amount of traffic departing an area or a complete lack of activity by the local population).
  - Indications of an imminent threat to U.S. forces or interests.
  - Identification of specific persons wanted for specific criminal or threat activity.
  - Identification of material or information with strategic value or impact.
  - Time-sensitive information relative to specific criminal activities or investigations.

POSTMISSION DEBRIEFINGS

B-6. The police intelligence debriefing is a process of questioning military police elements and other personnel returning from missions to collect information of potential value. The purpose of a debriefing is to identify and record data and information collected by the mission element. This data may pertain to assigned collection tasks or additional information and observations on the area of operations or to properly identifying and recording evidence gathered during the conduct of the mission.

B-7. Properly conducted police intelligence debriefings ensure that available police information is collected, collated, and assessed in an attempt to answer police intelligence requirements and expand situational understanding. A comprehensive and systematic debriefing program ensures that information from assigned collection tasks is gathered for analysis. It also allows staff and analysts conducting PIO to ask specific questions to pull information gained from observations made by military police elements to enhance situational understanding and fill gaps in current knowledge. When conducting debriefing operations, all mission elements should be debriefed. Debrief—

- Leaders returning from operational liaison positions or meetings.
- Military police and other law enforcement elements (at the conclusion of all missions).
- Functional and multifunctional assessment teams (following missions in the area of operations).
- Other personnel exposed to persons or environments where they may have obtained information of intelligence value.

B-8. The S-2 or G-2, the S-3 or G-3, or provost marshal section and police intelligence analysis personnel should—

- Debrief personnel or provide specific guidance for unit debriefs, to include reporting criteria.
- Collect, collate, and format reports, as required.
- Report police information and police intelligence through prescribed reporting channels based on the information and applicable constraints.

DEBRIEFING CONSIDERATIONS

B-9. After an element returns from a mission, the military police staff, unit leadership, or designated police intelligence debriefing team should conduct a thorough debrief. The debriefing should include all members of the mission element, including the leader, unit members, and any attached personnel. Missions should not be considered complete or personnel released until reports and debriefings are complete.

B-10. The debriefing typically follows the mission briefing format. By maintaining a standard format, the exclusion of critical aspects of the mission is prevented. If possible, reports generated during the mission should be reviewed by the personnel conducting the debriefing activities beforehand to provide a measure of situational awareness and help develop follow-on questions. A review of generated reports before conducting a debriefing of any element enables debriefing personnel to concentrate on filling in gaps and following up on the reported information. If the mission element used digital cameras (or other recording devices), it is helpful to use the photographs during the debriefing. A detailed sketch or map may also be useful for facilitating discussion and ensuring understanding by all parties.

B-11. During the debrief, avoid yes or no questions or questions framed in a way that leads the respondent to a particular answer. The goal of the debrief proceedings is to gain information from the mission element that is not currently available or that corroborates existing information. Debriefing personnel should also ask questions that may extract information from observations or provide other input that the mission element may deem as unimportant but, in fact, may provide police intelligence analysts, staff, and investigators with critical pieces of the police intelligence picture. For example, debriefing personnel should—

- Ask the mission element “What did you see (hear, learn)?” rather than “Did you encounter any criminal or threat activity?”
- Avoid asking questions only for the published police intelligence requirements. This may limit answers obtained from mission personnel, causing valuable information to be missed.
- Use follow-up questions to get complete information before leaving a specific discussion point.
  - “What else?”
  - “Is there anything else you remember?”
- Refrain from focusing only on visual observation; ask questions relating to all senses.
  - “Were there any smells that were particularly noticeable or out of the normal?”
  - “Were there any unusual sounds (lack of sounds)?”

B-12. At the conclusion of the debriefing, document collected observation and material evidence. A PIO debriefing report should be completed and include—

- The size and composition of the mission element.
- The mission type, location, and purpose.
- The departure and return date-time groups.
- The specific area of operations in which the mission was conducted, including routes, engagement areas, and the locations of specific observations and evidence collection sites.
- A detailed description of the terrain in which threat elements were documented or suspected.
- The results of police engagement with the local population or host nation police or officials.
- The unit status at the conclusion of the mission, including the results of any physical engagements with threat elements (include the exact site locations, disposition of dead or wounded Soldiers, and disposition of any dead or wounded civilian and threat persons).
- A description of any physical evidence or materials collected during the mission (including photographs or other recorded materials).
- Conclusions or recommendations.

RESPONSIBILITIES

B-13. The S-3 section or provost marshal section responsibilities include—

- Providing tasking and guidance on specific areas and objectives for police engagement and tactical questioning based on unit PIR and specific police intelligence requirements.
- Synchronizing police intelligence collection requirements with S-2 or G-2 military intelligence collection requirements.
- Providing relevant background police information, police intelligence, or military intelligence and information (to include open-source information) to mission elements to improve their cultural knowledge and situational awareness, thus facilitating effective police engagement, tactical questioning, and protection efforts.
- Establishing procedures to ensure that mission elements are debriefed at the end of the mission.
- Establishing and emphasizing procedures for the immediate reporting of information of critical or time-sensitive tactical value (such as a spot report in the size, activity, location, unit, time, and equipment format).
- Establishing procedures and disseminating special requirements for the proper evidence collection and handling of captured equipment or media (cellular telephones, documents, computers).
- Coordinating for any additional assets required to support police information collection requirements (HUMINT collection teams, civil affairs, engineer support, other support requirements) and to fill military police capability gaps.
- Identifying and briefing units and mission elements (such as site exploitation teams) regarding expedited reporting requirements for specific critical information or high-value targets.

B-14. Unit commander responsibilities include—

- Training and integrating specific collection techniques in the planning, preparation, and execution of military police missions.
- Providing tasking and specific planning guidance to subordinate leaders to ensure the adequate understanding of police intelligence and collection requirements.
- Reviewing intelligence preparation of the battlefield, police intelligence products, and other available data to ensure situational understanding and situational awareness and passing information specific to the unit area of operations to personnel in the S-3, G-3, or provost marshal section and, when applicable, the S-2 or G-2 to improve knowledge of the area of operations.
- Providing full support to unit PIO debriefing activities and compliance with established briefing and debriefing procedures by all military police elements.
- Reinforcing the importance of the procedures for the immediate reporting of information of critical or time-sensitive value.

B-15. Platoon, squad, section, team, and mission leader responsibilities include—

- Training and integrating specific collection techniques in the planning, preparation, and execution of military police missions.
- Providing tasking and specific mission guidance to platoons, squads, or sections to ensure the the adequate understanding of intelligence requirements, collection, and other specific mission requirements.
- Reinforcing the importance of the procedures for the immediate reporting of information of critical or time-sensitive value to personnel.
- Preparing for, and participating in, the unit debriefing activities after military police missions.
- Reporting information based on visual observations and police engagement during the debriefing or through the immediate reporting of critical or time-sensitive information.
- Conducting evidence collection and documentation and compiling written reports during military police missions carefully.

Appendix C

Police Intelligence Initiatives

The law enforcement community in the United States is universally committed to the timely and seamless exchange of terrorist and criminal information and intelligence. In light of the 11 September 2001 terrorist attack and the 2013 Boston marathon bombings, it is critical that law enforcement personnel work together to protect the nation. This appendix identifies some of the key civilian agencies participating in PIO or conducting their own PIO, and it identifies initiatives and coordination methods used by other law enforcement agencies in an effort to facilitate interagency coordination. The civilian law enforcement community typically uses criminal intelligence to refer to police intelligence; whereas, the Army uses police intelligence as the overarching term and criminal intelligence to refer specifically to police intelligence specific to criminal threats and vulnerabilities (typically associated with criminal investigations).

DEFINITIONS AND PROCESSES

C-1. In the civilian police community, there are several definitions and processes that describe criminal intelligence and the criminal intelligence process. Two of the most prevalent variations of the definition of criminal intelligence are the—

- Product of an analytic process that provides an integrated perspective to disparate information about crime, crime trends, crime and security threats, and conditions associated with criminality (see *Law Enforcement Intelligence: A Guide for State, Local, and Tribal Law Enforcement Agencies*).
- Information compiled, analyzed, and disseminated in an effort to anticipate, prevent, or monitor criminal activity (see *Criminal Intelligence Sharing: A National Plan for Intelligence-Led Policing at the Local, State, and Federal Levels: Recommendations From the International Association of Chiefs of Police Intelligence Summit*).

C-2. The civilian law enforcement community typically defines the criminal intelligence process as consisting of six basic steps—

- **Step 1.** Planning the gathering of information.
- **Step 2.** Gathering the information.
- **Step 3.** Processing the information.
- **Step 4.** Analyzing the information to produce an intelligence product.
- **Step 5.** Disseminating the intelligence product.
- **Step 6.** Evaluating the usefulness of the intelligence product.

C-3. The term *intelligence-led policing* is widely current among criminal justice researchers and national policymakers, although there is vigorous debate regarding a definitive description or definition. Regardless of their positions, most officials agree that intelligence-led policing integrates easily with other popular policing models, including community policing and problem-oriented policing. *Law Enforcement Intelligence: A Guide for State, Local, and Tribal Law Enforcement Agencies*, a community-oriented policing services publication, describes intelligence-led policing as the integration of community policing and law enforcement intelligence. *Intelligence-Led Policing: The New Intelligence Architecture*, issued by the Bureau of Justice Assistance and their partners, calls intelligence-led policing a collaborative enterprise based on improved intelligence operations and community-oriented policing and problem solving. ATP 3-39.10 discusses intelligence-led policing as one of seven policing models and strategies.

INITIATIVES AND PROGRAMS

C-4. The sharing of police information has received significant emphasis since the terrorist attacks on 11 September 2001. Several initiatives by the federal government to improve information sharing capabilities between federal, state, local, and tribal agencies have been implemented. The standardization of training to develop a common language, understanding police information and police intelligence, and the development of fusion centers will enable timely exchanges and transmission of police information. The following paragraphs provide information of some of the civilian law enforcement initiatives and programs that enable interagency cooperation and standardization of police intelligence training. These initiatives, while developed in the civilian law enforcement community, are open to Army law enforcement and a thorough understanding of civilian standards, policies, and procedures is critical in successful interagency cooperation between Army law enforcement and federal, state, local, and tribal agencies operating in the same area of operations.

UNITED STATES DEPARTMENT OF JUSTICE SYSTEM

C-5. The United States Department of Justice (DOJ) system, known as OneDOJ (formerly the Regional Data Exchange), is a repository for law enforcement information shared with other federal, state, local, and tribal law enforcement agencies through connections with regional information sharing partnerships. OneDOJ is used to share law enforcement information internally across investigative components and provide regional connectivity for authorized users to conduct searches of OneDOJ information and share law enforcement information. Additional information on OneDOJ can be accessed on the Department of Justice Web site.

C-6. All DOJ law enforcement components (Bureau of Alcohol, Tobacco, and Firearms; Bureau of Prisons; Drug Enforcement Administration; Federal Bureau of Investigation; and the United States Marshal Service) participate in OneDOJ. Criminal information shared includes open- and closed-case documents, investigative reports, witness interviews, data on criminal events, information on criminal histories and incarcerations, and information about individual offenders. Outside agencies connect with OneDOJ through regional sharing systems using a standard secure platform developed through the Law Enforcement Information Sharing Program. The DOJ, through the OneDOJ system, shares information with the Military Criminal Investigative Services (USACIDC, Naval Criminal Investigative Service, Air Force Office of Special Investigations).

Law Enforcement Information Sharing Program

C-7. The Law Enforcement Information Sharing Program is an effort by the DOJ to improve law enforcement information sharing between state, local, tribal, and other federal law enforcement partners. The objective of the program is to share law enforcement information across jurisdictional boundaries to prevent terrorism and to systematically improve the investigation and prosecution of criminal activity. Sharing of law enforcement information with agencies outside DOJ is accomplished through regional sharing centers. Additional information on the Law Enforcement Information Sharing Program can be accessed on the Law Enforcement Information Sharing Web site.

National Information Exchange Model

C-8. The National Information Exchange Model is a national information framework that eases across domain exchanges. It allows transfer of information using standard language and protocols enabling information sharing between various agencies involved in law enforcement, emergency management, homeland security, and other specific domains. The Law Enforcement Exchange Specification is the specific domain in the National Information Exchange Model that enables DOJ and other federal, state, local, and tribal law enforcement organizations to establish law enforcement information exchanges. The Law Enforcement Exchange Specification is the basis for the OneDOJ regional law enforcement information sharing partnerships. Additional information can be found on the National Information Exchange Model Web site.

NATIONAL CRIMINAL INTELLIGENCE SHARING PLAN

C-9. The *National Criminal Intelligence Sharing Plan* resulted from an effort to close identified gaps in police intelligence capability in the aftermath of the terrorist attacks on 11 September 2001. The plan outlines 28 recommendations for implementation by law enforcement agencies to improve sharing of police information. The recommended coverage areas (fusion centers, security clearances, core training standards, technology) emphasize the need to engage every law enforcement agency (regardless of size and type) in the sharing of police information. Additional information on the *National Criminal Intelligence Sharing Plan* and associated recommendations can be found on the Justice Information Sharing Web site.

Criminal Intelligence Coordinating Council and Global Intelligence Working Group

C-10. The Global Intelligence Working Group is composed of federal, state, local, and tribal justice representatives; homeland security representatives; and public safety representatives. The Global Intelligence Working Group has the capability of drawing on subject matter experts external to the working group, as needed. It operates in partnership with the Criminal Intelligence Coordinating Council. The Criminal Intelligence Coordinating Council was formed in 2004 to provide recommendations regarding the implementation and refinement of the national criminal intelligence-sharing plan. The Criminal Intelligence Coordinating Council membership represents law enforcement and homeland security agencies at all levels of government. It serves as an advocate for law enforcement agencies at all levels in the effort to develop and share police intelligence to promote public safety and national security. The Criminal Intelligence Coordinating Council is a policy level organization involved in setting priorities, directing research, and preparing advisory recommendations. The Global Intelligence Working Group and Criminal Intelligence Coordinating Council operate in the framework of the Global Justice Information Sharing Initiative.

Global Justice Information Sharing Initiative

C-11. The Global Justice Information Sharing Initiative is a federal advisory committee advising the U.S. Attorney General regarding law enforcement-related information sharing and associated initiatives. It was created to support the development of law enforcement information exchange applied across all law enforcement agencies and levels of government. The organization promotes standards-based electronic information exchange to provide the justice community with timely, accurate, complete, and accessible information in a secure and trusted environment. Additional information on the Global Intelligence Working Group, the Criminal Intelligence Coordinating Council, and the Global Justice Information Sharing Initiative can be accessed on the Justice Information Sharing Web site.

NATIONAL STRATEGY FOR INFORMATION SHARING

C-12. The *National Strategy for Information Sharing: Successes and Challenges in Improving Terrorism-Related Information Sharing* addresses a capability gap focused on the sharing of homeland security information, terrorism information, and law enforcement information related to terrorism from multiple sources. It calls for a national information-sharing capability through the establishment of a national integrated network of fusion centers. Sources of information addressed in the plan are interdisciplinary. They are from multiple sources at all levels of government and include private sector organizations and foreign sources.

C-13. In addition to traditional law enforcement uses, such information is used to—

- Support terrorism prevention efforts.
- Develop critical infrastructure protection and resilience plans.
- Prioritize emergency management, response, and recovery planning activities.
- Develop training and exercise programs.
- Allocate funding and other resources.

C-14. The *National Strategy for Information Sharing: Successes and Challenges in Improving Terrorism-Related Information Sharing* identifies baseline capabilities requirements for fusion cells. Defining these operational standards enables federal, state, and local officials to identify and plan for the resources needed (including financial and technical assistance and human support) to attain the baseline capacity required for

successful information fusion cells. The baseline capability ensures that fusion cells have the necessary structures, processes, and tools in place to support the gathering, processing, analysis, and dissemination of police information, which includes information and police intelligence in support of specific operational capabilities; suspicious activity reporting; alert, warning, and notification reporting; risk assessments; and situational understanding reporting.

REGIONAL INFORMATION SHARING SYSTEMS

C-15. The Regional Information Sharing Systems® are conduits for the exchange of criminal information and criminal intelligence among participating law enforcement agencies. The Regional Information Sharing Systems Program is composed of six regional centers that share intelligence and coordinate efforts against crime and criminal networks operating in many locations across jurisdictional lines. Typical targets of Regional Information Sharing Systems activities are terrorism, drug trafficking, violent crime, cybercrime, gang activity, identity theft, human trafficking, and organized crime and criminal activities. Each of the centers, however, selects its own target crimes and the range of services provided to member agencies. Additional information on Regional Information Sharing Systems can be accessed on the Regional Information Sharing Systems Web site.

Glossary

This glossary lists acronyms and terms with Army or joint definitions.

SECTION I – ACRONYMS AND ABBREVIATIONS

ACI2	Army Criminal Investigative Information System
ADRP	Army doctrine reference publicaiton
AR	Army regulation
AT	antiterrorism
ATP	Army techniques publication
attn	attention
ATTP	Army tactics, techniques, and procedures
BOLO	be on the lookout
CCIR	commander's critical information requirement
CFR	Code of Federal Regulations
COPS	Centralized Operator's Police Suite
D3A	decide, detect, deliver, and assess
DA	Department of the Army
DC	District of Columbia
DCGS-A	Distributed Common Ground System–Army
DD	Department of Defense form
DHS	Department of Homeland Security
DNA	deoxyribonucleic acid
DOD	Department of Defense
DODD	Department of Defense directive
DODI	Department of Defense instruction
DOJ	Department of Justice
DSCA	defense support of civil authorities
ECTA	economic crime threat assessment
EO	executive order
FM	field manual
G-2	assistant chief of staff, intelligence
G-3	assistant chief of staff, operations
G-3/5/7	assistant chief of staff for operations, plans, and training
HUMINT	human intelligence
JP	joint publication
LSTA	Logistics security threat assessment
MO	Missouri
MSCoE	Maneuver Support Center of Excellence
No.	number

PIO	police intelligence operations
PIR	priority intelligence requirement
PMESII-PT	political, military, economic, social, information, infrustructure, physical environment, and time
POLICE	police and prison structures, organized criminal elements, legal systems, investigations and interviews, crime-conducive conditions, and enforcement gaps and mechanisms
S-2	battalion or brigade intelligence staff officer
S-3	battalion or brigade operations staff officer
SAR	suspicious activity report
SIPRNET	Secret Internet Protocol Router Network
SOFA	status-of-forces agreement
TC	training circular
U.S.	United States
USACIDC	United States Army Criminal Investigation Command
USC	United States Code

SECTION II – TERMS

None.

References

REQUIRED PUBLICATIONS

These documents must be available to the intended users of this publication.

ADRP 1-02. *Terms and Military Symbols*. 2 February 2015.

JP 1-02. *Department of Defense Dictionary of Military and Associated Terms.* 8 November 2010.

RELATED PUBLICATIONS

These documents contain relevant supplemental information.

ARMY

Most Army publications are available online at <www.apd.army.mil>.

ADP 5-0. *The Operations Process.* 17 May 2012.

ADRP 1. *The Army Profession.* 14 June 2013.

ADRP 2-0. *Intelligence.* 31 August 2012.

ADRP 5-0. *The Operations Process.* 17 May 2012.

ADRP 6-0. *Mission Command.* 17 May 2012.

AR 10-87. *Army Commands, Army Service Component Commands, and Direct Reporting Units.* 4 September 2007.

AR 25-55. *The Department of the Army Freedom of Information Act Program.* 1 November 1997.

AR 190-24. *Armed Forces Disciplinary Control Boards and Off-Installation Liaison and Operations.* 27 July 2006.

AR 190-30. *Military Police Investigations.* 1 November 2005.

AR 190-45. *Law Enforcement Reporting.* 30 March 2007.

AR 190-53. *Interception of Wire and Oral Communications for Law Enforcement Purposes.* 3 November 1986.

AR 190-58. *Personal Security.* 22 March 1989.

AR 195-2. *Criminal Investigation Activities.* 9 June 2014.

AR 380-10. *Foreign Disclosure and Contacts With Foreign Representatives.* 4 December 2013.

AR 380-13. *Acquisition and Storage of Information Concerning Non-affiliated Persons and Organizations.* 30 September 1974.

AR 381-10. *U.S. Army Intelligence Activities.* 3 May 2007.

AR 381-12. *Threat Awareness and Reporting Program.* 4 October 2010.

AR 525-13. *Antiterrorism.* 11 September 2008.

ATP 2-01.3. *Intelligence Preparation of the Battlefield/Battlespace.* 10 November 2014.

ATP 2-33.4. *Intelligence Analysis.* 18 August 2014.

ATP 3-34.80. *Geospatial Engineering.* 23 June 2014.

ATP 3-37.2. *Antiterrorism.* 3 June 2014.

ATP 3-39.10. *Police Operations.* 26 January 2015.

ATP 3.39.12. *Law Enforcement Investigations.* 19 August 2013.

ATP 3-39.32. *Physical Security.* 30 April 2014.

ATP 5-19. *Risk Management.* 14 April 2014.

ATTP 4-10. *Operational Contract Support Tactics, Techniques, and Procedures.* 20 June 2011.

FM 2-22.3. *Human Intelligence Collector Operations.* 6 September 2006.

FM 3-34.170. *Engineer Reconnaissance.* 25 March 2008.

FM 3-39. *Military Police Operations.* 26 August 2013.

FM 3-55. *Information Collection.* 3 May 2013.

FM 3-60. *The Targeting Process.* 26 November 2010.

FM 3-63. *Detainee Operations.* 28 April 2014.

FM 3-81. *Maneuver Enhancement Brigade.* 21 April 2014.

FM 6-0. *Commander and Staff Organization and Operations.* 5 May 2014.

FM 27-10. *The Law of Land Warfare.* 18 July 1956.

TC 2-22.82. *Biometrics-Enabled Intelligence.* 21 March 2011.

TC 2-91.8. *Document and Media Exploitation.* 8 June 2010.

DEPARTMENT OF DEFENSE

Most DOD publications are available online at <http://www.dtic.mil/whs/directives/>.

DODD 3025.18. *Defense Support of Civil Authorities (DSCA).* 29 December 2010.

DODD 5200.27. *Acquisition of Information Concerning Persons and Organizations Not Affiliated With the Department of Defense.* 7 January 1980.

DODD 5240.01. *DOD Intelligence Activities.* 27 August 2007.

DODI 2000.12. *DOD Antiterrorism (AT) Program.* 1 March 2012.

DODI 2000.16. *DOD Antiterrorism (AT) Standards.* 2 October 2006.

DODI 3025.21. *Defense Support of Civilian Law Enforcement Agencies.* 27 February 2013.

JOINT

Most joint publications are available online at <www.dtic.mil/doctrine/new_pubs/jointpub.htm>.

JP 2-0. *Joint Intelligence.* 22 October 2013.

JP 3-0. *Joint Operations.* 11 August 2011.

OTHER

5 USC 552. *Freedom of Information Act.* 4 July 1966. <http://uscode.house.gov/view.xhtml?req=(title:5 section:552 edition:prelim) OR (granuleid:USC-prelim-title5-section552) &f=treesort&edition=prelim&num=0&jumpTo=true>, accessed on 30 January 2015.

18 USC 1385. *Use of Army and Air Force as Posse Comitatus.* <http://uscode.house.gov/view.xhtml?req=(title:18 section:1385 edition:prelim) OR (granuleid:USC-prelim-title18-section1385)&f=treesort&edition=prelim&num=0&jumpTo=true>, accessed on 30 January 2015.

Bureau of Justice Assistance. *Intelligence-Led Policing: The New Intelligence Architecture*. September 2005. <https://www.ncjrs.gov/pdffiles1/bja/210681.pdf>, accessed on 30 January 2015.

Carter, David L., *Law Enforcement Intelligence: A Guide for State, Local, and Tribal Law Enforcement Agencies.* Michigan State University. November 2004. <http://www.cops.usdoj.gov/pdf/e09042536.pdf>, accessed on 30 January 2015.

Criminal Intelligence Sharing: A National Plan for Intelligence-Led Policing at the Local, State, and Federal Levels: Recommendations from the International Association of Chiefs of Police Intelligence Summit. August 2002. < http://ric-zai-inc.com/Publications/cops-w0418-pub.pdf>, accessed on 30 January 2015.

Department of Justice. *National Criminal Intelligence Sharing Plan.* Version 2.0. October 2013. <https://it.ojp.gov/gist/150/National-Criminal-Intelligence-Sharing-Plan-Version-2-0>, accessed on 30 January 2015.

DHS/DOJ. Global Justice Information Sharing Initiative. *DHS/DOJ Fusion Process: Technical Assistance Program and Services.* 8th Edition. October 2014. <https://www.ncirc.gov/documents/public/Fusion_Process_catalog_of_services_version_8.pdf>, accessed on 12 March 2015.

DOJ. Global Justice Information Sharing Initiative. *Findings and Recommendations of the Suspicious Activity Report (SAR) Support and Implementation Project.* October 2008. <http://nsi.ncirc.gov/documents/SAR_Report_January_2009.pdf?AspxAutoDetectCookieSupport=1>, accessed on 30 January 2015.

DOJ. Global Justice Information Sharing Initiative. *Fusion Center Guidelines: Developing and Sharing Information and Intelligence in a New Era.* August 2006. <http://it.ojp.gov/documents/fusion_center_executive_summary.pdf>, accessed on 30 January 2015.

DOJ. Global Justice Information Sharing Initiative. *Law Enforcement Analytic Standards*. April 2012. <https://it.ojp.gov/gist/91/Law-Enforcement-Analytic-Standards>, accessed on 30 January 2015.

DOJ. Global Justice Information Sharing Initiative. *Minimum Criminal Intelligence Training Standards for Law Enforcement and Other Criminal Justice Agencies in the United States: Findings and Recommendations.* October 2007. <https://it.ojp.gov/gist/108/Minimum-Criminal-Intelligence-Training-Standards>, accessed on 30 January 2015.

DOJ. Global Justice Information Sharing Initiative. *Privacy and Civil Liberties Policy Development Guide and Implementation Templates Overview.* February 2008. <https://it.ojp.gov/privacy206/>, accessed on 30 January 2015.

EO 12333. *United States Intelligence Activities.* 4 December 1981. <http://www.archives.gov/federal-register/codification/executive-order/12333.html>, accessed on 30 January 2015.

Federal Bureau of Investigation National Crime Information Center Operating Manual. December 1999. <http://chesapeakesheriff.com/Log%20in%20page/VCIN%20Manuals/NCIC-OP-MANUAL/NCIC_Operating_Manual.htm>, accessed on 11 March 2015.

National Disclosure Policy. <http://www.dod.mil/pubs/foi/homeland_defense/intelligence/371.pdf>, accessed on 30 January 2015.

National Strategy for Information Sharing: Successes and Challenges in Improving Terrorism-Related Information Sharing. October 2007. <http://nsi.ncirc.gov/documents/National_Strategy_for_Information_Sharing.pdf?AspxAutoDetectCookieSupport=1>, accessed on 30 January 2015.

PRESCRIBED FORMS

None.

REFERENCED FORMS

Unless otherwise indicated, DA forms are available on the Army Publishing Directorate Web site at <www.apd.army.mil>. DD forms are available on the Office of the Secretary of Defense Web site at <www.dtic.mil/whs/directives/infomgt/forms/formsprogram.htm>.

DA Form 2028. *Recommended Changes to Publications and Blank Forms.*

DD Form 1408. *Armed Forces Traffic Ticket* (Available through normal forms supply channels).

WEB SITES

Army Knowledge Online, Doctrine and Training Publications Web site, <https://armypubs.us.army.mil/doctrine/index.html>, accessed on 30 January 2015.

Army Publishing Directorate, Army Publishing Updates Web site, <http://www.apd.army.mil/AdminPubs/new_subscribe.asp>, accessed on 30 January 2015.

Department of Justice Web site. OneDOJ. <http://www.justice.gov>, accessed on 30 January 2015.

Federal Bureau of Investigations Web site. <http://www.fbi.gov/>, accessed on 30 January 2015.

Justice Information Sharing Web site. <http://it.ojp.gov/>, accessed on 30 January 2015.

Law Enforcement Information Sharing Program Web site. <http://www.ise.gov/law-enforcement-information-sharing> accessed on 30 January 2015.

National Crime Information Center database. <http://www.mass.gov/eopss/law-enforce-and-cj/cjis/national-crime-information-center-ncic.html>, accessed on 30 January 2015.

National Information Exchange Model Web site. <https://www.niem.gov/Pages/default.aspx>, accessed on 30 January 2015.

Regional Information Sharing Systems Web site. <http://www.riss.net/>, accessed on 30 January 2015.

RECOMMENDED READINGS

28 CFR 23. *Criminal Intelligence Systems Operating Policies.* 1998. <https://it.ojp.gov/documents/28CFR_Part_23.PDF>, accessed on 30 January 2015.

50 USC 3003. War and National Defense. <http://uscode.house.gov/view.xhtml?req=(title:50 section:3003 edition:prelim) OR (granuleid:USC-prelim-title50-section3003)&f=treesort&edition=prelim&num=0&jumpTo=true>, accessed on 30 January 2015.

ADP 1. *The Army.* 17 September 2012.

ADP 7-0. *Training Units and Developing Leaders.* 23 August 2012.

ADRP 3-0. *Unified Land Operations.* 16 May 2012.

ADRP 3-07. *Stability.* 31 August 2012.

ADRP 3-90. *Offense and Defense.* 31 August 2012.

ADRP 7-0. *Training Units and Developing Leaders.* 23 August 2012.

AR 195-6. *Department of the Army Polygraph Activities.* 29 September 1995.

ATP 2-22.4. *Technical Intelligence.* 4 November 2013.

ATP 3-57.30. *Civil Affairs Support to Nation Assistance.* 1 May 2014.

Gottlieb, Steven et al. *Crime Analysis: From First Report to Final Arrest.* Alpha Publishing. 1994.

The National Security Act of 1947. <http://www.state.gov/1997-2001-NOPDFS/about_state/history/intel/intro6.html>, accessed on 30 January 2015.

Index

Entries are by page number.

This page intentionally left blank.

ATP 3-39.20 (ATTP 3-39.20)
6 April 2015

By Order of the Secretary of the Army

RAYMOND T. ODIERNO
General, United States Army
Chief of Staff

Official:

GERALD B. O'KEEFE
Administrative Assistant to the
Secretary of the Army
1508202

DISTRIBUTION:
Active Army, Army National Guard, and United States Army Reserve: Distributed in electronic media only (EMO).

PIN: 105125–000