ATP 3-39.20

POLICE INTELLIGENCE OPERATIONS

MAY 2019

DISTRIBUTION RESTRICTION: Approved for public release; distribution is unlimited.

This publication supersedes ATP 3-39.20, 6 April 2015.

Headquarters, Department of the Army

This publication is available at the Army Publishing Directorate site
(<https://armypubs.army.mil>) and the Central Army Registry site
(<https://atiam.train.army.mil/catalog/dashboard>).

*ATP 3-39.20

Army Techniques Publication
No. 3-39.20

Headquarters
Department of the Army
Washington, DC, 13 May 2019

Police Intelligence Operations

Contents

DISTRIBUTION RESTRICTION: Approved for public release; distribution is unlimited.

*This publication supersedes ATP 3-39.20, 6 April 2015.

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 task that supports the operations process and protection supporting tasks across all phases of conflict by collecting and providing police information and police intelligence products to enhance situational understanding, protect the force, and assist homeland security across the operational environment. Military police and United States Army Criminal Investigation Command (USACIDC) personnel collect information as they conduct military police operations throughout the operational area. PIO supports decisive-action tasks (offensive, defensive, and stability or defense support of civil authorities [DSCA]) by planning and directing the collection, production, and dissemination of police information and police intelligence products that identify and analyze crime problems, environmental factors creating crime opportunities, and criminal actors that may affect the operational environment.

This publication is written for military police and USACIDC Soldiers and Civilians conducting PIO. This publication focuses on establishing the framework of PIO, guiding the conduct of PIO, and describing the integration of police intelligence products within the three military police disciplines (police operations, detention operations, and security and mobility support) in support of Army operations through the 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, international and, in some cases, host-nation laws and regulations. Commanders at all levels ensure that their Soldiers operate the law of war and the rules of engagement. (See FM 27-10.)

ATP 3-39.20 uses joint terms where applicable. Selected joint and Army terms and definitions appear in the glossary and text. For definitions shown in 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 the Active Army, Army National Guard/Army National Guard of the United States and United States Army Reserve unless otherwise stated.

This publication contains copyrighted material.

The proponent of ATP 3-39.20 is the United States Army Military Police School (USAMPS). The preparing agency is the Assistant Chief of Staff, (G-3)/Directorate of Training and Doctrine (DOTD), Maneuver Support Center of Excellence (MSCoE). Send comments and recommendations on DA Form 2028 (*Recommended Changes to Publications and Blank Forms*) to Commander, MSCoE, ATTN: ATZT-OPD-D, 14000 MSCoE Loop, Suite 270, Fort Leonard Wood, MO 65473-8929; by e-mail to <usarmy.leonardwood.mscoe.mbx.mpdoc@mail.mil>; or submit an electronic DA Form 2028.

Acknowledgements

The copyright owners listed here have granted permission to reproduce material from their works.

Crime and Everyday Life. Marcus Felson and Mary Eckert. The requestor is authorized to use the information from the *Crime and Everyday Life* (5th Edition, 2016) idea of the three stages of crime in chapter 1 of ATP 3-39.20, *Police Intelligence Operations*.

Integrated Intelligence and Crime Analysis: Enhanced Information Management for Law Enforcement Leaders Guide. Ratcliffe, Jerry H. The requestor is authorized to use the information from the *Integrated Intelligence and Crime Analysis: Enhanced Information Management for Law Enforcement Leaders* (2d Edition, August 2007) guide in chapters 1 and 4 of the revision of ATP 3-39.20, *Police Intelligence Operations.*

Introduction

Police intelligence has been included in U.S. Army military police doctrine since the 1960s. PIO focuses on the analysis of information to predict illegal, criminal, or subversive activities, and the environmental conditions that create opportunities for crime. This allows military police and supported commanders to anticipate, disrupt, and defeat criminal and other irregular threats.

In the complex world of today, criminal activity is not confined within national borders and is not solely an internal state concern. Belligerents of all types and scales (transnational criminal organizations, nonstate terrorist or insurgent networks, and revisionist nation-states) coalesce into organizations with similar or overlapping structures and characteristics; employ criminal tactics, techniques, and procedures; or affiliate with criminal organizations to threaten or harm the interests of the United States and its allies for different strategic goals, objectives, and motivations. Countering such hybrid threats requires capabilities that fill information and intelligence gaps across transregional geopolitical boundaries. Military intelligence remains a preeminent source of traditional intelligence production; however, restrictions on authority, limits to jurisdictional reach, and limited experience at investigating, interpreting, and controlling criminal behavior require commanders to have access to police intelligence capabilities that are dedicated to understanding the criminal aspects of the operational environment.

Fundamentally, PIO enhances situational understanding and informs decision making. PIO enables military police and supported commanders by improving situational awareness, contributing to understanding the operational environment, and providing police intelligence that allows commanders to make informed decisions on the criminal aspects of the operational environment. PIO provides timely, relevant, and accurate criminal intelligence and crime analysis products that identify crime patterns, trends, hotspots, environmental conditions, and problems that threaten the accomplishment of the commander's desired end state. In the end, the effectiveness of PIO, facilitates effective decision making aimed at preventing, mitigating, and reducing crime, the fear of crime, and disorder across the operational environment.

PIO provides unique technical skills and perspectives gained through experience in preventing, controlling, and investigating crime and criminal offenders. The law enforcement, corrections, and investigative skills that military police and USACIDC personnel employ daily while conducting military police operations make them a valuable asset for understanding crime environments, criminal activity, and criminal threats operating in increasingly complex operational environments. Military police leaders must be capable of articulating the value of PIO to supported commanders, and of producing police intelligence outcomes that contribute to mission success. The ability of PIO to fill knowledge gaps regarding crime, criminals, criminal networks, and organized criminal activity is a direct result of the capability and capacity of military police and USACIDC organizations to conduct PIO and leverage police intelligence to enhance situational understanding and decision making across the range of military operations.

Continuing the expansion of military police and USACIDC technical capabilities (including biometrics, forensics, crime analysis technology, and crime mapping software) has greatly enhanced the contributions of PIO to the Army and joint force globally. Such technical capabilities have greatly improved the commander's ability to identify, attribute, understand, and analyze criminals beyond the scope of traditional law enforcement and investigations on bases and base camps. Expeditionary solutions, such as the Defense Forensics Science Center forensics exploitation teams, continue to provide deployable forensic analysis capabilities that deny anonymity and impunity to criminal and terrorist threats. Additionally, forensics exploitation teams enhance the ability to investigate and prosecute criminals and irregular threat networks through the preservation and analysis of potential evidence for use in criminal prosecution. When consolidating gains, prosecution under the rule of law is critical to restoring a criminal justice system capable of providing peaceful conflict resolution and returning society to a sense of normalcy, which is an essential component of long-term stability and peace.

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

- **Chapter 1** describes crime and criminal threats that exist within complex operational environments, establishes the revised PIO framework, discusses roles and responsibilities, and describes how PIO contributes to unified land operations.
- **Chapter 2** introduces the first step in PIO of planning and directing information collection.
- **Chapter 3** provides detailed guidance for the collection of police information and its subsequent processing and reporting.
- **Chapter 4** describes the integrated criminal and crime analysis processes that produce police intelligence. This chapter discusses the critical thinking and predictive analysis techniques applied by trained police intelligence analysts to support understanding of crime and criminal activity.
- **Chapter 5** demonstrates how police intelligence products are disseminated to influence military police operations, support homeland operations, and support the Army operations process through the integrating processes. This chapter highlights the importance of collaboration and fusion with relevant stakeholders to ensure that police intelligence is delivered in a manner that supports decision making and produces desired outcomes.
- **Appendix A** addresses the applicable laws, regulations, and directives that are most relevant to PIO.
- **Appendix B** provides examples of different types of police intelligence products.
- **Appendix C** discusses employment considerations at various echelons to help practitioners operationalize PIO.

Throughout this publication, military police (31-series military occupational specialty) analysts are referred to as police intelligence analysts, while analysts assigned specifically to USACIDC organizations are often called investigative analysts due to their heavy focus on criminal intelligence support to the USACIDC investigative mission. Police intelligence analyst is an overarching term used to describe those analysts who have completed the Crime and Criminal Intelligence Analyst Course at the USAMPS and are assigned to military police organizations to perform criminal and crime analysis as part of PIO.

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

Chapter 1

Police Intelligence Foundations

FM 3-39 discusses the foundations of military police operations based on the three military police disciplines. PIO remains an integral part of conducting effective military police operations in its role as an integrated task. This chapter discusses the context for PIO in complex operational environments, provides a framework for military police forces conducting PIO, evaluates roles and responsibilities for PIO, and describes the contributions of PIO to the Army and unified action partners.

CRIME IN COMPLEX OPERATIONAL ENVIRONMENTS

1-1. An *operational environment* is a composite of the conditions, circumstances, and influences that affect the employment of capabilities and bear on the decisions of the commander (JP 3-0). Due to the complexity of operational environments, units often confront multiple threats across multiple domains simultaneously. The commander must understand how current and potential threats organize, equip, and employ forces, and how friendly elements are organized, equipped, and employed to defeat those threats. This is especially true of host-nation (HN) police and prison systems critical to countering criminal threats and supporting stability and order. When integrated into the operations process, PIO helps leaders and commanders understand criminal activity and how it facilitates crime, disorder, insurgency, terrorism, and instability. The understanding and insights gained by PIO help influence military police and Army operations designed to prevent crime, disrupt criminal activity, and reduce the fear of crime and disorder in complex operational environments.

Note. USACIDC and military police planners must integrate with each of the supported commands and interagency partners to effectively integrate PIO with the supported command targeting process. Typically, special operations forces and the Department of State have primacy and are the focus to prevent and shape operations during unified land operations. Conventional forces surge efforts during large-scale ground combat operations and the consolidation of gains. All of the aforementioned stakeholders may be active throughout the entire operation, but the unique capabilities of each are relied on at different times, depending on the desired effect.

1-2. Crime exists in every part of the world and in every society. There is no standard definition or categorization of crime because varying societies and governments possess different norms and laws that regulate human conduct. Crime is influenced by several factors. Understanding the core elements of crime allows police intelligence analysts to isolate relevant factors and evaluate the root causes of crime problems to produce a holistic understanding of crime and criminal activity.

1-3. Crime varies across operational environments based on the interplay of criminal offender motivations to commit crime, the presence of victims vulnerable to crime, and the environmental conditions that make a place conducive to crime, such as an exposed vulnerability and the absence of a capability to protect that vulnerability. Military police seek to understand these three basic elements of crime by using the crime triangle depicted in figure 1-1, page 1-2.

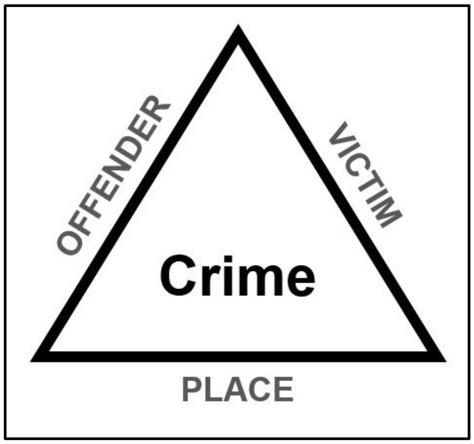


Figure 1-1. Crime triangle

1-4. Crime is a social phenomenon in which people are generally perpetrators and victims (whether directly or indirectly victimized). Understanding the characteristics of offenders and the methods of committing crime greatly enhances the ability of military police and USACIDC personnel to identify, investigate, apprehend, and control criminal offenders. Similarly, understanding the victims and targets of crime enables military police to reduce vulnerabilities, harden critical assets, and raise awareness of criminal threats through proactive crime prevention.

1-5. Crime is influenced by the perceptions of the people who decide to commit crime. First, people may make rational calculations and commit crime if they determine that the benefits of crime (such as financial rewards) outweigh the risks of being caught by police authorities. This type of criminal activity denotes a relative level of planning, preparation, and forethought. Second, people may commit crime regardless of the risks due to a desire for profit, social acceptance, recognition, or intimidation. People often commit crimes within criminal networks and organizations to gain status or generate fear that translates into greater power. More broadly, criminals may seek recognition or notoriety in the eyes of the public through crime (particularly heinous crime) based on a sense of grandeur or to intimidate populations. Third, people may commit unanticipated and relatively unplanned crime based on temptations and opportunities for crime presented during the course of their routine daily activities, including unplanned crimes of passion or aggression in reaction to decreased inhibitions or provocations.

Note. People who commit crimes are described by three common terms in this publication, depending on the specific meaning that is intended. Offender refers to a person who commits a specific criminal offense, whether or not they are detected, investigated, or convicted. Subject may be used when referring to a person who is suspected of committing a crime, whether or not they have actually committed it (see ATP 3-39.12 for details on law enforcement investigations of those suspected of committing crimes). Criminal is used in the broadest sense for persons engaged in ongoing criminal activities, with or without direct reference to a specific criminal act.

1-6. When a potential offender and victim converge in space and time, an opportunity exists for a crime to occur. However, crime does not occur in a vacuum. Crime occurs across time in three phases: before the crime, the crime (also called criminal incident), and the second- and third-order effects that occur as a result of the crime. Understanding crime as an isolated act and in relation to the conditions and actions that happen before and after a crime incident helps military police and USACIDC special agents understand the totality of a criminal act. This allows insights into the motivation and intent influencing an offender's decision to commit a crime and into the situational circumstances and conditions that created a crime opportunity. Figure 1-2 demonstrates the three stages of crime that, when combined together, are collectively described as criminal activity.

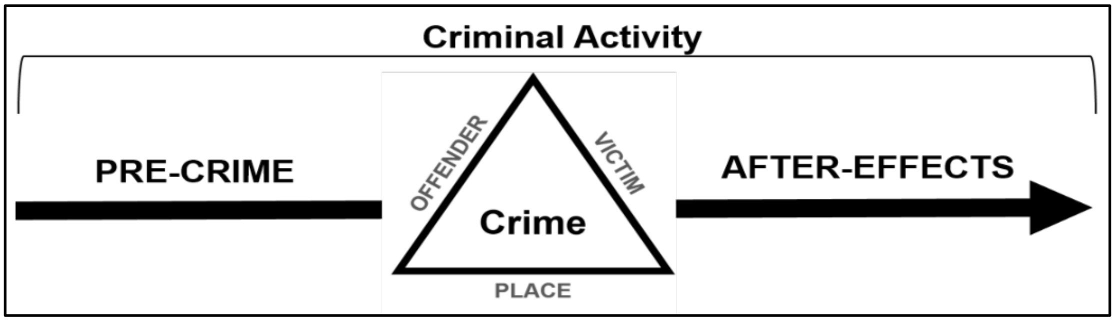


Figure 1-2. Crime and criminal activity across time

1-7. While each crime may be evaluated individually, criminals often engage in multiple crimes simultaneously, sequentially, or in coordination with other offenders. The relationship between people, places, and time produces identifiable patterns that police intelligence analysts evaluate. By approaching crime from an environmental perspective, police intelligence analysts seek to understand what motivates criminal offenders to choose to commit crimes, why crime occurs at some places or against some victims and not others, and what opportunities are generated that are conducive to crime. By understanding the setting and context in which criminal offenders make their decisions to engage in crime, military police, USACIDC personnel, and police intelligence analysts can better understand the motivations and intent that manifest themselves as criminal threats. Commanders and staffs use this analysis to prevent, deter, or better respond to criminal threats that may have an impact within an operational environment.

> ***Note.*** For this publication, the terms space and place are similar but are used in different contexts to refer to the spatial dimensions of crime. Space denotes a broader application, referring to a broad area without distinct boundaries, including virtual spaces such as cyberspace. Place refers to a specific location that may be analyzed based on specific geographic factors.

CRIMINAL THREATS

1-8. Criminals exist in all operational environments, but the level of threat that criminals pose to U.S. forces varies across time and space. A *threat* is any combination of actors, entities, or forces that have the capability and intent to harm U.S. forces, U.S. national interests, or the homeland (ADRP 3-0). Criminal threats are typically distinguishable from other threats in the motive for profit or power, as opposed to political, religious, or ideological motives. As such, criminals may be neutral, armed or unarmed noncombatants, or combatants based on their affiliation with other threats or their demonstrated capability and intention to harm U.S. interests. Criminals operate as individuals, networks, and organizations that vary based on size, level of concentration or dispersion, degree of hierarchy, scale of criminal activities, and relative power or influence.

Organization and Scale of Criminal Threats

1-9. Most crime is relatively small-scale, despite perceptions of crime as massive, organized pursuits. Typically, small-scale crime does not significantly threaten large-scale ground combat operations. Criminals are generally concerned with avoiding detection and disruption of their criminal activities so they can continue producing illicit profits. Small-scale crime, also referred to as street crime, is typically perpetrated by—

- Individual criminal offenders (repeat or one-time offenders).
- Co-offending networks (criminals conspiring to commit crime together).

1-10. While small-scale crime may not present a significant threat to large-scale ground combat operations, the cumulative impact of crime may threaten the ability to consolidate gains by creating perceptions of instability and undermining the legitimacy of a civil governing authority. Crime creates a sense of fear and disorder among populations and erodes the confidence and trust people have in the government and in the capabilities and capacities of security forces to provide security, order, and justice. Regardless of its accuracy to reality, the widespread fear of crime can undermine the sense of social cohesion and normalcy necessary for civil authorities to govern effectively. High volumes of crime, especially violent crime and corruption, contribute to narratives about government illegitimacy or incapacity and undermine friendly force ability to stabilize the operational environment and consolidate gains.

1-11. Beyond individuals and co-offenders, criminals often work on a broader basis in criminal networks and organizations that may span local, state, or regional boundaries. Criminal networks and organizations capable of large-scale crime may threaten civil order within states and across region, influence or corrupt political institutions, and challenge governance through paramilitary-like forces. Criminal organizations include—

- Gangs (local or networked street criminals).
- Large-scale criminal networks (networked individuals across multiple localities, states, or regions).
- Transnational criminal organizations (international cartels, paramilitary criminal organizations, mafia-style crime syndicates).

1-12. Assessing the presence, potential impacts, and possible affiliations of criminals within the operational area or area of operations is an integral aspect of joint intelligence preparation of the environment and intelligence preparation of the battlefield (IPB). (See ATP 2-01.3 and JP 2-01.3.) PIO contributes to these integrating processes by leveraging police knowledge, skills, and experience in identifying, investigating, and controlling criminal populations. The deliberate focus of PIO on criminal activity assists military intelligence activities by identifying criminal elements that may combine into hybrid threats.

Hybrid Threats

1-13. When criminal elements combine with other threat forces, a hybrid threat is established. A *hybrid threat* is the diverse and dynamic combination of regular forces, irregular forces, terrorist forces, or criminal elements unified to achieve mutually benefitting threat effects (ADRP 3-0). Hybrid threats combine traditional forces governed by law, military tradition, and custom with unregulated forces that act with no restrictions on violence or target selection. These may involve nation-state actors, possibly using proxy forces to coerce and intimidate, or nonstate actors (such as criminal and terrorist organizations) that employ protracted forms of warfare using operational concepts and high-end capabilities traditionally associated with states. Such varied forces and capabilities enable hybrid threats to capitalize on perceived vulnerabilities, making them particularly effective. Hybrid threats exist across multiple operational environments and reveal the multiplicity of actors involved and the increasing complexity blurring traditional elements of conflict. This often results in the ambiguity or anonymity for threat actors that prevents the identification and defeat of threats through traditional methods alone. See TC 7-100 for additional information of hybrid threats.

1-14. A hybrid threat is a composite of different threat forces working toward a common goal. The simple existence of many diverse threats in an operational environment does not automatically comprise a hybrid threat. To be considered a threat, an actor (criminal or otherwise) must have the capability and intent to challenge the United States or its partners. Two or more threat forces possessing such capability and intention must cooperate or coordinate threat effects toward a common objective to be considered a hybrid threat. Working together often results in affiliation, which is when two organizations cooperate toward a common goal despite having no formal command or organizational relationship. Any two or more of the following forces working in affiliation may constitute a hybrid threat:

- Regular or traditional military forces (uniformed nation-state military).
- Nation-state controlled paramilitary forces (internal security forces, police, or border guards).
- Irregular military forces (insurgent groups, guerilla units, or nonstate paramilitary forces).
- Criminal organizations (gangs, drug cartels, trafficking or hacker networks).

1-15. Criminals may affiliate with nation-state or nonstate actors when interests coincide. These shared interests may include shared cultural identities and values; common religious or ideological beliefs; financial incentives or the potential for profit; or the potential to increase power, prestige, and influence over rivals or governing authorities. When interests naturally coincide, uncoordinated criminal activity may appear to support adversary narratives or objectives without actual coordination or agreement. When criminals do cooperate with external forces, they may act in unison toward common goals or follow the deliberate plans and directives of a nation-state or nonstate actor to help them achieve their tactical, operational, or strategic objectives. Criminals may contribute to other forces by—

- Providing financial means and financial networks for nonstate or terrorist actors.
- Providing information, intelligence, or reconnaissance from their location within local societies.
- Influencing local politicians through bribery or extortion using violence or the threat of violence.
- Influencing local populations by professing allegiance or ideological affiliation to advance external actor narratives.
- Providing a proxy force for nation-state or nonstate actors to achieve political or military objectives without deploying identifiable or attributable forces.

1-16. Nation-states seeking political or military gains without detection or attribution may seek criminals to serve their purpose. In such cases, criminals carry out actions according to the direction or interests of an external nation-state as a result of promises or assurances of increased wealth and power or based on common identities and values that cause interests to coincide. The use of criminals as a proxy force to achieve a nation-state creates ambiguity, prevents attribution, and allows a nation-state to pursue its objectives covertly to avoid international sanction or military action. Nation-states may employ covert forms of regular military forces and/or special-purpose forces to coordinate and direct local criminals. This type of hybrid threat tactic was effectively employed by Russia during conflicts in Georgia in 2008 and the Ukraine in 2014.

1-17. Nonstate actors may also seek to gain the assistance of criminals—or resort to criminal activity themselves—to finance or equip their operations. Several terrorist networks threaten transregional security and order in the Middle East, North Africa, and beyond through coordination with and co-opting of local criminal elements. While such groups are focused on achieving the political objectives of advancing their ideology, these networks often overlap with and mimic criminal networks operating across the same regions. Both participate in illicit activities, leverage corruption to achieve their ends, and use similar criminal methods and violence that undermine regional security and stability.

Threat Network Overlap

1-18. In complex operational environments, the distinction between criminal and terrorist threats is blurred due to the employment of similar methods, overlapping individuals and networks, and converging interests—often called the crime-terror nexus. PIO addresses challenges associated with the crime-terror nexus by providing commanders with technical police capabilities, knowledge, and experience to analyze and understand criminal behaviors and activities and the relevant factors within the operational environment that promote opportunities for crime. Terrorist groups, insurgents, and other belligerents often use or mimic the methods, organizational structure, and activities associated with criminal networks to move contraband, raise funds, or achieve their objectives through indirect means (see ATP 5-0.6 for additional information on threat networks). PIO focuses on identifying the linkages between criminals and other irregular forces to enable commanders and staffs to better understand and act in complex environments.

1-19. Even when not united or working toward common goals, threat networks may appear to be working together due to the use of similar illicit methods that collectively undermine civil governance or disrupt U.S. military efforts. The use of similar methods makes identifying criminal activity versus identifying activity that is political in nature increasingly difficult. Often, networks (criminal or terrorist) use the same criminal infrastructure and illicit means to achieve different operational or strategic purposes. While criminals typically focus on material ends, terrorist and insurgent networks may use criminal methods to acquire or generate the resources needed to achieve their ideological ends. When criminal organizations move beyond financial motives to pursue political objectives or when terrorist organizations sacrifice aspects of their ideology in the pursuit of material gains, the distinction between the two is greatly obscured. Table 1-1, page 1-6, shows potential criminal or terrorist/insurgent ends served by the use of similar criminal methods or tactics and the common effects that such methods may have on military forces or civil governing authorities. See TC 7-100 for additional information on criminal methods.

Table 1-1. Criminal methods and tactics

Method/Tactic	*Effects*	*Criminal Ends*	*Terrorist/Insurgent Ends*
Theft Taking another person's property without that person's permission or consent with the intent to deprive the rightful owner of it, or— **Fraud** Intentional deception made for personal gain and/or to damage another individual or entity	**Military:** • Undermine military readiness • Allow threats access to stolen material or information • Increase the cost of military operations **Civil:** • Undermine formal economy by generating illicit markets • Create grievances in population to fuel civil conflict • Deprive government of critical resources or material • Rampant/publicized fraud may increase the general distrust of institutions	• Produce illicit profits and personal wealth • Increase status or stature among criminal associates • Financial means to fund criminal organizations • Financial means to corrupt or bribe political or police authorities • Deny competitors competitive advantage • Undermine economic oversight or control that threatens criminal organization interests	• Financial means to carry out terrorist operations • Disrupt/deny material resources of military/civil authority • Undermine government legitimacy and economic stability by producing black markets to sell stolen goods • Create perceptions of economic instability and disorder that enhances terrorist narratives • Attack military force morale by entrapping individual Soldiers • Expose corruption in military or civil humanitarian or reconstruction efforts
Bribery Giving money or other favors to influence someone, or— **Extortion** Obtaining money, material, information, or support by force or intimidation	**Military:** • Undermine readiness by reducing available funds for military operations • Compromise classified information by gaining leverage over military personnel **Civil:** • Undermine governance capability and capacity • Undermine legitimacy by corrupting people and institutions responsible to the public interest • Intimidate population, governing authorities, or other entities posing a potential threat to organizations	• Influence decisions by political, police, or judicial authorities to prevent disruption to criminal enterprise • Produce financial gains for personal wealth and status • Entrap military or civil personnel to gain leverage to blackmail personnel if they threaten criminal interests • Control populations for the interests of criminal organization	• Influence politicians, police, or military officials to prevent disruption of terrorist activities • Cause fear in population to force the population to support terrorist organization or interest • Prevent population from supporting government or sharing information about the organization • Gain leverage over personnel in crucial civil and military positions to achieve impunity

Table 1-1. Criminal methods and tactics (continued)

Method/Tactic	*Effects*	*Criminal Ends*	*Terrorist/Insurgent Ends*
Hijacking Stealing or commandeering a conveyance, or— **Kidnapping** Abduction or transportation of a person or group by force, or— **Hostage taking** Overt seizure of a person or persons to gain publicity, concessions, or ransom	**Military:** • Disrupt military operations or logistics systems to degrade combat power • Seize important military personnel • Undermine military narratives or perception in the ability to protect populations **Civil:** • Undermine perceptions of civil authority capability and capacity to protect its population • Produce high-profile hostage events that bring media attention to the organization's capability, cause, or narrative	• Profit or gain local power among rivals from the possession of hijacked military equipment • Produce personal profits through ransoms • Gain status or notoriety among criminal competitors • Obtain leverage to ease pressure on criminal activities • Obtain means of escape or attempt to trade kidnapped personnel for imprisoned criminal affiliates	• Employ hijacked conveyance as a weapon of mass destruction • Enhance the narrative of the organization or ideology • Gain media attention for an ideological or political cause • Disrupt global supply lines transporting military supplies into active operational areas • Generate ransoms for financing terrorist operations • Gain leverage over political rivals and undermine civil authorities legitimacy • Spread fear among the population to showcase the ability to use violence to enforce its vision of society or order
Murder Unlawful killing of another human being without justification or excuse, or— **Maiming** Deliberate act to mutilate, disfigure, or severely wound a person so as to cause lasting damage, or— **Assassination** Murder (usually of a prominent person) by a sudden and/or secret attack	**Military:** • Disrupt military operations or harm U.S. personnel • Defeat stability activities and the consolidation of gains by spreading violence and disorder • Defeat support for U.S. operations among a population or public opinion **Civil:** • Undermine legitimacy of civil authority by showing inability to control the means of violence • Punish people or enforce will on people; produce fear in a population • Eliminate prominent social, political, or military figures threatening the organization	• Punish internal dissidence • Eliminate criminal rivals • Gain power or prestige • Generate revenue through murder-for-hire schemes • Profit by contract killing • Eliminate political leaders or police who threaten criminal enterprise • Leverage fears of violence to extort populations by offering protection in exchange for loyalty to the criminal organization	• Eliminate political opponents, internal betrayals, or noncompliant populations • Highlight the inability of governing authority to protect its own people • Undermine the credibility of civil authority's ability to maintain peace and order • Cause fear and anxiety among population to increase the incentives to make a deal or accept terrorist organization as legitimate actor in local governance • Control political decision making through fear of retaliation

Table 1-1. Criminal methods and tactics (continued)

Method/Tactic	*Effects*	*Criminal Ends*	*Terrorist/Insurgent Ends*
Smuggling Clandestine transportation of illegal goods or persons –or– **Trafficking** Transportation of goods or persons for the purpose of making a profit-includes drug, arms, and human trafficking	**Military:** • Provide illegal arms and supplies to enemy threats • Support operations against U.S. forces from sanctuaries • Undermine international standards, norms, borders **Civil:** • Undermine civil authority ability to control its economy • Illegally move goods across international borders • Facilitate illegal migrations that undermine sovereign authority of the state	• Profit from illicit trade, smuggling, or trafficking • Gain access to illegal arms to exert power and influence over rival criminals or local populations • Facilitate transnational criminal networks such as drug trafficking networks • Gain leverage over vulnerable populations to force them to perform activities or supply labor for the criminal organization • Facilitate black markets while avoiding detection or seizure of illicit goods	• Provide financial means to conduct terrorist attacks • Provide arms and other illegal supplies to facilitate terrorist operations • Infiltrate migrant movements into Western societies to conduct attacks • Provide weapons, supplies, or money to proxies from isolated sanctuaries • Gain control over vulnerable populations to impose ideology or political order
Cyberspace crimes Offenses targeting or using information technology	**Military:** • Threaten the integrity and security of the DODIN • Disrupt operations by degrading military systems and digital infrastructure • Access information to determine friendly intention, disposition, vulnerabilities **Civil:** • Steal information from civilian populations • Undermine the ability of civil or business entities to protect people's information • Disrupt infrastructure or systems related to civil society or the economy	• Steal information or infiltrate networks for personal or financial gains • Facilitate other criminal activities like money laundering, extortion, fraud, or trafficking • Gain anonymity or impunity to conduct criminal activities • Disrupt efforts to control, target, or destroy the criminal organization	• Deny or disrupt military systems targeting the organization • Attack government or commercial networks to achieve political purposes • Undermine the confidence the population has in civil authority or private businesses • Create fear and anxiety in the population to advance terrorist ideology or narrative • Connect, communicate, and inspire dispersed followers to commit terrorist acts • Spread the terrorist narrative or message through digital means
Legend: DODIN Department of Defense information network U.S. United States			

1-20. Humans are members of multiple networks based on the diversity of individual identities and multiple types of social roles, connections, and relationships. People may simultaneously identify with and participate in threat, neutral, and friendly networks that comprise their daily social interactions. Examples of possible networks of people include insurgent, terrorist, criminal, social, political, professional, familial, tribal, religious, ethnic, or demographic. Criminal networks often leverage their connections within legal networks to achieve their illegal purposes. This allows criminals to mask illicit activities behind the appearance of legitimate enterprises to protect their criminal activity from detection, disruption, or interdiction. Given the abundance of human networks within a society, the challenge for commanders and staffs is to discover which networks pose a threat and identify the critical people who overlap between threat networks. These individuals typically serve as the critical nodes of power, influence, or importance who empower the network's critical capabilities and functions. Figure 1-3 shows the different connections with criminal and terrorist networks that an individual may possess given different identities and affiliations.

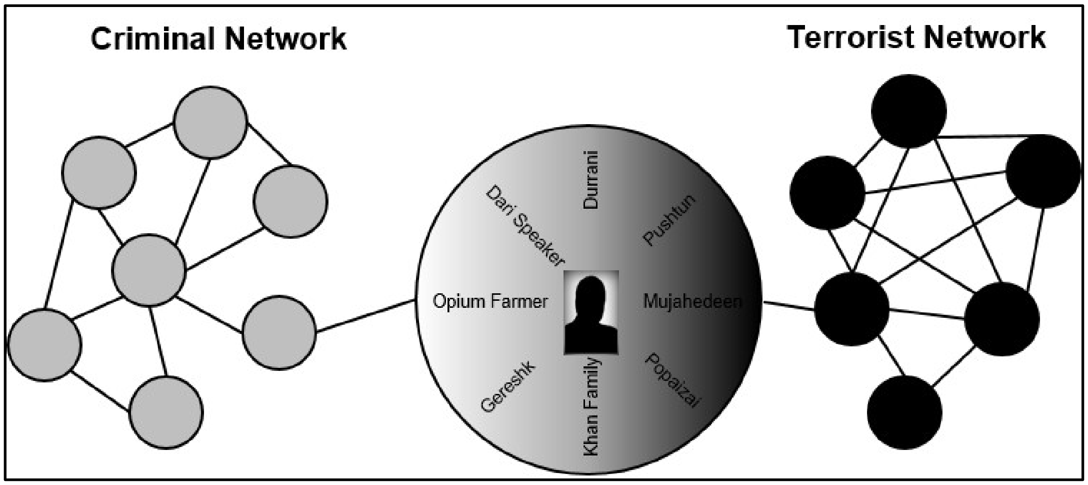


Figure 1-3. Individuals with multiple identities and affiliations

1-21. Threat networks converge at critical nodes (people, places, and things) that facilitate the essential functions necessary to achieve their purposes. In complex operational environments, terrorist and criminal networks often converge because of their reliance on overlapping individuals to perform their tasks and functions. Overlap may include using the same personnel for technical or functional tasks, such as logistics, finances, or weapons procurement. Terrorist and criminal networks depend on weak governance and an absence of police presence to allow their networks to operate and flourish. Threat networks often leverage neutral or friendly networks, such as legitimate businesses or social networks, to conceal their illicit activities, blur the lines between combatants and noncombatants, and frustrate U.S. military and partner-nation actions to counter threat networks. See JP 3-25 for additional information on countering threat networks.

1-22. Sometimes threat networks overlap so extensively with criminal or other networks that they defy ease classification into clearly defined categories. In some cases, threat networks may appear to be a terrorist network; in other cases, a criminal network; and in other cases, a neutral network providing social services to a population through legitimate means. Such multifaceted networks often contain individuals who are affiliated with the network for different motivations, each possessing different levels of connection to the network. Individual low-level actors may support a network solely for criminal or ideological motivations or for both. Likewise, mid-level cadre may specialize or oversee criminal or terrorist cells in the organization or coordinate activities across organizations. Top leadership seeks to use any combination of means that help them achieve their goals. Figure 1-4 provides an example of threat network convergence.

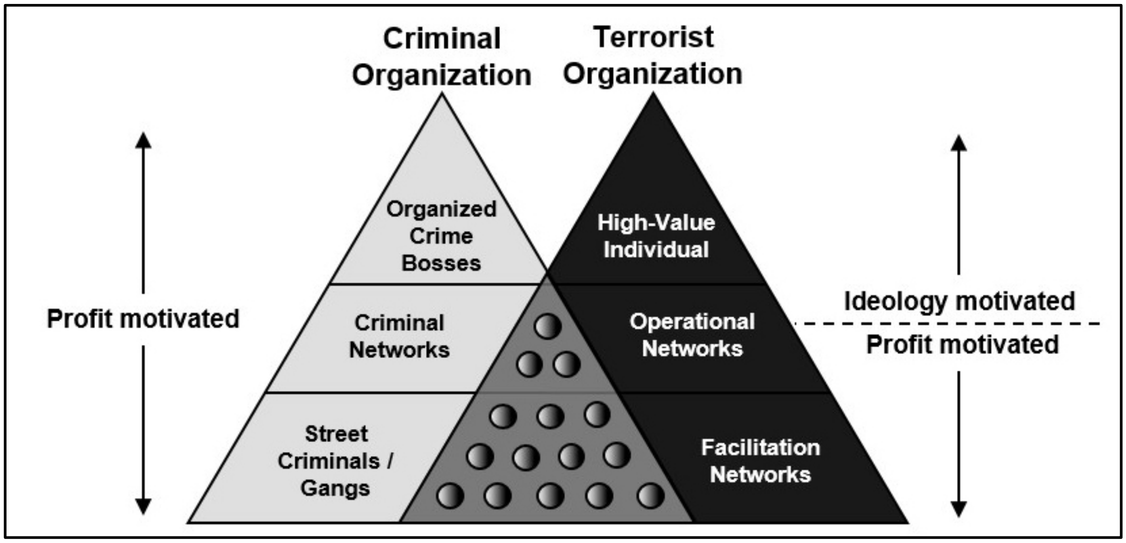


Figure 1-4. Threat network convergence

Threat Diffusion

1-23. In addition to threat overlap, criminal threats increasingly possess the capability and capacity to operate across multiple domains. Threat diffusion across multiple domains means that threats do not only operate solely in one domain or another, but they may also operate in or threaten multiple domains simultaneously. Examples of criminal activities that cross multiple domains requiring information sharing and collaboration among unified action partners include—

- Smuggling (illegal goods or services) or trafficking (drugs, humans, arms) across the land, air, and maritime domains from production bases to markets and consumers.
- Hijacking and hostage-taking carried out from sanctuaries in the land domain against vulnerable targets in sea or air domains.
- Criminal interdiction and theft of military equipment transiting global logistics supply lines in transit to and from the home station and theater via land, air, and maritime domains.
- Cyberspace crimes committed through land-based information network connections for the conduct of financial crimes (money laundering, identify theft, fraud) or for more nefarious purposes related to national security, such as cyberspace espionage and cyberspace attacks.

1-24. Criminal activity across multiple domains presents significant challenges to identifying, attributing, and countering criminal threats. Criminal activity that crosses through or impacts other domains typically emanates from the land domain and requires a land-based police and investigative capability and capacity to identify, monitor, and apprehend criminal subjects for investigation and prosecution.

1-25. In the cyberspace domain, threats may initially be identified, reported, and investigated as criminal acts. In such instances, a criminal investigation (typically conducted by the USACIDC Computer Crimes Investigation Unit) may reveal connections to broader threat networks that threaten operational missions or national security. The domain linkages of criminal and other threats require proficient, timely, and legally sound information and intelligence sharing. PIO supports this by leveraging established information-sharing networks that enable criminal intelligence to be shared with relevant stakeholders according to the restrictions and limitations established by U.S. law and policy. Police intelligence networks that exist before crimes occur are crucial to identifying the complex overlap of hybrid threats that do not organize along clearly distinguishable force categories or domain boundaries. Cyberspace crimes that may reveal connections to broader criminal or irregular threat networks may include—

- Extortion, theft, or fraud facilitated by phishing, spearphishing, or whaling attacks used to gain information, blackmail, or compromise Soldiers or Civilians supporting U.S. forces.
- Financial crimes (money laundering, racketeering, fraud) that reveal connections to terrorist or irregular threat finance networks.
- Child pornography investigations by digital forensics examiners that may provide connections or information related to human trafficking networks.
- Cyberspace intrusions that result in the theft of personally identifiable information to enable identity fraud, sensitive or classified information for national security crimes (such as espionage or sabotage), or technological trade secrets that enhance the proliferation of military-related technology to adversary nation-state and nonstate actors.

1-26. Although hybrid threats pose a significant threat when they are unified, their destruction and disintegration does not eliminate the threat that they pose. As military forces successfully destroy hybrid threat capabilities and linkages, criminal elements will likely not be eliminated completely and criminal activity may even accelerate. Hybrid threats use their organizational structure to control and direct the use of criminal activity for distinct political or ideological purposes; however, the destruction of that structure is often replaced by a multitude of uncontrolled and decentralized criminal actors. In such disintegration, criminality is likely to increase, although in a less centralized manner and through smaller and more loosely associated networks. There are several examples of an increase in criminality and proliferation of crime following the defeat or deterioration of a nation-state, nonstate actors, or criminal organizations that may be components of hybrid threats. Examples include—

- **Nation-state collapse or defeat.** When a nation-state is defeated or collapses, there is often an immediate power vacuum that may destabilize society and undermine civil order. This results in an atmosphere that is conducive to widespread crime because of the general absence of legitimate and capable law enforcement, security, and justice institutions. This occurred in 2003 following the rapid military defeat of Saddam Hussein's Ba'athist regime in Iraq, which was followed by a power vacuum that presented widespread opportunities for crime. The result was rampant looting and other spontaneous criminal activity that significantly undermined the transition from large-scale ground combat operations to stability and order.
- **Centralized to decentralized networks.** Terrorist organizations may also display a trend toward decentralization and dispersion following the defeat of centrally organized structures. Al Qaeda gained notoriety as the preeminent global terrorist organization following the attacks on the World Trade Center and the Pentagon on September 11, 2001. Since that time, U.S. military operations have degraded the capability, capacity, and effectiveness of Al Qaeda but have not succeeded in destroying the threat of violent extremist organizations fueled by radical ideologies. As Al Qaeda's organized structure was degraded in the decade following 2001, decentralized branches evolved independently into more dispersed networks, such as the evolution of Al Qaeda in Iraq into the Islamic State in Iraq and Syria, who eventually vied for the allegiance of radical Islamists around the world.
- **Drug cartel proliferation.** Counterdrug operations in the late 1980s led to success in countering Colombian drug cartels using Caribbean networks to smuggle cocaine but did not end drug trafficking into the United States. Rather, success was largely offset by the rise of Mexican drug cartels. Efforts in the last decade to counter large-scale drug cartels have likewise been successful in countering such criminal organizations as *Sinaloa* and capturing its chief kingpin, Joaquin (El Chapo) Guzman. Rather than decreasing drug trafficking, this has resulted in a further diffusion from large-scale centralized networks to dozens of small- to medium-scale drug trafficking networks, leading to a proliferation of crime, increases in unconstrained coercive violence, and rampant corruption of local governing institutions.

1-27. As hybrid threats face defeat, criminal elements generally disperse within the population. The diversity and density of the population provides criminals the concealment necessary to resume the pursuit of purely criminal endeavors without being defeated in conjunction with other hybrid threat forces. This diffusion into the population may result in more loosely coordinated actions between hybrid threat components or the complete severing of affiliation and cooperation. When hybrid threats disintegrate and disperse into the local population, the ability of U.S. forces and unified action partners to understand, target, and defeat those persistent threats is significantly degraded despite success on the military battlefield.

1-28. Hybrid threats facing imminent defeat no longer possess an interest in maintaining social cohesion, order, and control; they may release masses of incarcerated prisoners to create further chaos, disorder, and dispersion of criminal threats within the population to undermine U.S. efforts to stabilize society and consolidate gains. The problem of criminal dispersion into populations following hybrid threat disintegration is greatly increased given the trend toward urbanization of the world population into complex, densely populated urban environments.

Complex Urban Environments

1-29. Over 50 percent of the world population currently lives in urban areas; therefore, complex urban environments have become a critical aspect in understanding contemporary operational environments. In 2014, the United Nations *World Urbanization Prospects* identified 28 cities as megacities, which are defined as cities with ten million inhabitants or more. By 2030, the world is projected to possess 41 megacities, and the population levels within those cities are projected to continue increasing.

1-30. Because crime is a human and social phenomenon, the increasing concentration of people in large and complex urban environments and the increased pace of human interactions naturally increase the potential for crime and other destabilizing events when conditions become conducive to crime. For example, crime opportunities abound when guardianship and enforcement mechanisms are absent or lack sufficient capacity.

While the concentration of people does not automatically signal increased crime relative to population size, several aspects of complex urban environments bear on the decisions of criminals and should be considered during criminal and crime analysis. See TC 2-91.4 for military intelligence techniques and considerations in urban environments.

Complex Urban Terrain

1-31. Because the diversity of people, places, patterns, and problems exists within cities, complex urban terrain increases the importance of understanding the environmental aspects of crime. No two cities are the same, regardless of common cultural, national, or political traits. This means that while trends and commonalities may be understood across an area of operations, understanding crime in an urban area requires deliberate criminal and crime analysis to determine the specific crimes prevalent in the area, where crime is occurring, why it is occurring in those places, who is committing crime, what crime patterns exist, and what underlying problems can be deduced to guide effective prevention and response efforts that allow the commander to solve the right problems, in the right places, against the right people.

1-32. The complexity of urban terrain and the pace of urban life often result in an abundance of information. The central challenge is to correctly identify the root problems and active criminal threats hidden amidst the overwhelming amount of information. In complex urban terrain, given the proximity and density of the population, the local population often possesses information critical to identifying and countering criminal threats. The challenge becomes how to collect and obtain information the population knows about criminals and other irregular threats present in the area. This type of collection depends on the population’s trust and confidence in the capability, capacity, and legitimacy of U.S. or partner-nation police and security forces. Military police constantly interact with and build rapport with populations during routine policing. The information gained through police engagement with populations is critical in identifying the most essential information regarding crime, criminals, and conditions contributing to crime.

1-33. Urban areas accelerate the frequency of human interaction and multiply the patterns of human activity. Crime reflects, and is integrally linked to, other forms of human activity. It follows the same routes, patterns, and social concentrations as other patterns of life. The increased patterns of human activity generated by rapid urbanization and dense concentrations of people greatly expand opportunities for crime. Increased interactions among people raise the potential for conflict between individuals and introduce more occasions for potential offenders and victims to converge at places. Social problems associated with urban life expand the sources of potential crime problems.

Operations Among Dense Urban Populations

1-34. Sustained land operations are inherently operations among populations. Within urban environments, operations take place among dense populations. The complexity of urban terrain and the density of populations significantly restrict freedom of movement, action, mobility and firepower advantages. The restrictions placed on Army forces operating among dense urban populations allow weaker adversaries and enemies to negate Army advantages while empowering asymmetrical or irregular tactics.

1-35. The ability to decentralize, empower small unit leadership, and interact with diverse populations requires unique skills and attributes that military police develop in the course of daily law enforcement and policing. Military police excel in gathering information while engaging with populations due to their ability to establish trust and rapport with communities; focus on providing safe, secure, and stable environments; and gain voluntary compliance to the law using the minimum necessary use of force. See ATP 3-55.4 for discussion regarding information collection during operations among populations.

1-36. Large-scale ground combat operations may dramatically increase the level of crime in an urban area due to the disruption of the local economy, loss of jobs, and increased demand for money-making enterprises to make up for lost income, destroyed infrastructure, or disrupted economy. The greater the divide between opportunities for legal commerce and business and the greater the demand for work, the greater the incentive for illicit activity to supplement or provide basic survival income.

1-37. Criminals may depend on populations for support or cooperation or require the absence of informal social control within a population that can interfere with or disrupt criminal activities. This support may result from coercive violence that intimidates a population into cooperating, or it may be gained by providing the population with essential social, economic, or security services that the government is incapable or unwilling to provide. Informal social patronage and economic welfare systems often challenge formal governing authorities responsible for providing such services and may undermine U.S. efforts to stabilize environments and enable civil authority.

1-38. Consolidating gains is not a quick process and may require sustained effort and engagement with populations over a significant period of time. As U.S. forces transition from large-scale ground combat operations to the consolidation of gains, emphasis shifts from actions to defeat conventional threat forces to stability tasks that address the needs of urban populations, manage public perceptions, and transition responsibility from U.S. forces to the HN or other organizations.

1-39. This period of transition often increases risk. Crimes generally increase in unstable and transitional environments as criminals seize opportunities to commit crimes due to limited or unclear governance authority and gaps in civil security and civil order. Commanders and staffs should anticipate increased crime and criminal activity during transitions and ensure that planning efforts focus on the security, stability, and enforcement mechanisms necessary to ensure a smooth transition from large-scale ground combat to the consolidation of gains.

Ubiquitous Media Coverage

1-40. Although the development of strong, independent local media is not a primary responsibility of the military, it is a critical aspect of the information environment that can impact perceptions of the legitimacy and competence of public institutions. A free, responsible, and robust media is an important component of participation and can mitigate the sense of grievance within a population that may cause people to seek alternate means of justice from nonstate criminal or insurgent organizations. The media can be an important accountability mechanism for the government, helping to maintain the rule of law and support effective governance. By providing communications about public and government activities, the media can encourage civic participation, give citizens a sense of empowerment, and undermine threat narratives. The media plays an important role in building a stable social and political order.

1-41. Media coverage can also have an adverse impact on society. Criminals capitalize on disorder, fear, and instability. In densely populated urban terrain, ubiquitous international media may contribute to perceptions of disorder and fear when coverage overwhelmingly focuses on violence, disorder, and destabilizing events. Within a population, fear often increases the opportunities from which criminals can benefit. When populations fear for their security or property and believe the government is incapable or unwilling to protect them, they may turn to criminal organizations for protection in exchange for money, allegiance, or support. Given these conditions, criminals may exploit such opportunities to extort the population by contributing to and perpetuating the sense of fear, instability, and violence so that people continue to seek their protection. This cycle of violence and crime is most prevalent in areas lacking effective governance.

GOVERNANCE CHALLENGES

1-42. *Governance* is the state's ability to serve the citizens through the rules, processes, and behavior by which interests are articulated, resources are managed, and power is exercised in a society (JP 3-24). Instability undermines governance and contributes to security environments that may necessitate military operations or assistance. Crime and criminal threats may contribute to instability by weakening governance; replacing legitimate government structures with those of a criminal organization; or corrupting political, judicial, or police institutions. The effects of instability within states and across regions undermine the ability of stable states to govern effectively and participate peacefully with other states.

1-43. Stable states are those states capable of—

- Protecting their populations from external and internal threats (for example, providing civil security) through a monopoly on the legitimate use of violence.
- Upholding civil order and rule of law through legal frameworks, public order, accountability to the law, and access to justice.
- Governing according to the rule of law by peacefully resolving political differences and settling political grievances through dispute resolution institutions (court of law).

- Promoting infrastructure and economic development.
- Maintaining legitimacy in the eyes of the population and the international community.

Weak, Absent, or Alternative Governance

1-44. The ability of society to achieve civil order and stability is largely reflective of the capability, capacity, and willingness of civil authorities to prevent, mitigate, and reduce crime and disorder. Weak governance occurs when governing institutions and structures are incapable of enforcing civil authority. Weak, absent, or alternative governance provides sanctuary for criminals. Sanctuary is a method that puts threat forces beyond the reach of friendly forces. It is a form of protection derived from a combination of political, legal, and physical boundaries that restrict freedom of action by a friendly force commander. Criminal threats may achieve sanctuary through the deliberate construction of protected space (for example, based on the threat capability) or through the absence of effective government and police institutions capable of enforcing laws and maintaining civil order. States with weak, absent, or alternative governance are often unable to fulfill the basic functions and responsibilities associated with stable states.

Weak Governance

1-45. A fragile state suffers from institutional weaknesses serious enough to threaten the stability of its central government. Fragile states include failing states, failed states, and recovering states. A failed state may only have remnants of a government due to collapse or regime change or it may have a government that exerts weak governance in all or large portions of its territory (ungoverned areas). A failing state is still viable, but it has a reduced capability and capacity to protect and govern the population. A recovering state is moving toward normalcy, but it may have an imperfect level of viability. States within the fragile state framework are susceptible to significant criminal activity due to the limited capacity of government and law enforcement institutions. In such conditions, criminals often contribute significantly to disorder that perpetuates instability to prevent disruption to their illicit activities. See ADRP 3-07 and JP 3-07 for additional information on the fragile state framework.

1-46. Weak governance in fragile states provides lucrative environments in which crime can flourish. The perpetual lack of governance and law enforcement in these places undermines the ability to protect people and property. In such places, crime opportunities are rampant due to the lack of guardianship over vulnerable targets and to the ability of criminals to perpetrate crimes with relative impunity. This is especially apparent in ungoverned areas.

Ungoverned Areas and Spaces

1-47. Ungoverned areas are those physical areas without effective governance due to lack of capability, lack of capacity, lack of will, political corruption, or combinations of these factors that undermine the ability of formal governing institutions to maintain stability and order. Those states that lack a governing authority capable of securing the populace, maintaining order, implementing justice, and protecting rights are often classified as failed or failing states and may possess significant ungoverned areas in which there is a complete lack of governance.

1-48. Ungoverned areas typically refer to physical or geographic places lacking governance; however, the concept extends into other spaces in which governance is absent, such as cyberspace. Within cyberspace, virtual ungoverned spaces exist and create sanctuaries for criminals. Through virtual sanctuaries, criminals may commit crimes with anonymity and impunity. Often, cyberspace crime is most effective where physical and virtual ungoverned space coincides. Where governance is lacking, criminals may establish computer infrastructure and hacking networks that, when combined with the lack of regulation and oversight in the cyber domain, create weaknesses and opportunities for cyberspace crimes.

Alternative Governance Structures

1-49. While governance may be predominantly provided by a formal central government, this is not always the case and governance is not always synonymous with government. Governance typically denotes the actors or institutions that fulfill governance functions—security, order, economic and social wellbeing, and dispute resolution—while government generally refers to formal institutions vested with authority to perform those governance functions, regardless of whether or not they are actually capable of doing so. Governance functions may be carried out by a variety of actors in an operational area with considerable local variation. Formal governance structures may include central, regional, and local governments. Informal governance structures may include tribal and clan structures, religious and spiritual leaders, clubs and associations, and criminal or insurgent organizations. When informal governance structure surpasses or replaces formal governance structure in the fulfillment of governance functions, it is commonly called an alternative governance structure.

1-50. While ungoverned areas explain those situations for which there is no governing authority capable of providing security and order (such as anarchy), in reality, areas most often considered ungoverned are actually governed through alternative governance structures. Alternative governance structures fill the vacuum created by the lack of a capable government. Alternative governance structures may include nonstate or criminal organizations that fulfill the traditional functions of the state. They often possess the capability and capacity to provide internal security and control, justice to settle grievances or violations of norms, and economic or social services to the population.

1-51. Places that appear ungoverned from a Western perspective are often governed by alternative governance structures that are seen as illegitimate or unacceptable because they violate international laws and norms or the basic human rights of their citizens.

Corruption of Governing Individuals and Institutions

1-52. Beyond spaces that lack governance completely or those that are governed by alternative governance structures, established government institutions and individuals may be corrupted in ways that provide similar benefits to criminals and other irregular forces. This corruption may result from criminal activities like bribery, extortion, or intimidation. It may also derive from more traditional sources of corruption that are not necessarily criminal in nature and may be accepted as normal in non-Western cultures, such as nepotism, tribal loyalty, or political patronage networks. The benefits derived from corrupting government institutions and individuals include impunity to operate without law enforcement apprehension or government prosecution; access to political decision-making processes and authorities to shape decisions in criminal organization interests; and financial incentives or monetary payouts from government revenues. See the United States Agency for International Development *Anticorruption Assessment Handbook* for additional information on assessing corruption.

1-53. It is useful to distinguish between grand and petty corruption. Grand corruption refers to practices pervading the highest levels of government, leading to an erosion of confidence in the rule of law. Petty corruption involves exchanging small amounts of money or granting minor favors by those seeking preferential treatment. The difference between the two is that grand corruption involves the distortion of state governance functions, whereas petty corruption exists within the context of established social frameworks. Petty corruption needs to be controlled as part of the stability mission only when it exceeds what is acceptable within local norms or when it impinges on the security and well-being of the population. Otherwise, petty corruption is best dealt with by host-government agencies.

1-54. Another area in which military police focus attention is corruption in contracting and aid. Corruption in contracting and the distribution of foreign humanitarian assistance or aid may produce unintended negative effects and undermine U.S. efforts. When local businesses, actors, or organizations have connections to criminal organizations or engage in criminal activities themselves, the effort to establish legitimate governance and economic and security institutions under the umbrella of the rule of law may be significantly threatened. Improper allocation or corruption of contracting and aid may alter local power dynamics, empowering and financing criminal or terrorist networks and organizations. Additionally, the mismanagement or lack of oversight of contracting and aid processes can create crime opportunities for graft, corruption, and patronage while undermining the emergence of local businesses and sustainable economies. See ATP 4-10 for additional information on operational contract support.

Understanding Governance Challenges

1-55. Military police provide PIO support that is critical to understanding the crime and criminal drivers of instability and governance challenges resulting from or influenced by crime, disorder, and the fear of crime within a society. PIO provides police information and police intelligence focused on crime environments, organized criminal activity, and the operational effectiveness of two critical parts of the criminal justice system—police and corrections. PIO enhances the understanding of governance challenges by—

- Providing police information gathered during police engagement, HN police training, and regular interactions with the local police force that may provide indicators of local or ministerial corruption in police, law enforcement, or justice institutions.
- Policing to restore and maintain order and to provide information collection focused on crime, criminal activities, fear of crime within a population, and other destabilizing factors that undermine civil order.
- Continuously feeding the intelligence process with police information and police intelligence related to HN police and corrections efforts to effectively prevent, control, and reduce crime and criminal threats.

POLICE INTELLIGENCE OPERATIONS FRAMEWORK

1-56. PIO is a continuous military police task integrated within all military police operations. *Police intelligence operations* 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). It supports the operations process and influence military police operations through the analysis of police information collected during military police activities and shared police information received from unified action partners and from the production and dissemination of police intelligence products. Commanders direct information collection by approving commander’s critical information requirement (CCIRs) and by driving the operations process. The success of information collection is measured by its contribution to the commander’s understanding, visualization, and decision making.

1-57. Military police meet information collection requirements during the conduct of military police operations that may contribute to CCIRs; influence intelligence-led, time-sensitive operations; or shape policing strategies as necessary to forecast, anticipate, and preempt crime or disruptive activities to maintain order. Collected police information and the subsequent analysis enhance situational understanding, protection, civil control, and law enforcement. Generally, PIO drives military police operations focused directly on crime and criminal activity, such as law enforcement, corrections, and criminal investigations. PIO complements, but does not replace, traditional military intelligence processes during the conduct of decisive-action tasks.

1-58. PIO occurs throughout all phases of joint operations, but it may differ in significance based on where one is focused within the operational framework. For instance, units engaged in large-scale ground combat in the close area are heavily reliant on traditional intelligence, with a primary focus on the most capable threats possessing significant mobility, range, and lethality. As combat units move forward and divisions and corps create consolidation areas to perform area security tasks and transition to stability tasks to consolidate gains, the relative role and importance of PIO increase. As conventional threats are defeated or as they disperse into local populations for concealment, the primary threat evolves from conventional to irregular and criminal. As this occurs, the contributions of PIO become paramount. The deliberate focus and skill in understanding and interpreting crime and criminal activity provide technical capabilities in understanding the causes of disorder and the drivers of instability that undermine the transition from armed conflict to security and civil order according to the rule of law.

1-59. PIO is complementary to military intelligence. Because military intelligence personnel are required to maintain focus and continue to prioritize information collection and intelligence analysis of the most capable threat present in the theater. PIO often serves as an economy of force for the commander to ensure that threats which appear insignificant early in a campaign, such as those of a criminal or irregular nature, are addressed from the very beginning of the campaign and that assets are dedicated to understanding, monitoring, and disrupting criminal activities that may be linked to conventional threats or may undermine the long-term ability to consolidate gains by laying the seeds of disorder and instability within a population before the end of large-scale ground combat operations.

1-60. Military police and USACIDC personnel develop PIO skills and knowledge while supporting police operations on Army installations. This enables military police to leverage these skills across all military police disciplines—police operations, detention operations, and security and mobility support—in support of decisive action. Key definitions that provide the framework and understanding for PIO include the following:

- *Police information* is information collected during military police operations concerning crime, disorder, criminal activity, and criminal threats (FM 3-39). Police information includes, but is not limited to, a variety of data and information about crime, law enforcement, police institutions and their effectiveness, and other general information in the operational environment that is collected for analysis through a policing lens to solve crime and disorder problems. Police information is analyzed to produce police intelligence.
- *Crime analysis* is the systematic examination and interpretation of police information to determine when, where, and why crime, disorder, fear of crime, and other destabilizing events occur in specific places (FM 3-39). It may be specifically categorized as administrative, tactical, or strategic crime analysis based on the focus of analysis and the purpose it is intended to serve.
- *Criminal intelligence* is police information compiled, analyzed, and disseminated in an effort to anticipate, prevent, or monitor criminal activity (FM 3-39). It may be specifically categorized as tactical or strategic criminal intelligence based on the direction given to analysis and the purpose it is meant to serve.
- *Police intelligence* is the product resulting from the collection, processing, analysis, and integration of criminal intelligence and crime analysis about crime, disorder, criminal activity, and criminal threats (FM 3-39). Police intelligence provides commanders and military police with an in-depth picture of the criminal environment.

1-61. PIO is conducted in four deliberate steps. First, military police commanders and staffs plan and direct PIO by establishing the information collection plan and tasking collection assets. Second, military police collection assets collect and process police information. Third, police intelligence analysts produce police intelligence products through continuous and deliberate criminal and crime analysis processes that generate the knowledge products of criminal intelligence and crime analysis. Fourth, military police personnel disseminate police information and police intelligence to military police, Army organizations, and authorized unified action partners to influence current and future operations.

1-62. Figure 1-5, page 1-18, provides the framework for conducting PIO in support of military police operations and the operations process. This framework depicts the steps as sequential and independent; however, there is often significant overlap. Simultaneous actions occur across the steps based on different roles, and there are iterative cycles of activity during which collected information may produce additional information requirements that drive additional collection while other information is routed for analysis or immediate dissemination.

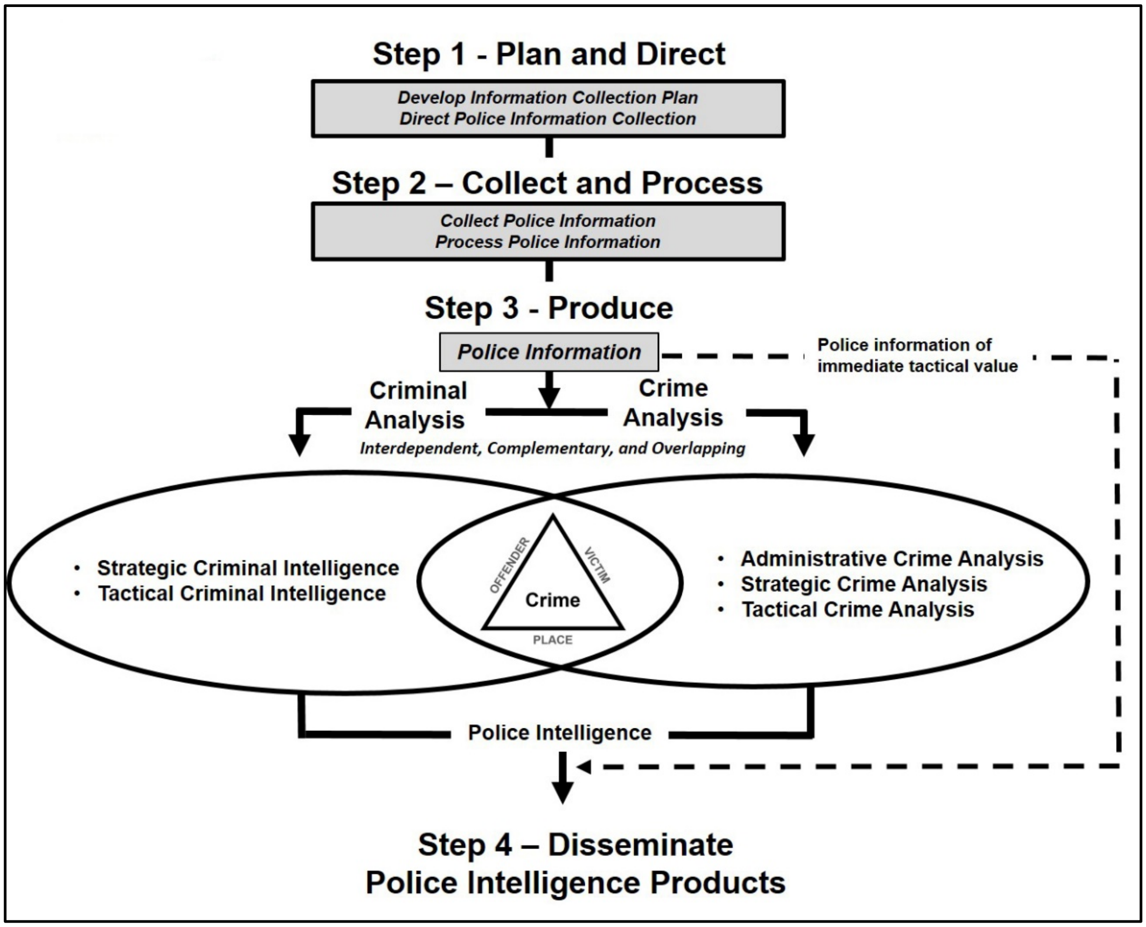

Step 1 - Plan and Direct
Develop Information Collection Plan
Direct Police Information Collection
Step 2 – Collect and Process
Collect Police Information
Process Police Information
Step 3 - Produce
Police Information
Police information of immediate tactical value
Criminal Analysis
Crime Analysis
Interdependent, Complementary, and Overlapping
• Strategic Criminal Intelligence
• Tactical Criminal Intelligence
OFFENDER
VICTIM
Crime
PLACE
• Administrative Crime Analysis
• Strategic Crime Analysis
• Tactical Crime Analysis
Police Intelligence
Step 4 – Disseminate
Police Intelligence Products

Figure 1-5 PIO framework

1-63. PIO supports commanders at all levels through the integration of police intelligence within military police operations. It enables military police, USACIDC staff, and police intelligence analysts to identify connections and correlations between people, places, events, times, and things, allowing for the identification of trends, patterns, problems, and associations pertinent to crime and disorder. PIO supports the operations process and protection supporting tasks by providing police information and police intelligence to enhance situational understanding, protect the force, enable the rule of law, and assist homeland security.

1-64. Commanders and provost marshals must determine the best way to employ available staff resources to integrate and monitor the execution of PIO within their jurisdiction or area of operations. The PIO framework provides a tool to assist military police personnel responsible for conducting PIO. Given the extension of threat networks, organizations, and capabilities beyond distant and isolated battlefields all the way to the homeland, PIO is a critical component to generating holistic understanding. The focus of PIO on crime, disorder, fear of crime, drivers of instability, criminal activity, criminal threats, and other irregular threats provides the commander with a source of technical skills and capabilities that complement traditional intelligence. The PIO framework is organized around the same framework as the Army intelligence process to maximize common understanding and enable collaboration and information sharing, as authorized by law and policy.

POLICE INTELLIGENCE OPERATIONS AND THE INTELLIGENCE PROCESS

1-65. PIO follows the Army intelligence process steps 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 and process, produce, and disseminate). In addition, there are two continuing activities (analyze and assess). (See ADP 2-0 for additional information on the Army intelligence process.) Military police commanders, staffs, and police intelligence analysts conducting PIO may perform similar tasks as traditional military intelligence personnel, but they may differ significantly in the focus, authority, and functional role of PIO.

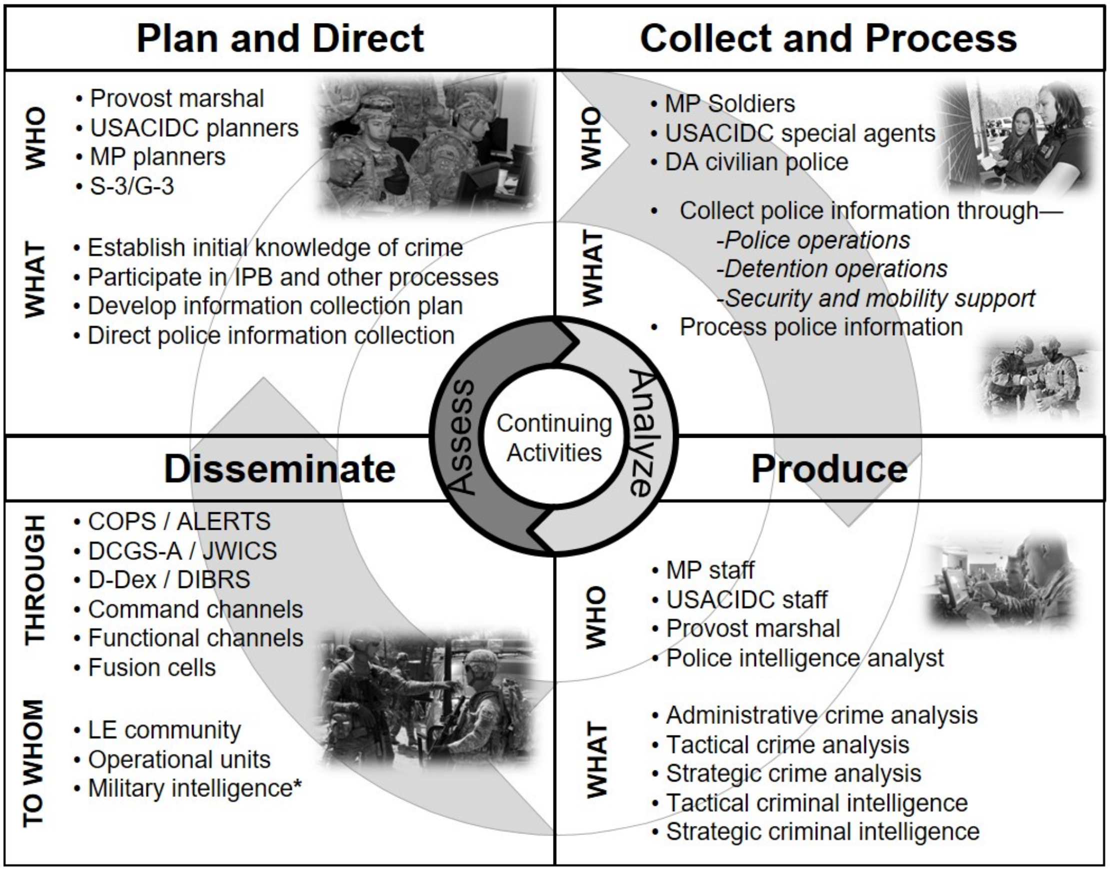
> ***Note.*** Military intelligence personnel may collect information from U.S. citizens only when it is necessary to fulfill an assigned function and when it falls within one of several categories. (See DODD 5240.01.) Military intelligence personnel will not direct military police or USACIDC elements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

1-66. PIO differs from traditional military intelligence in several distinct ways. First, PIO focuses on the collection of information relating to crime, criminal activity, policing, detention, and investigations in a particular area of operations. This information is critical to provide commanders and provost marshals a more complete understanding of criminal threats and to prevent, monitor, and address criminal activities and crime-conducive conditions during decisive action. Second, PIO is applied by military police and USACIDC personnel operating in a law enforcement capacity. This authorization is based on the presence of criminal predicate and allows for information collection serving criminal investigations and law enforcement purposes. It is not restricted in the same manner as the intelligence community (non-law enforcement) when collecting information against U.S. personnel. Third, PIO is not an intelligence discipline; it is a policing task conducted in the operations section and by operational military police elements.

> ***Note.*** Reasonable suspicion or criminal predicate is established when information exists that establishes sufficient facts to give a trained law enforcement or criminal investigative agency officer, investigator, or employee a basis to believe that there is a reasonable possibility that an individual or organization is involved in a definable criminal activity or enterprise (see 28 Code of Federal Regulations [CFR] 23).

1-67. Military police staffs and police intelligence analysts coordinate with and synchronize their activities to share police information and police intelligence with military intelligence personnel consistent with mission and legal constraints. PIO parallels the intelligence process to develop a mutual understanding based on common terminology, enable collaboration and authorized information sharing at each step in the process, and simplify the ability of military police commanders and staffs to integrate police information and police intelligence into the intelligence process at any stage. Figure 1-6, page 1-20, shows the tasks, outputs, dissemination channels, and responsibilities that enable effective collaboration between PIO and the intelligence process.

1-68. PIO differs from intelligence operations in focus, authority, and functional role; however, PIO also differs in manner and purpose of collection. Similar to intelligence operations, PIO may be guided and directed to fill specific information gaps related to crime and criminal threats through the formal process of planning and directing collection assets for deliberate collection. This is not the only, or even the primary, method for collecting police information. Most police information used for analysis, production, and dissemination originates from routine policing, corrections, and investigative activities that collect, process, and report police information for the primary purpose of fulfilling law enforcement and investigative reporting and storage requirements. Police information collected and reported as part of routine policing, corrections, and investigations is stored in law enforcement databases that serve as a critical source of resident data to produce police intelligence products.



Note. *See appendix A for legal considerations.

Legend:

ALERTS	Army Law Enforcement Reporting and Tracking System
COPS	Centralized Operations Police Suite
D-Dex	Defense Data Exchange
DA	Department of the Army
DCGS-A	Distributed Common Ground System-Army
DIBRS	Defense Incident Based Reporting System
G-3	assistant chief of staff, operations
IPB	intelligence preparation of the battlefield
JWICS	Joint Worldwide Intelligence Communication System
LE	law enforcement
MP	military police
S-3	battalion or brigade operations staff officer
USACIDC	United States Army Criminal Investigation Division Command

Figure 1-6. PIO and the intelligence process

POLICE INTELLIGENCE OPERATIONS AND THE ARMY DESIGN METHODOLOGY

1-69. *Army design methodology* is a methodology for applying critical and creative thinking to understand, visualize, and describe unfamiliar problems and approaches to solving them (ADP 5-0). It includes interconnected thinking activities that aid in conceptual planning and decision making. By first framing an operational environment and associated problems, it enables commanders and staffs to think about the situation in depth. From this understanding, commanders and staffs develop a more informed approach to solve or manage identified problems. PIO contributes to the Army design methodology by helping commanders and staffs form an understanding of the operational environment, identify problems associated with criminal and other irregular threats, and develop possible solutions that address the crime, the criminal, and instability aspects of the operational environment to promote enduring and stable outcomes. During operations, the Army design methodology supports organizational learning through reframing—a maturing of understanding that leads to a new perspective on problems or resolutions. PIO is a continuous and iterative process; it continually supports and provides commanders and staffs valuable police information and police intelligence that can assist in framing and reframing the operational environment, problems, and potential solutions throughout execution. See ATP 5-0.1 for greater details on the Army design methodology.

Framing an Operational Environment

1-70. Framing an operational environment involves critical and creative thinking by a group to build models that represent the current conditions of the operational environment (current state) and models that represent what the operational environment should look like at the conclusion of an operation (desired end state). The planning team also models the future natural tendency of the operational environment and constructs models of desired future states of other actors as points of comparison with the desired end state. Members of the planning team capture their work in an environmental frame (visual models supported by narratives) that describes and shows the relationship among the operational variables, including the social relationships and motivations of relevant actors for the current and future states of an operational environment.

Framing Problems

1-71. Identifying and understanding problems are essential for solving problems. As the commander and planning team gain an initial understanding of an operational environment, they shift their efforts to identifying and understanding those issues impeding progress toward achieving the desired end state. Through critical thinking and dialogue, the planning team frames problems by examining the differences between the current state of an operational environment and the desired end state. They also examine the differences between the natural tendency of an operational environment and desired future states of relevant actors with the desired end state. These differences are tensions (frictions, conflicts, competitions) between relevant actors, including geographic, demographic, economic, religious, and resource consumption trends. Combined, these tensions represent a set of interrelated problems (a system of problems) that requires resolution. Crime and criminal networks are often woven into the fabric of a given system. Whether criminal networks facilitate other irregular threat networks through illicit financing or they control populations directly themselves, they often contribute significantly to the overall problems that the commander and staff seek to solve.

Framing Solutions

1-72. With an understanding of the operational environment and its associated problems, including crime and the criminal aspects of those problems, the commander and planning team consider an operational approach—the broad, general actions and means to solve or manage identified problems. The commander and planning team use elements of operational art to visualize and describe the operational approach. In developing the operational approach, the commander and planning team consider the resources to support the operational approach and the associated risk. The team describes the operational approach in a visual model with supporting text. The operational approach forms the basis for the commander's planning guidance used to develop an operations order or operations plan during the military decisionmaking process. Given an adequate understanding of the crime aspects of the operational environment and problems, commanders are supported by the contributions of military police staff and police intelligence analysts who can help incorporate crime considerations into the overall adopted operational approach.

Reframing

1-73. Assessment precedes and guides the other activities (plan, prepare, and execute) of the operations process. Assessment involves comparing forecasted outcomes with events to determine the effectiveness of force employment. Assessment helps the commander determine progress toward attaining the desired end state, achieving objectives, and performing tasks. It involves monitoring and evaluating the operational environment to determine what changes affect operations; however, operations may not proceed as visualized during planning. Commanders reframe after assessing that desired conditions have changed or are unattainable by executing the current plan (including associated branches and sequels). Reframing includes revisiting early hypotheses, conclusions, and the operational approach that underpins the current plan. In reframing, the commander and staff revise their understanding of the operational environment and problem. If required, they develop a new operational approach to overcome the challenges or opportunities that precipitated the need to reframe. PIO supports the Army design methodology by continuously assessing and contributing to the commander and staff understanding of crime and criminal threats.

POLICE INTELLIGENCE OPERATIONS AND THE SCANNING, ANALYSIS, RESPONSE, AND ASSESSMENT MODEL

1-74. The scanning, analysis, response, and assessment model is a problem-solving approach developed and used in the law enforcement community. 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, and the process is repeated in iterative loops until the problem is solved.

1-75. The following is a brief discussion of each aspect of the model:

- **Scanning.** 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.

1-76. PIO supports the scanning, analysis, response, and assessment process by leveraging the unified efforts of military police and USACIDC commanders and staffs with the analytical capabilities of police intelligence analysts. Using a team approach, military police formations identify crime problems; analyze those problems to determine the root causes of crime, disorder, and fear of crime; and assess policing effectiveness in preventing and reducing crime and criminal activity. Subsequently, military police and USACIDC commanders make informed decisions based on police intelligence that influences effective police responses to solve and reduce crime problems. Figure 1-7 shows how military police commanders, staffs, and police intelligence analysts can integrate and employ PIO to support problem-oriented and preventative policing using the scanning, analysis, response, and assessment model.

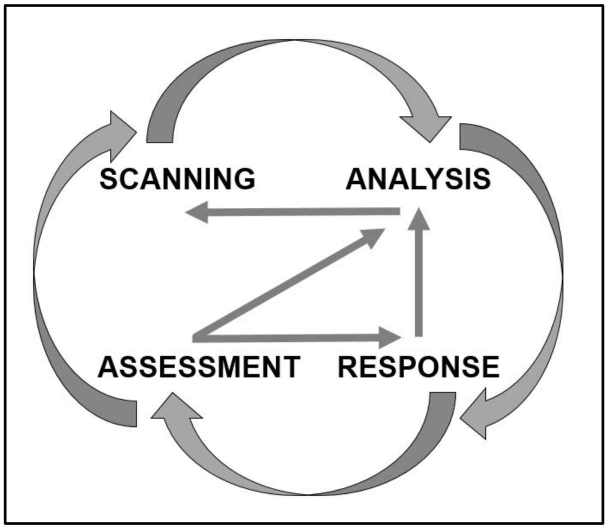


Figure 1-7. Military police employment of the scanning, analysis, response, and assessment model

ROLES AND RESPONSIBILITIES

1-77. Military police commanders and provost marshals at all echelons are typically responsible for PIO. Military police, USACIDC, and provost marshals provide police intelligence that helps commanders identify indicators and contributing factors promoting crime, disorder, criminal threats, and criminal behavior impacting Army operations or threatening Army property, facilities, or personnel. The focus of these police intelligence products can be for administrative, tactical, and/or strategic purposes (see a description of various focuses in chapter 4).

1-78. Military police staffs and provost marshals at all levels perform PIO to varying degrees, depending on mission requirements, available personnel and capabilities, 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.

ROLES AND RESPONSIBILITIES FOR CONDUCTING POLICE INTELLIGENCE OPERATIONS

1-79. During the analysis of police information, stakeholders (commanders, provost marshals, law enforcement investigators) must deconflict their priorities to ensure that 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 roles and responsibilities of commanders, provost marshals, and investigators so that decisions and priorities regarding collection, analysis, and dissemination are consistent with stakeholder requirements.

Military Police Commander and Staff

1-80. Commanders play a critical role in establishing priorities for collection, production, and dissemination and for providing focus and direction to the criminal and crime analysis processes. They determine information requirements needed to plan and execute an operation. The commander provides guidance to the staff to ensure that collection 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 priority intelligence requirement (PIR). In addition to providing clear and concise guidance and direction, military police commanders are responsible for organizing, training, and employing PIO capabilities within military police, detention, and investigative organizations.

1-81. 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 information collection activities are implemented and support the commander's intent and information requirements. This includes ensuring that PIO is fully integrated into all military police operations and that it is synchronized with the operations process. The S-3 works closely with the battalion or brigade intelligence staff officer (S-2) to ensure this synchronization.

1-82. Military police and USACIDC elements contribute to decisive action by conducting police, detention, and security and mobility support. Police information and police intelligence, when integrated into these operations, facilitate effective decision making aimed at preventing, mitigating, and reducing crime and criminal activities. When military police perform law enforcement, corrections, and criminal investigations within the United States or concerning U.S. Soldiers, PIO plays a primary role in driving police operations, while traditional military intelligence plays little to no part in these law enforcement-related functions according to the dictates of U.S. laws and policy.

Note. Domestically, military intelligence involvement is limited. However, military intelligence personnel may actively participate in PIO activities while they are assigned to a law enforcement agency when supporting law enforcement missions. See DODD 5200.27.

Criminal Investigation Division

1-83. USACIDC bears special roles and responsibilities as it relates to criminal intelligence and crime prevention programs. As the Army criminal investigative organization, USACIDC bears the responsibility established in DODI 5525.18 to establish and maintain a criminal intelligence function. AR 195-2 specifically assigns USACIDC primary responsibility to operate a criminal intelligence program. USACIDC detachments employ crime analysis and criminal intelligence to detect, analyze, and prevent criminal activity affecting Army operations, material, personnel, and installations. Criminal intelligence is the category of police intelligence focused on organized criminal activity and specific criminal threats. Criminal intelligence generates holistic understanding of crime when it is combined with the crime analysis, which is the other focus area of police intelligence.

Criminal Intelligence Responsibilities

1-84. Specific USACIDC responsibilities related to criminal intelligence include the following:

- Coordinate with other military and civilian law enforcement agencies on matters of common interest according to the Department of Defense (DOD) and Department of Justice (DOJ) instructions concerning criminal intelligence sharing.
- Disseminate criminal intelligence regarding an individual outside of law enforcement channels only to persons whose official duties create a definite and identifiable need for them to have access.
- Restrict the contents of Army investigative files to information that is necessary and relevant to authorized criminal investigation and law enforcement information-gathering activities.
- Release information regarding imminent criminal threats to the safety and security of Army operations, personnel, or material to the extent necessary to prevent the commission of the offense.
- Maintain law enforcement source confidentiality during dissemination or when sharing information with authorized unified action partners.

Note. Criminal intelligence and information concerning criminal activity shared with other law enforcement agencies are released according to the provisions of AR 195-2 and see AR 380-5 for classified information.

Command Intelligence Operations Center

1-85. The Command Intelligence Operations Center, under the direction of the USACIDC assistant chief of staff, intelligence (G-2)/assistant chief of staff, operations (G-3), is the focal point of USACIDC efforts to provide criminal intelligence and domestic threat and law enforcement information support through collaborative efforts for the Army. The Command Intelligence Operations Center consists of two branches: Investigative Analysis and Threat Analysis.

1-86. The Investigative Analysis Branch is responsible for—

- Producing quantitative and qualitative criminal intelligence reports in direct support of USACIDC investigations and operations.
- Providing support to command staff, internal USACIDC units, and external federal agencies in response to requests for assistance and requests for information.
- Providing support and analysis for specific cases, requested by command or field agents, by producing link analysis, timelines, and association charts or by the collection of relevant case information.

1-87. The Threat Analysis Branch is responsible for the collection, analysis, and dissemination of processed criminal intelligence threat information and products, which are provided to commanders, staffs, and relevant unified action partners. In addition to having analytical support at USACIDC, there are also assigned investigative analysts at several Army installations. They work alongside USACIDC special agents to evaluate data and provide products, such as link analysis and investigative reports.

Crime Prevention Responsibilities

1-88. Crime prevention is a command responsibility. A successful PIO program requires continuous command emphasis to prevent criminal activity from detracting from mission accomplishment. An effective crime prevention program enhances the safety and security of military communities in peace and war. A crime prevention program reduces crime by—

- Instilling appropriate crime prevention attitudes, procedures, and behavior through public awareness campaigns and programs.
- Protecting potential victims or property from criminal acts by anticipating and eliminating potential crime opportunities.
- Discouraging potential offenders from committing criminal acts.

1-89. USACIDC elements are critical in supporting Army crime prevention programs. In this capacity, USACIDC leverages unique skills in crime analysis to provide support beyond simply investigating and apprehending offenders. The tools and techniques of crime analysis (such as crime pattern analysis, crime sprees and series, linkages among crimes, and crime trends or trajectories) enable USACIDC personnel to evaluate crime environments, assess unit or specific target location vulnerabilities, and produce police intelligence products, such as crime prevention surveys, crime prevention flyers, and threats and vulnerability assessments. Such products are crucial to prevent crimes within an area of operations and to support Army commanders responsible for protecting their personnel, property, and readiness against potential crime and criminal threats. See AR 190-13 for details on the Army crime prevention program.

Provost Marshal

1-90. While military police and USACIDC commanders are responsible for PIO for their assigned missions, jurisdictions, or area of operations, provost marshals are responsible for PIO in support of law enforcement on bases and base camps. Typically, the provost marshal office or police station responsible for law enforcement on installations falls under the directorate of emergency services and reports to the garrison commander and/or the senior installation commander.

1-91. The provost marshal staff may have a trained Soldier or DA Civilian police intelligence analyst assigned or attached to perform PIO as part of the operations section. These PIO analysts provide the provost marshal with the capability to fulfill senior commander information and intelligence requirements related to crime and to produce crime analysis products to support crime prevention, community awareness, and police engagement. Provost marshal staffs, in conjunction with USACIDC personnel, use PIO to help commanders identify indicators of potential crimes and criminal threats against Army operations, property, and personnel.

1-92. In brigade combat teams and echelons above brigade, PIO is conducted and managed by the provost marshal operating as part of the S-3/G-3. In these organizations, the provost marshal 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. The contributions of PIO help develop a more comprehensive common operational picture for the commander through a dedicated focus and understanding of crime and disorder and through destabilizing criminal activities threatening the commander's physical assets, readiness and discipline, and ability to accomplish the assigned mission.

Police Intelligence Analyst

1-93. The term police intelligence analyst is used to describe police intelligence analysts who work for military police formations and provost marshal staffs and investigative analysts who retain the criminal intelligence designator given the responsibility to maintain a criminal intelligence program and the focused criminal investigative mission of USACIDC. Police intelligence analysts (regardless of unit assignment) are trained and certified to perform criminal and crime analysis after completing the Crime and Criminal Intelligence Analyst Course at USAMPS. Following certification at this course, police intelligence analysts may be employed in various police intelligence roles and across military police formations to fulfill the analytical function necessary to conduct PIO.

1-94. Regardless of the environment, police intelligence analysts conduct criminal and crime analysis of police information to produce police intelligence to support commanders, provost marshals, and investigators. The ultimate goal for police intelligence analysts and staffs performing PIO is to develop useable police intelligence products. The trained police intelligence analyst provides the following capabilities to the unit commander, provost marshal, or law enforcement investigator:

- The development of initial background data and knowledge relative to police operations and the crime environment for a specific area of operations or law enforcement investigation.
- The compilation of collected police information for analysis or immediate dissemination.
- Police information and police intelligence that identify crime and criminal trends, patterns, associations, and other police-related statistics and information that increase the understanding of—
  - Offenders, groups, and criminal networks.
  - Criminal funding sources.
  - Specific individual and group (supporter, financier, corrupt official, supplier, trafficker, smuggler, recruiter) activities.
  - Geographic relationships of crime and criminals.
  - The population from the perspective of policing and the criminal dimension.
- The identification of police information gaps and recommendations of information requirements and collection strategies.
- The identification of systemic issues in police organizations.
- The 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 specific missions or audiences.
- Support to the targeting process.
  - Creating police intelligence products.
  - Giving recommendations for targeting strategies.
- Support to law enforcement and law enforcement investigators in case developments.
  - The identification of background information and criminal history.
  - The identification of gaps in information relevant to specific investigations.
  - Recommendations for additional law enforcement and investigation efforts.

Police Intelligence Training and Certification

1-95. The quality of police intelligence products that police intelligence analysts may produce rests largely on their analytical ability, creative thinking skills, and a solid foundation of training and certification. Military police and USACIDC commanders and staffs should dedicate special attention to identifying the most highly qualified, mature, and independent individuals for selection as police intelligence analysts.

Police Intelligence Analyst Selection

1-96. Soldiers selected to attend training and certification as police intelligence analysts should possess the following skill sets:

- Technical expertise in policing, corrections, or investigations.
- Knowledge of targets and targeting processes.
- Experience and expertise in criminal analysis and crime analysis techniques.
- Research and organization abilities.
- Inductive reasoning and data-synthesizing abilities.
- Knowledge in select criminology theories.

- Ability to evaluate the integrity of information.
- Knowledge of criminal behavior.
- Understanding of the criminal justice system.
- Reading comprehension and critical thinking skills.
- Report writing and briefing abilities.
- Word processing, spreadsheet, and Internet research skills and abilities.
- Applied research methods in crime analysis.
- Evaluation of quantitative and qualitative information.

1-97. In the absence of assigned police intelligence analysts, military police commanders and staffs may still develop police intelligence analyst capabilities and capacities by training and certifying qualified and experienced military police and USACIDC personnel who possess policing, corrections, or investigative experience in preventing, monitoring, controlling, and responding to crime and criminal activity. Appendix C provides additional information for organizing and employing PIO across various echelons.

Crime and Criminal Intelligence Analyst Course

1-98. The Crime and Criminal Intelligence Analysts Course at USAMPS is the approved course to train police intelligence analysts for military police and USACIDC units. In support of bases or base camps, PIO is typically conducted more exclusively by USAMPS-trained and -certified police intelligence analysts. Police information and police intelligence products remain in law enforcement channels due to legal restrictions placed on the intelligence collection on U.S. citizens. (See appendix A for additional information on legal authorities pertaining to PIO.) In support of unified land operations outside the United States or its territories, police intelligence analysts may use their unique police intelligence training, skills, knowledge, and experience analyzing crime and criminals to support and complement the intelligence process through collaboration and fusion with the S-2/G-2.

1-99. Police intelligence analysts provide specific analytical expertise regarding crime and criminality in support of PIO. The first step for military police and USACIDC formations to build PIO capability and capacity is to send qualified and experienced military police and USACIDC personnel to the Crime and Criminal Intelligence Analyst Course. This course provides a common foundation for police intelligence analysts to perform criminal and crime analysis. Building on this foundation, military police and USACIDC commanders may further enhance PIO capability through unit and individual professional development and through assignments to perform criminal and crime analysis and gain on-the-job experience. This combination of institutional training coupled with additional self-development and operational experience is necessary to understand the complex fields of crime, criminality, and criminal behavior. The selection of personnel who possess the interest and self-motivation to develop such knowledge and capacity beyond the baseline course is critical to the success of a unit's police intelligence capability.

POLICE INTELLIGENCE OPERATIONS CONTRIBUTIONS TO UNIFIED LAND OPERATIONS

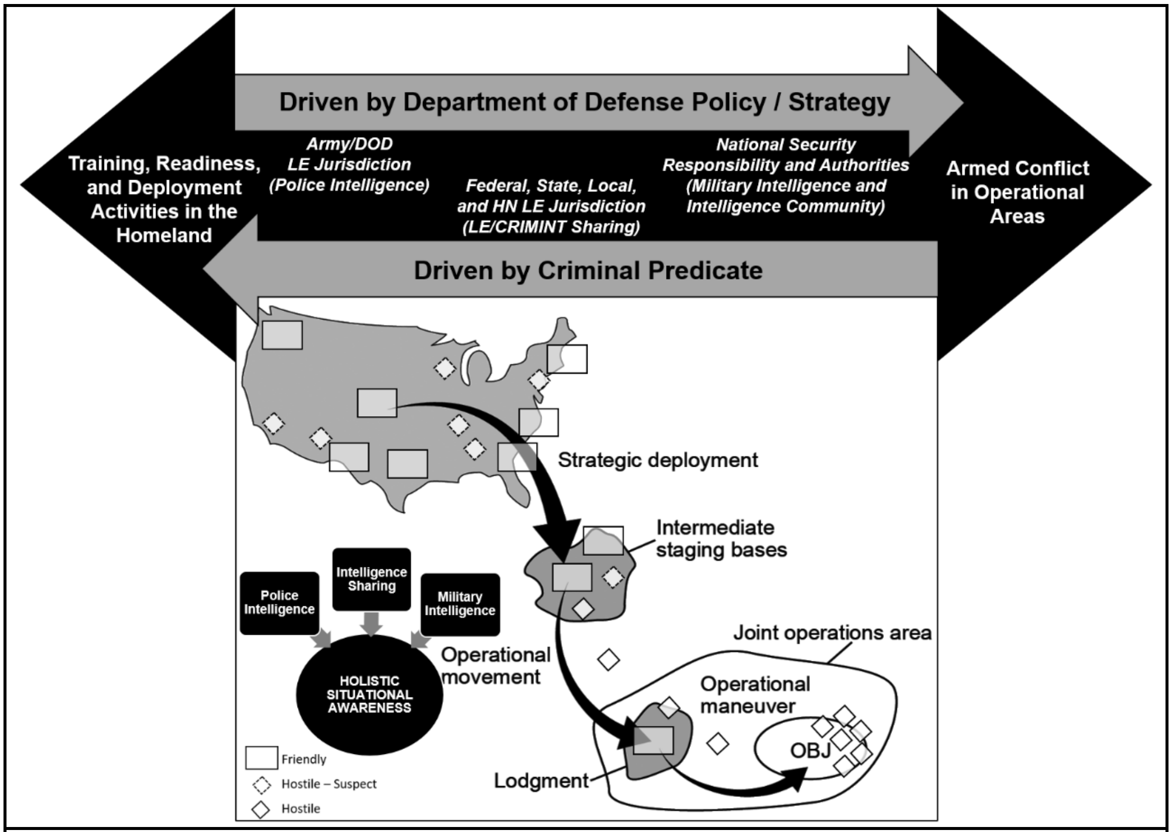
1-100. The role of PIO is to support commanders, provost marshals, and staffs in gaining a situational understanding of criminal threats, criminal activities, and crime environments to support decision making by providing criminal intelligence and crime analysis products generated from a unique policing perspective. Police information and police intelligence is integrated within the common operational picture to enable commanders to take effective actions against threat forces at home station and overseas. The ultimate goal of PIO is to—

- Assist commanders and provost marshals in preventing, investigating, and reducing crime on bases and base camps.
- Enhance commander crime prevention and protection programs.
- Feed the Army operations process and its integrating activities.

1-101. Commanders at all levels are responsible for the good order and discipline of their formations. Military police and USACIDC support commanders in fulfilling this responsibility by providing law enforcement, corrections, and investigations to prevent, deter, control, investigate, and reduce crime and criminal threats on bases and base camps and within military formations. PIO enables military police to produce policing, corrections, and investigative effects for commanders by enhancing understanding of crime environments; analyzing crime places, patterns, and problems; and supporting criminal investigations with focused crime analysis. The situational understanding that PIO delivers to commanders and provost marshals enables them to reduce and mitigate the effects of criminal activity to Army personnel, equipment, and facilities. In addition, PIO develops criminal intelligence for in-transit security and focuses the development and implementation of threat countermeasures to safeguard Army personnel, material, and information going to and returning from operational theaters.

1-102. Despite the clear distinction between home station activities and decisive-action tasks conducted in overseas operational environments, criminal threats to military operations are often not as equally clear-cut. Criminal activities threaten to disrupt military discipline, readiness, and operations at home station, in transit to and from operational theaters, and while executing decisive-action tasks in overseas joint operations areas. Because of the dynamic and ever-present threat of crime throughout the strategic depth of Army formations, PIO provides a capability that bridges the gap that traditional military intelligence cannot cross. PIO supports the commander’s protection efforts to preserve the force at home station and protect against the disruption of combat power by criminal threats across globally extended lines of communication. See AR 525-2 for additional information on the Army Protection Program.

1-103. 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/G-2 to ensure that PIO is synchronized and integrated with the intelligence process. During offensive and defensive operations, PIO plays a secondary but complementary role to traditional military intelligence operations. In this role, PIO enables the staff to identify criminal organizations and networks in the area of operations that provide indications of disruptive activities and criminal threats that may produce a significant negative effect on military operations. As operations transition from offensive and defensive focuses to stability operations and the consolidation of gains, PIO plays a larger role in identifying and evaluating crime and disorder problems, patterns of criminal activity, enduring criminal threats, and HN police and corrections capabilities and effectiveness in establishing civil security and civil control, protecting communities from criminal threats, and restoring legitimate governance and civil order according to the rule of law. Figure 1-8 demonstrates the contributions of various participants from strategic to tactical levels that contribute to holistic situational awareness across strategic depths based on unique jurisdictions and authorities.


Driven by Department of Defense Policy / Strategy
Training, Readiness, and Deployment Activities in the Homeland
Army/DOD LE Jurisdiction (Police Intelligence)
Federal, State, Local, and HN LE Jurisdiction (LE/CRIMINT Sharing)
National Security Responsibility and Authorities (Military Intelligence and Intelligence Community)
Armed Conflict in Operational Areas
Driven by Criminal Predicate
Strategic deployment
Intermediate staging bases
Police Intelligence
Intelligence Sharing
Military Intelligence
HOLISTIC SITUATIONAL AWARENESS
Operational movement
Joint operations area
Operational maneuver
OBJ
Lodgment
Friendly
Hostile – Suspect
Hostile

Legend:

CRIMINT	criminal intelligence
DOD	Department of Defense
HN	host nation
LE	law enforcement
OBJ	objective

Figure 1-8. Information sharing across strategic depth

Note. Figure 1-8 does not use official symbology to demonstrate the contributions of various participants from strategic to tactical levels that contribute to holistic situational awareness across strategic depths based on unique jurisdictions and authorities.

INFORMATION GAP BRIDGING

1-104. PIO provides capabilities that bridge the gap between traditional military intelligence and information focused on policing and crime environments in several ways. When the S-2/ 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. The S-2/G-2 develops an information collection plan to help the commander fill this information gap. Military police staffs and provost marshals also identify information gaps pertinent to policing activities and develop recommended intelligence requirements to fill gaps related to crime and criminal activity. Recommended intelligence requirements may be coordinated with the S-2/G-2 as a request for information and then, if necessary, added to the collection plan as an intelligence gap.

1-105. The ability of commanders to maintain good order and discipline and to protect personnel, equipment, and operations from criminal activity and threats is linked to the capability of military police and USACIDC elements to identify, prevent, control, and investigate crime and criminal activity. Military police and USACIDC elements capitalize on connections and information-sharing networks with federal, state, and local civilian law enforcement agencies to obtain information generally not obtainable through non-law enforcement sources. PIO uses this information and employs crime analysis techniques to identify crime places, patterns, and problems that may negatively impact the good order and discipline of Army formations. Additionally, PIO provides commanders and provost marshals with the timely criminal intelligence required to disrupt threats posed by criminal offenders, networks, and organizations operating on, near, or against military installations and base camps to preserve readiness and protect the force.

1-106. 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.
- Along main supply routes.
- In support or consolidation areas.
- In support of a movement corridor. (See FM 3-81.)

1-107. Concurrent with the requirements to collect information in support of identified intelligence requirements, military police personnel collect police information related to the police and criminal environment to facilitate the transition to stability operations and the establishment of civil security and civil control. As operations transition from offense and defense to stability, 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 HN 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.

1-108. Part of the senior intelligence officer collection strategy is to select the best collection asset available to cover each information requirement. 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-organize or coordinate for nonorganic collection assets. In brigade combat teams, divisions, and corps, the provost marshal coordinates with the S-2/G-2 to ensure that military police-related information requirements are synchronized and integrated into the overall information collection plan. After a thorough analysis (to include availability, capability, and performance history), the S-2/G-2 identifies which collection assets can best be used. When military police or USACIDC personnel are tasked with an information collection mission, they are provided specific guidelines and prioritized collection requirements to enable the planning and direction of information collection to fill the gaps related to crime, criminal activities, and police effectiveness.

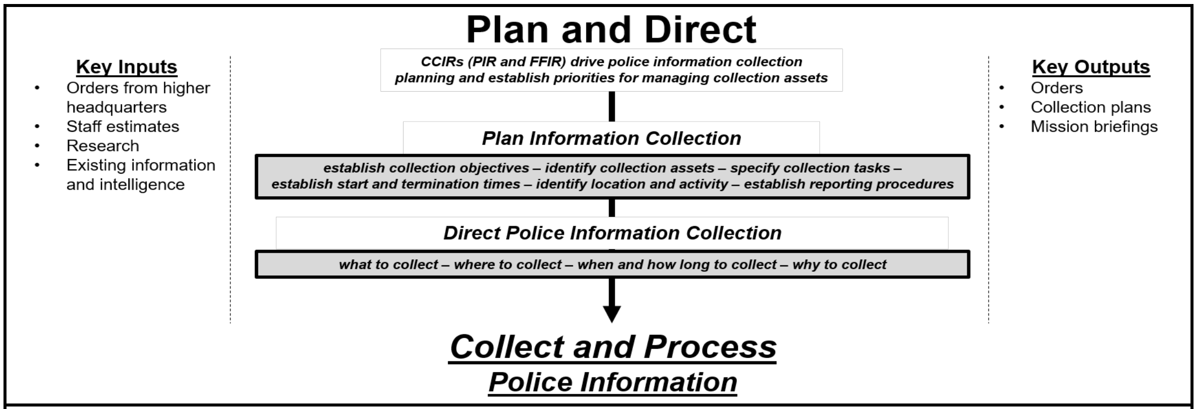
Chapter 2

Plan and Direct

This chapter describes step one of the PIO framework: plan and direct. PIO is a requirements-driven process that focuses on answering information and intelligence requirements. Planning originates with the commander's visualization and is developed by the staff to achieve the commander's intent, guidance, and desired end state. The information collection plan involves several factors that need consideration before directing collection assets to execute the information collection plan in support of military police or Army operations.

REQUIREMENTS DRIVEN

2-1. PIO is an iterative process that begins and ends with the continuous assessment of crime environments, criminal threats, and police effectiveness to determine the information required to prevent, investigate, control, and reduce crime. Military police constantly scan the environment for crime, disorder, fear of crime, and other destabilizing effects that disrupt good order and discipline, threaten the readiness of the force, and undermine stability. Military police use their presence and situational awareness to identify criminal threats and crime problems that require police prevention and response. The information necessary to effectively police and protect military installations, bases, formations, and populations combines with information and intelligence requirements to drive the planning process and the direction of police information collection. Figure 2-1 illustrates the first step of PIO.


Plan and Direct
Key Inputs
• Orders from higher headquarters
• Staff estimates
• Research
• Existing information and intelligence
CCIRs (PIR and FFIR) drive police information collection planning and establish priorities for managing collection assets
Plan Information Collection
establish collection objectives – identify collection assets – specify collection tasks – establish start and termination times – identify location and activity – establish reporting procedures
Direct Police Information Collection
what to collect – where to collect – when and how long to collect – why to collect
Key Outputs
• Orders
• Collection plans
• Mission briefings
Collect and Process
Police Information

Legend:

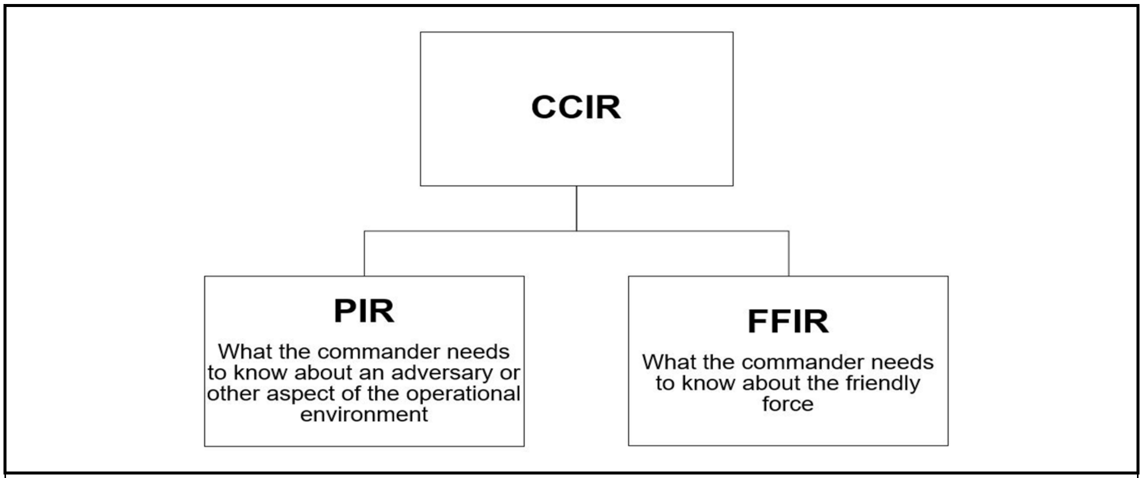
CCIR	commander's critical information requirement
FFIR	friendly forces information requirement
PIR	priority intelligence requirement

Figure 2-1. Plan and direct police intelligence operations

2-2. Military police support Army commanders at home station and during decisive action by conducting PIO that complement traditional military intelligence and fill information gaps related to crime, criminal threats, and other irregular threats. Military police commanders and staffs planning PIO must first thoroughly understand the commander's intent and concept of operations. This understanding leads to the identification of information gaps, especially those related to crime, criminals, irregular threats, and police or correctional institutions responsible for maintaining security and stability. During mission analysis, military police planners review the CCIRs to help establish priorities and provide guidance for the management of military police collection assets. Planners inform the collection effort by using all available information through reachback, research, or other means to establish a baseline of knowledge. Information not available may be designated as an information requirement. See FM 3-39 for additional information on military police and the military decisionmaking process.

2-3. An *information requirement* is any information element the commander and staff require to successfully conduct operations (ADRP 6-0). It includes all elements necessary to address the mission variables (mission, enemy, terrain and weather, troops and support available, time available, and civil considerations). Military police planners consider the operational variables when planning information requirements. In particular, PIO contributes significant information to the commander's understanding of social, economic, and political variables, where crime is often a leading driver of instability, disorder, social conflict, illicit activities, markets that disrupt economic growth and prosperity, and corruption or coercive violence that undermines political authority and sovereignty. Prioritized information requirements are used to develop the information collection plan. The information collection plan provides focus and direction to collection efforts by documenting, prioritizing, and assigning collection assets against specific information requirements to enhance the situational understanding of crime within the operational environment. See FM 3-39 for an additional discussion of military police considerations of the operational variables.

2-4. Commanders designate the most important, time-sensitive information needed for the CCIR; PIO anticipates and responds to the CCIR. A *commander's critical information requirement* is an information requirement identified by the commander as being critical to facilitating timely decision making (JP 3-0). The commander is supported in determining the CCIR by his staff, including intelligence, provost marshal, and other staff sections and subordinate units. The staff recommends information requirements for the commander to designate as CCIR. They also recommend changes to CCIR based on the continuous assessment of ongoing operations. CCIR is composed of two categories: friendly force information requirement (FFIR) and PIR. Figure 2-2 depicts the relationship of CCIR, PIR, and FFIR.


CCIR
PIR
What the commander needs to know about an adversary or other aspect of the operational environment
FFIR
What the commander needs to know about the friendly force

Legend:

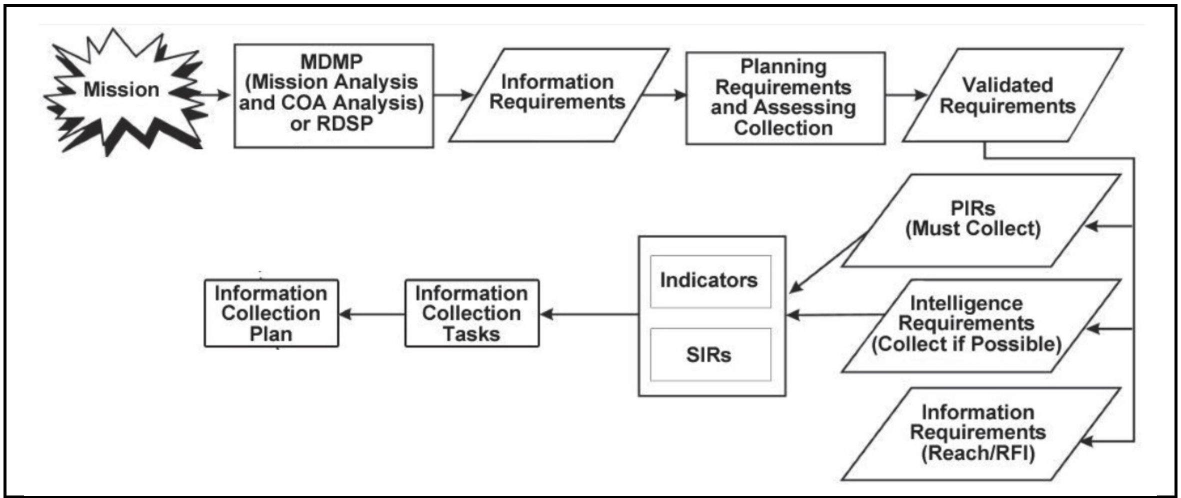
CCIR	commander's critical information requirement
FFIR	friendly force information requirement
PIR	priority intelligence requirement

Figure 2-2. Information requirements

2-5. A *friendly force information requirement* is information the commander and staff need to understand the status of friendly force and supporting capabilities (JP 3-0). FFIRs identify the information the commander considers as most important regarding the mission, troops and support available, and time available for friendly forces. The S-3/G-3 manages FFIR for the commander. PIO produces significant amounts of information regarding friendly forces through internally focused law enforcement, corrections, and criminal investigations that support the commander's readiness and ability to uphold good order and discipline. PIO also supports the commander's understanding of the friendly force protection status through a deliberate focus on assessing friendly force vulnerabilities to criminal and other irregular threats (terrorists, insurgents, guerrillas, insider threats).

2-6. An *intelligence requirement* is a requirement for intelligence to fill a gap in the command's knowledge or understanding of the operational environment or threat forces (JP 2-0). Intelligence requirements are filled through a number of methods and capabilities. The information collection plan addresses intelligence requirements that, when answered, fill gaps in knowledge and understanding. Military police direct the information collection plan (or contribute to the supported commander's information collection plan) by focusing military police collection assets on the crime, criminal activity, disorder, fear of crime, and other destabilizing events occurring throughout an area of operations. Information collection to fulfill intelligence requirements may result from military police sources and methods discussed in chapter 3 and through coordination and liaison with other military units (U.S. and multinational), including civil affairs, elements conducting reconnaissance, sustainment units, other policing and law enforcement agencies, and nongovernmental organizations.

2-7. Those intelligence requirements deemed as the most critical to mission success are prioritized for collection. A *priority intelligence requirement* is an intelligence requirement that the commander and staff need to understand the threat and other aspects of the operational environment (JP 2-01). The intelligence staff manages PIRs for the commander; however, the commander must limit the number of PIRs to focus the efforts and limit collection assets. Military police personnel—notably provost marshals, military police commanders, and police intelligence analysts—monitor the PIR and other intelligence requirements to influence collection planning and maintain awareness of those intelligence requirements that require immediate dissemination of collected police information to support timely decision making. Figure 2-3 depicts the requirements development process.


Mission
MDMP (Mission Analysis and COA Analysis) or RDSP
Information Requirements
Planning Requirements and Assessing Collection
Validated Requirements
PIRs (Must Collect)
Indicators
SIRs
Intelligence Requirements (Collect if Possible)
Information Requirements (Reach/RFI)
Information Collection Tasks
Information Collection Plan

Legend:

COA	course of action	RFI	request for information
MDMP	military decisionmaking process	SIR	specific information requirement
PIR	priority intelligence requirement		
RDSP	rapid decision making and synchronization process		

Figure 2-3. Requirements development

2-8. Police information 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 sources of police information. Police-related 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-related intelligence requirements, and investigative requirements. Regardless of the phase of the operation or the operational area, the integration of police information and police intelligence to answer information or intelligence requirements is the most crucial aspect of successful PIO. The end state of successful PIO is supporting decision making that enables the commander to address criminal threats and the drivers of crime and instability in the operational environment.

2-9. Requirements related to police and prison systems, policing activities, and crime environments are of specific interest to military police, USACIDC commanders and staff, and police intelligence analysts. A PIR of interest to police intelligence analysts may include the identification of previously unknown criminal or other irregular threat networks, such as networks or methods and routes used for the concealment and movement of contraband (weapons, money, drugs). Also of specific concern and focus for military police and USACIDC personnel are the capability and capacity of HN police, prison systems, and infrastructure; the determination and impact of criminal activity in the area of operations; and the functionality of the criminal justice system.

2-10. Before tasking military police to collect police information, commanders and staffs employ police intelligence analysts to perform activities that generate knowledge and information about the crime environment or to fulfill the information requirement without requesting the employment of collection assets. These activities include—

- Performing searches and queries of police or detention databases (the Army Law Enforcement Reporting and Tracking System [ALERTS], Army Corrections Information System, or Detainee Reporting System).
- Data mining police databases with analytical software to generate initial statistical or other data that directly answers information requirements without requiring further analysis.
- Coordinating and providing liaison activities with other military units (U.S. and multinational), including civil affairs, special operations forces, and elements conducting reconnaissance and security operations.
- Employing military intelligence personnel (when authorized) to leverage organic Distributed Common Ground System–Army (DCGS-A) capabilities for the query of intelligence databases and the integration of information from intelligence sources.
- Sharing information and collaborating with unified action partners (local law enforcement organizations, federal law enforcement agencies, partner nation law enforcement personnel).

2-11. At times, information may be specific enough to be recognized as having immediate value to answer the PIR. Other times, information may fulfill other intelligence requirements that fill in a piece of the puzzle. Military police and police intelligence analysts must distinguish between information that must be disseminated immediately to inform the commander, protect U.S. forces, or accomplish the mission or information that may be used during criminal and crime analysis to deduce patterns, make inferences, and generate the police intelligence necessary to fill gaps in knowledge related to crime and criminal activity.

PLAN INFORMATION COLLECTION

2-12. The commander plays a central role in developing the information collection plan by providing the commander's intent, planning guidance, and approving the CCIR. The CCIRs (PIR and FFIR) drive the planning of the information collection effort and establish priorities for the management of collection assets. The commander's visualization provides the basis for staff planning as the commander and staff work in unison to achieve the desired end state. Commanders communicate their visualization with the their staff and subordinates by describing the desired end state and articulating their initial vision in terms of—

- The initial commander's intent.
- Planning guidance, including an initial concept of operations.
- Collection requirements.

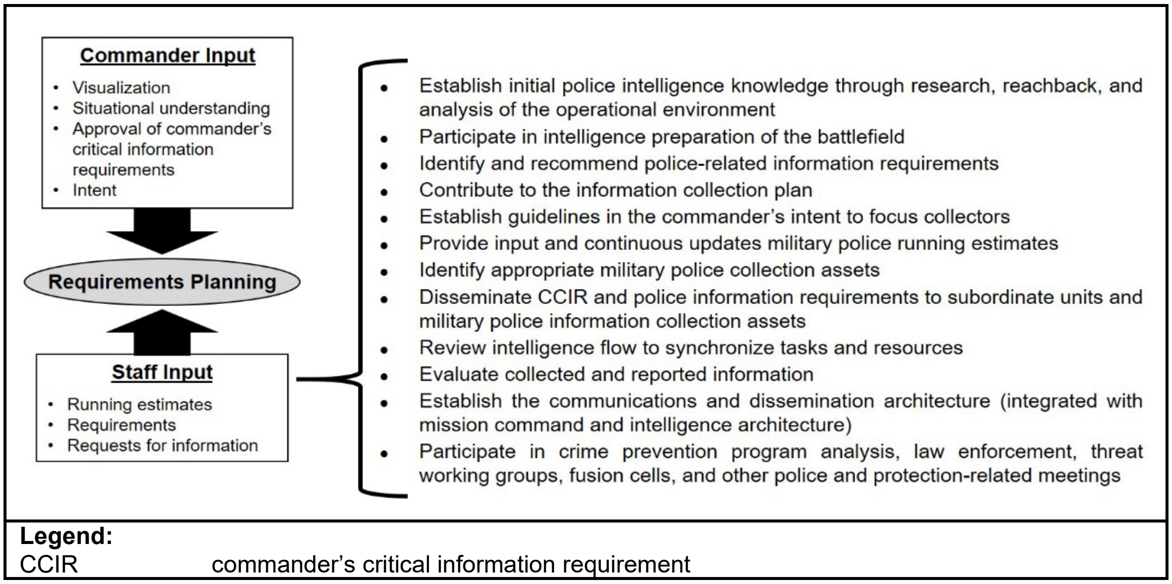
2-13. Military police staff use the commander's inputs to develop the information collection plan or support the development of the overall information collection plan. Within military police and USACIDC formations, the S-2/G-2 works closely to develop the information collection plan that puts the commander's intent, guidance, and requirements into action through tasking orders to organic or attached military police collection assets. Planning information collection tasks helps to leverage unique military police or USACIDC collection capabilities, skills, and knowledge to achieve an understanding of crime environments and organized criminal activity relevant to current and future military police operations.

2-14. Military police staff who plan law enforcement, investigation, and detention operations on bases and base camps use similar planning processes to shape patrol distribution, investigative priorities, and detention guard force employment. Planning often focuses on local prioritization, direction, and mission briefings from direct leadership where formal staffs do not exist. The following are examples of planning efforts within various military police formations:

- **Installation provost marshal/police station.** The provost marshal and operations staff oversee the management of information and intelligence priorities to meet the installation commander's intent, fulfill CCIRs, and determine the requirements necessary to provide a safe and secure installation. Police station direct leadership (watch commanders, the operations officer, and patrol supervisors) plan patrol distribution, information collection priorities, and specify collection tasks through regular guard mount mission briefs.
- **Criminal investigation division element.** The special agent in charge of a USACIDC office supporting an installation prioritizes investigative missions and the associated information and intelligence requirements. Through direction and mission briefings, the special agent in charge communicates priorities to individual USACIDC special agents to execute information collection to influence investigative priorities or meet installation and USACIDC commander CCIRs.
- **Detention facility staff.** The detention facility staff manages the detention facility commander's CCIR focused on PIR about the detained population (U.S. military prisoners or detainees) and FFIR focused on the guard force and detention staff. Daily guard force briefings provide direction and priorities for passive information collection in the course of routine detention tasks.

2-15. During decisive action, the brigade combat team (or higher) S-3/G-3 integrates the efforts of the staff to develop the overall information collection plan. The provost marshal must work closely with the S-3/G-3 and S-2/G-2 to synchronize and integrate information collection planning requirements and priorities into the coordinated information collection plan. In doing so, the provost marshal may recommend requirements for attached or supporting military police collection assets or prioritize information from other sources vital to generating the understanding of crime and criminal effects necessary to achieve the commander's desired end state (see figure 2-4). The provost marshal provides input into staff requirements planning by continuously feeding crime and police-focused—

- Running estimates.
- Requirements.
- Requests for information.


Commander Input
• Visualization
• Situational understanding
• Approval of commander's critical information requirements
• Intent
Requirements Planning
Staff Input
• Running estimates
• Requirements
• Requests for information

- Establish initial police intelligence knowledge through research, reachback, and analysis of the operational environment
- Participate in intelligence preparation of the battlefield
- Identify and recommend police-related information requirements
- Contribute to the information collection plan
- Establish guidelines in the commander's intent to focus collectors
- Provide input and continuous updates military police running estimates
- Identify appropriate military police collection assets
- Disseminate CCIR and police information requirements to subordinate units and military police information collection assets
- Review intelligence flow to synchronize tasks and resources
- Evaluate collected and reported information
- Establish the communications and dissemination architecture (integrated with mission command and intelligence architecture)
- Participate in crime prevention program analysis, law enforcement, threat working groups, fusion cells, and other police and protection-related meetings

Legend:

CCIR	commander's critical information requirement

Figure 2-4. Military police contributions to requirements planning

Police Information

2-16. Police information is an overarching term referring to various forms of data and information collected or integrated by military police to influence PIO and generate an understanding of crime, and criminal activity, and police effectiveness in countering those activities. *Data* is unprocessed signals communicated between any nodes in an information system, or sensing from the environment detected by a collector of any kind (human, mechanical, or electronic) (ADRP 6-0). Data can be quantified, stored, and organized in files and databases; however, data only becomes useful when it is processed into information. Information is the meaning that a human assigns to data by means of known conventions used in their representation. The types of data and information that may comprise police information include an array of different types, including—

- **Crime data.** Crime data is data regarding crime that is stored in databases and files that may be processed and analyzed. Crime data may be collected and processed across operational environments and may be stored in various types of databases, depending on the setting and the authorities involved in collection. During overseas decisive action, databases used may include law enforcement, detention, or intelligence-focused databases. Crime data may include reports of crimes, crime statistics, and military police data entries directly related to a criminal incident (time, date, location, complainant, witness, subject, type of offense, characteristics of subject).
- **Law enforcement data.** Law enforcement data is data related to law enforcement activities, operations, and programs focused on enforcing the law. Calls for service, patrol response times, police manning, and patrol distribution are examples of law enforcement data that may be analyzed to generate understanding of police effectiveness in preventing, deterring, and reducing crime and disorder.
- **Criminal information.** Criminal information (sometimes called investigative information) is information pertaining directly to a criminal offender or subject. Criminal information regarding U.S. citizens must adhere to strict policy and regulations regarding use, storage, and sharing. (See AR 190-45 and AR 195-2.) Criminal information regarding foreign threat personnel in overseas operational areas is less constrained.
- **Biometric data.** *Biometric data* is computer data about and individual created by biometric systems during an enrollment, verification, or identification process (ATP 2-22.82). The categories of biometric data are called modalities. A biometric modality is a type or class of biometric sample originating from a person. Commonly collected modalities include facial or iris images, fingerprints, voice wave files, and palm prints. Some emerging modalities that may be collected in the future are vascular mapping, retina images, gait (manner of walking), hand geometry, and handwriting. See ATP 2.22.82 and ATP 2-22.85 for additional details on biometrics and biometrics-enabled intelligence.
- **Forensic information.** Forensic information results from materials collected at a crime scene or incident site linked to threat operations or personnel. Analysis of forensic materials establishes facts that prove or disprove links to people or events. Examples of forensic materials are fingerprints, deoxyribonucleic acid (DNA), blood, tool markings, electronics, electronic media, explosive materiel, explosive residue, weapons, manuals, documents, illicit drugs, currency, or footprints. See ATP 3-39.12 and ATP 3-90.15 for more details on evidence, forensic material collection at crime scenes and site exploitation.
- **Geospatial information.** *Geospatial information* is information that identifies the geographic location and characteristics of natural or constructed features and boundaries on the Earth, including: statistical data and information derived from, among other things, remote sensing, mapping, and surveying technologies; and mapping, charting, geodetic data and related products (JP 2-03).
- **Criminal justice data.** Criminal justice data is information related to the criminal justice system that can be used to measure police and detention effectiveness in preventing and reducing crime and holding offenders accountable for criminal activity. This may include data related to criminal apprehensions, prosecutions, detention, and release from the criminal justice system, including arrest rates, prosecution outcomes, sentencing data, and recidivism rates.

- **Other types of data.** Demographic, population, historical, and other relevant data may be integrated from diverse sources, depending on the situation and the crime problem being solved. The root causes of crime often result from factors beyond the immediate control of military police organizations. Understanding crime problems requires consideration of all relevant factors influencing crime environments, crime problems, and criminal activity.
- **Other information obtained through military police patrols and police engagement.** The most common sources of police information are the personal observations of military police and USACIDC personnel and the information provided directly by relevant populations during the conduct of military police operations. Military police integrate information collection considerations into the performance of all tasks and missions by employing active and passive methods of collection. While passive collection occurs continuously during the performance of all military police operations, active collection is driven by deliberate and planned collection objectives and collection asset tasking. See chapter 3 for an additional discussion of the methods and sources of information collection.

ESTABLISH COLLECTION OBJECTIVES

2-17. Information and intelligence requirements are used to build the information collection plan. Military police begin developing the information collection plan by establishing the objectives they seek to achieve through collection. This purpose-driven approach focuses the collection effort on the results and end state to be achieved from the start. The information collection plan is prepared based on specific intelligence requirements, the commander’s guidance, and available collection assets. The information collection plan is developed to document and prioritize information requirements and pair those requirements against collection assets.

2-18. Collection objectives should focus on—

- Fulfilling the CCIR.
- Informing investigative leads.
- Involving relevant aspects of the crime environment.
- Targeting criminal offenders and organized criminal activities.
- Ensuring that collection is directed according to appropriate legal and policy requirements.
- Applying irregular threat forces of crime to support their organizations and operations.
- Using collusion among criminal networks, irregular threat networks, and nation-state governments.

IDENTIFY COLLECTION ASSETS

2-19. Identifying and evaluating potential collection assets are critical to creating a feasible collection plan. Potential collection assets should be evaluated for availability, capability, and reliability. Planners balance the requirements that must be fulfilled with available collection assets to achieve collection objectives. The commander or provost marshal, supported by the operations staff, selects collection assets based on their capabilities and limitations.

2-20. Military police and USACIDC personnel are trained collectors and are highly adaptable to any collection plan. They operate in direct contact with the local population and government authorities, allowing them to identify, assess, and interact with potential sources of information. Military police personnel can effectively collect information as a deliberate collection task or in concurrence with the conduct of other missions. 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 environments and 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 ground combat.

SPECIFY COLLECTION TASKS

2-21. Military police planners specify the tasks to be performed by military police collection assets to achieve desired collection objectives. Military police collection assets are typically assigned multiple tasks during the course of a mission. It is imperative that these tasks be prioritized based on the mission, intelligence requirements, and available time. Appropriate tasking orders or support are issued to request collection assets or a capability beyond those organic to the initiating command. Tasking orders or requests should specify—

- **Collection objectives.** Establish the ends that the collection effort is meant to achieve.
- **Collection tasks.** Generate specified tasks that establish where to look (named areas of interest), who to look for (identities to be included in local biometric watch lists), what tasks must be performed, and PIR with indicators.
- **Start and termination times.** Identify the duration of collection efforts or the specific hot times that surveillance is required.
- **Adjacent units.** Locate and know activities of other elements operating in the area of operations.
- **Special support.** Identify and coordinate for linguists or special skills personnel (civilians or HN police, engineers, special forces, military information support operations personnel, civil affairs personnel, military intelligence personnel, reconnaissance assets).
- **Special reporting procedures.** Prepare additional instructions not already covered by unit standard operating procedures (to whom, how often, what frequency net to use).
- **Additional details.** Collect and analyze other necessary information bearing on operations in the area of operations.

> ***Note.*** The Army's primary information collection tasks are reconnaissance, surveillance, security operations, and intelligence operations. This manual refers to collection tasks performed by individual military police patrols and formations. They are employed to perform aspects of the primary collection tasks through policing means and other tasks not inherent in the primary tasks that military police routinely perform that enable them to passively collect police information.

ADDITIONAL PLANNING CONSIDERATIONS

2-22. Depending on the circumstances and the level of control the commander and staff determine is necessary to accomplish the mission or achieve the desired results, commanders may vary the command emphasis toward mission command or detailed command approaches. When following mission command, planners guide military police collection efforts by providing collection objectives, assigning collection assets, and dictating collection tasks to be accomplished by tasked elements. The tasked element is responsible for determining how to perform the tasks and meet the objectives assigned. When the circumstances call for more detailed command, planners may specify how to accomplish the collection effort by providing greater detail and direction in the tasking order.

2-23. Typically, the higher the level of command, the more the information collection plan will approach mission command. Military police planners operating at higher echelons often seek to employ a wide range of military police collection capabilities across an entire jurisdiction or operational area to fulfill operational information requirements. At the lower levels of command, the information collection plan may approach the detailed command when specific techniques or technical procedures are required to accomplish the information collection mission. Military police leaders and USACIDC special agents at the company level and below often follow a more detailed approach by dictating the time, duration, locations, and methods employed to achieve the desired results. See ADRP 6-0 for a greater discussion of the differences between mission command and detailed command approaches.

2-24. Before directing the employment of military police collection assets, planners consider the following and adjust planning as necessary to ensure that the effective execution of the collection effort:

- **Nature of the mission.** Each information collection mission has different requirements, timeframes, rules of engagement, and other differences that may influence how information collection capabilities are employed. For instance, under the guidelines of the uniform code of military justice, law enforcement surveillance of a U.S. Soldier who is the subject of a criminal investigation differs significantly from tactical surveillance performed by an observation post in support of decisive action in an overseas operational area. Misunderstanding the nature of the mission—and the legal and policy implications—can put the commander, collection assets, and mission accomplishment at risk.

- **Rules of engagement (or rules for the use of force).** The *rules of engagement* are directives issued by competent military authority that delineate the circumstances and limitations under which U.S. forces will initiate and/or continue combat engagement with other forces encountered (JP 1-04). *Standing rules for the use of force* are preapproved directives to guide U.S. forces on the use of force during various operations (JP 3-28). Rules for the use of force are generally restrictive measures aimed at limiting the application of force to a minimum necessary to accomplish the mission. These considerations are critical to planning and may significantly limit when, where, or what techniques, methods, or tasks may be performed to accomplish police information collection. See AR 190-14 for policy on the use of force by law enforcement and security personnel.
- **Impact on the population and public opinion.** Sometimes a task or method employed to successfully achieve a tactical result can produce unanticipated strategic consequences. Planners consider such potential consequences before tasking collection assets to ensure that the pursuit of tactical objectives does not undermine strategic ends. For example, the use of unmanned aircraft systems may enhance tactical effectiveness, but when employed in an operational area with significant legal constraints or expectations of privacy (such as in support of DSCA or in support of partner nations overseas), such surveillance methods could achieve a tactical result at the expense of operational or strategic efforts. See FM 3-39 for ways in which military police can build trust, legitimacy, and public support.
- **Need for operations security.** *Operations security* is a capability that identifies and controls critical information, indicators of friendly force actions attendant to military operations and incorporates countermeasures to reduce the risk of an adversary exploiting vulnerabilities (JP 3-13.3). Military police staffs balance the need for information with the need to avoid revealing intentions by conducting police information collection. Operations security may dictate the selection of assets (such as a covert law enforcement asset instead of overt) or dictate the need for passive rather than active collection methods to gather information without triggering a negative response from the targeted population. Additionally, military police consider the sensitivity of law enforcement, investigative, and corrections information before sharing outside official military police channels. See ADP 3-37 for a discussion of operations security.
- **Risk to military police collection assets.** Commanders use the risk management process to assess risk and incorporate risk considerations into their guidance for police information collection. This may preclude the use of some types of assets or methods of collection. For example, a drug suppression team may conduct covert surveillance of illicit drug activities that places the collection asset at significant risk if detected or identified. See ATP 5-19 for details on risk management.
- **Available assets and time available.** The most significant planning consideration in planning and directing police information collection is the availability, capability, and limitations of military police collection assets and the time available to execute police information collection. For instance, military police responding to an active criminal incident may require immediate execution of information collection to determine the likely evasion route, identity, and location of a criminal offender and must rely on the police patrol or investigative assets available at the time. On the other hand, a series of burglaries of houses during a particular period of time may require detailed planning, identification of the most capable military police collection assets, and discrete methods of police information collection to avoid detection.

DIRECT POLICE INFORMATION COLLECTION

2-25. Military police direct collection assets through the operations process and Army planning methodologies based on the information collection plan. (See FM 3-39 for the military police application of the military decisionmaking process and troop leading procedures.) Collection assets typically consist of organic or attached military police patrols, but they may include other specialty military police personnel, such as USACIDC special agents, detention specialists, or military working dog (MWD) teams. After a thorough evaluation of the availability, capability, and disposition of the potential collection resources, the information collection plan is implemented through the execution of asset tasking. The tasking process provides the selected collection assets with prioritized requirements and directs their employment to accomplish the desired results.

2-26. Using the information collection plan as a guide, the staff must complete several important activities to achieve a fully synchronized, efficient, and effective plan. Updating information collection throughout execution is crucial to successful information collection. As military police and USACIDC leaders assign collection tasks to assets, they provide details that clearly define the collection requirements. The requirements include—

- What to collect (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).

2-27. A part of collection planning and direction includes coordination with all stakeholders before initiating 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 eliminate the duplication of effort, interference with an ongoing effort, or the violation of legal limitations. In a deployed operational environment, coordination and synchronization is conducted with the S-2/G-2. 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.

RESPONSIBILITIES

2-28. The S-3 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 intelligence requirements.
- Synchronizing military police collection efforts with the S-2/G-2 to meet intelligence requirements.
- Providing relevant background police information, police intelligence, or military intelligence to military police mission elements to improve situational awareness and cultural understanding and to facilitate 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 additional assets required to support information collection requirements (human intelligence [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.

2-29. 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 adequate understanding of information collection requirements.

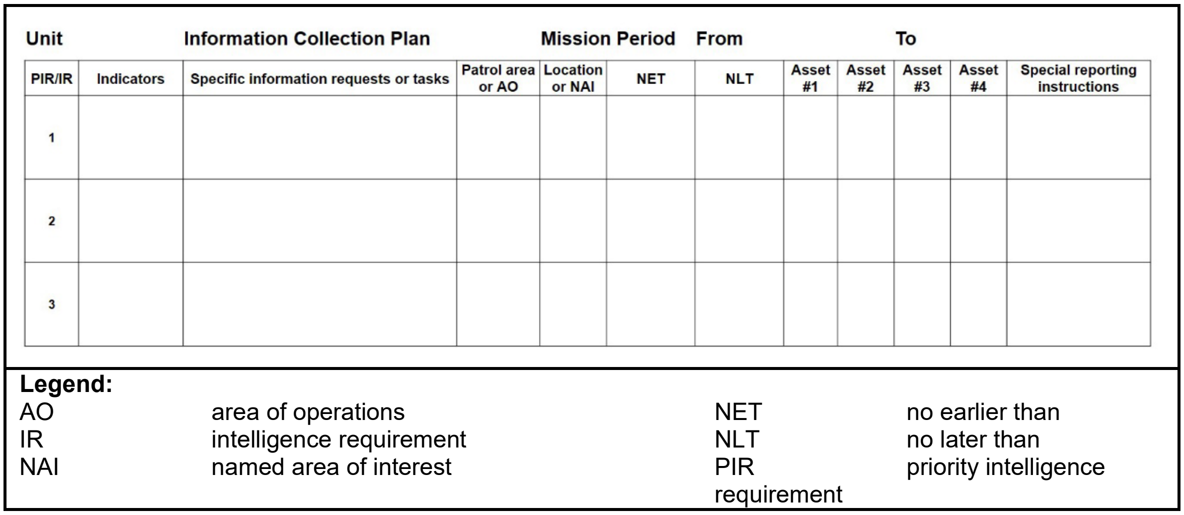
- Reviewing IPB, police intelligence products, and other available information to ensure situational understanding and situational awareness and to relay information specific to the unit area of operations to personnel in the S-3/G-3 provost marshal section and, when applicable, the S-2/G-2 to increase knowledge of the area of operations.
- Providing full support to unit PIO collection and debriefing activities and ensuring compliance with established briefing and debriefing procedures by military police elements.
- Reinforcing the importance of the procedures for immediate reporting of information of critical or time-sensitive value.

2-30. 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 adequate understanding of intelligence requirements, the information collection plan, 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, 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 processing and carefully compiling written reports during military police missions.

Information Collection Plan

2-31. Military police commanders and staffs use several variations of tools and techniques to direct information collection. Regardless of the format and methods used, the tools that military police use to translate the commander's intent into information collection actions to fulfill the desired end state may be considered an information collection plan. Figure 2-5 provides an example of an information collection plan that military police may use to manage information collection assets or to contribute to the overall information collection effort. Additional examples and formats for information collection can be found in FM 3-55.



Unit Information Collection Plan Mission Period From To

PIR/IR	Indicators	Specific information requests or tasks	Patrol area or AO	Location or NAI	NET	NLT	Asset #1	Asset #2	Asset #3	Asset #4	Special reporting instructions
1											
2											
3											

Legend:

AO	area of operations	NET	no earlier than
IR	intelligence requirement	NLT	no later than
NAI	named area of interest	PIR	priority intelligence requirement

Figure 2-5. Example of an information collection plan for a military police unit

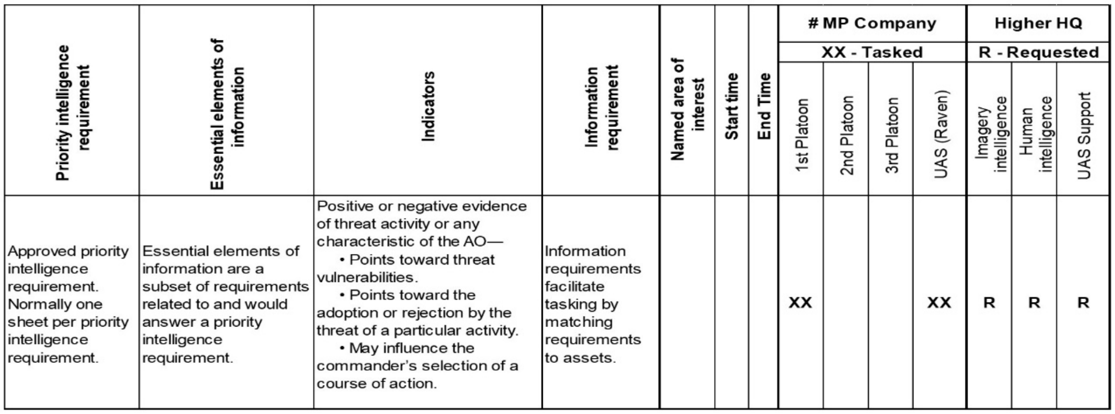
Operations Order

2-32. Annex L of an operations order contains the overall information collection plan to support the concept of operation. The information collection annex clearly describes how information collection activities support the conduct of offensive, defensive, and stability or DSCA tasks described in an operations order. It synchronizes activities in time, space, and purpose to achieve objectives and accomplish the commander's intent for reconnaissance, surveillance, and intelligence operations. When military police provide support to the Army operations process, they contribute to the development of annex L by recommending collection priorities and describing military police collection asset capabilities and availability for tasking. See ADRP 5-0 for the operations process and FM 6-0 for details on orders production.

INFORMATION COLLECTION MATRIX

2-33. When military police commanders and staffs must coordinate with external elements to meet information and intelligence requirements, they may use an information collection matrix to synchronize internal and external collection assets or use their contributions to meet the CCIRs. Figure 2-6 shows a potential information collection matrix used by a military police company. See FM 3-55 for additional information on collection matrix examples.

> ***Note.*** Apart from tracking internal information collection efforts, military police often contribute to the overall information collection plan of a supported unit. When supporting Army operations, military police units seek to nest their planning and tracking processes with supported organization formats and reporting procedures to ensure standardization and synchronization.



							# MP Company				Higher HQ		
							XX - Tasked				R - Requested		
Priority intelligence requirement	Essential elements of information	Indicators	Information requirement	Named area of interest	Start time	End Time	1st Platoon	2nd Platoon	3rd Platoon	UAS (Raven)	Imagery intelligence	Human intelligence	UAS Support
Approved priority intelligence requirement. Normally one sheet per priority intelligence requirement.	Essential elements of information are a subset of requirements related to and would answer a priority intelligence requirement.	Positive or negative evidence of threat activity or any characteristic of the AO— • Points toward threat vulnerabilities. • Points toward the adoption or rejection by the threat of a particular activity. • May influence the commander's selection of a course of action.	Information requirements facilitate tasking by matching requirements to assets.				XX			XX	R	R	R

Legend:

AO	area of operation
HQ	headquarters
MP	military police
R	requests for collection by nonorganic assets (from organic or task organized
headquarters	intelligence staff)
UAS	unmanned aircraft system
XX-Tasked	organic assets tasked to perform collection

Figure 2-6. Example of an information collection matrix for a military police company

INFORMATION COLLECTION OVERLAY

2-34. The staff may issue an information collection overlay depicting the information collection plan in graphic form (or the staff may contribute to the development of the overall information collection plan overlay included as an appendix to annex L of an operation order). This is especially important when supporting area security in support and consolidation areas. (See FM 3-55 for additional information on information collection overlays.) Typical items on an information collection overlay include—

- Friendly boundaries and phase lines.
- Named areas of interest and target areas of interest.
- Limits of advance, limits of reconnaissance, and reconnaissance handover lines.
- Graphics depicting zone, area, or route reconnaissance.

- Route start points, release points, and checkpoints.
- Primary and alternate observation post locations and scanned sectors for sensors.
- Unmanned aircraft system flight paths.

2-35. Information collection overlays designed to support law enforcement or detention operations typically require less graphic control measures due to the limited coordination requirements within a given law enforcement jurisdiction or detention facility. Typical items on an information collection overlay supporting law enforcement may include—

- Police and prison structures.
- Jurisdiction boundaries.
- Hotspots or target areas.
- Prohibited or sensitive areas to avoid.
- Observation posts.
- Checkpoints, access control points, or special traffic control or enforcement posts.
- Mission-essential vulnerable areas.

Mission Briefings

2-36. The purpose of a mission briefing is to ensure that personnel conducting missions (where the collection of police information is likely or directed) are aware of specific information and reporting requirements, information gaps, and unique mission requirements. Mission briefings 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 staffs. These briefings also include a review of collection objectives and methods to be employed.

2-37. 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 police information and police intelligence being disseminated.

2-38. A mission briefing may be conducted as a separate presentation or, ideally, may be integrated into planned mission briefings. 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.

2-39. Planning for mission briefings requires the consideration of several key elements. Initially, the identification of the briefing audience is required (consistent with investigative requirements, operational objectives, and information dissemination restrictions). 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 mission briefing (see figure 2-7, page 2-14) should also provide criteria for reporting immediate, time-sensitive information; reporting requirements for nonpriority reporting; and reporting the location and procedures for postmission debriefings.

1. Situation.

- Enemy. Criminal and police situation update.
- Crime environment updates and indicators of criminal activity.
- Threat update (typically focused on criminal or other irregular threats).
    - Individual criminals, criminal networks, and criminal organizations operating in the area.
    - Known and potential high-threat areas and specific threats in the area.
    - Route information and current available information and intelligence.
    - Specific types of criminal threats, methods of activity, and modes of operation.
- Friendly forces Police situation update, patrol distribution, assessment guidance, troop to task.

2. Mission. Who, what, when, where, and why of the collection effort.

3. Execution. Concept of operations, objectives, methods, techniques, and tasks for police collection assets. How the commander envisions accomplishing mission with available collection assets.

4. Sustainment. Specific collection sustainment requirements.

5. Command and signal. Chain of command, radio frequencies, special communication instructions (police codes used), reporting procedures.

Special collection considerations and requirements.

- Identification of specific persons wanted for specific criminal or threat activity (BOLO, warrants, wanted persons, mission persons/ personnel recovery).
- Identification of material or information with strategic value or impact.

    Evidence collection priorities, handling, custody, and disposition procedures for collected documents, media, and other material evidence.
- Requirements for handling and disposition of detained personnel and captured material/evidence.
- Specific requirements for use of digital photography and documentation of the crime scene or site exploitation.
- Time-sensitive information relative to specific criminal activities or investigations.

Legend:

BOLO	be-on-the-lookout

Figure 2-7. Example of a mission briefing

ASSESSING COLLECTION

2-40. Before executing police information collection, the staff makes certain that mechanisms are in place and that subordinates understand reporting procedures to ensure that information obtained through collection is used effectively to enhance situational awareness or influence decision making. Unclear reporting procedures, insufficient feedback mechanisms, and a failure to update information collection planning and direction according to evolving circumstances undermine the effort and risk assumed in executing the information collection plan.

Reporting Procedures

2-41. The commander and staff establish clear reporting procedures to ensure that collected police information can be evaluated and routed properly. This enables the staff to screen reports and debriefings to determine if collection tasks have been met and to assess the following:

- **Relevance.** Does the information actually address the collection task? If not, can the staff use this information to satisfy other requirements?
- **Completeness.** Is essential information missing? Are there elements of information the military police collection asset must address or tasks that must be repeated?
- **Timeliness.** Was the information received in a timely manner? Was it collected, reported, and disseminated to appropriate channels in time to influence decisions or shape police operations?

- **Opportunities for cueing**. Can this asset or another asset take advantage of new information to increase the effectiveness and efficiency of the overall information collection effort? If the report suggests an opportunity to cue other assets, military police staff immediately cue operations and intelligence staff for potential adjustments to the overall information collection plan.

Feedback Mechanism

2-42. Military police planners ensure that planning and directing police information collection includes a feedback mechanism to deliver necessary feedback from collection assets to planners. This allows planners to assess collection effectiveness. When necessary, such feedback may identify ways to modify or improve the collection effort and determine if collection tasks or objectives must be modified or updated.

2-43. Feedback is essential to maintain information collection effectiveness and alert leaders of deficiencies to correct. By monitoring operations, correlating reports to requirements, screening reports, and providing feedback, the staff ensures the most effective employment of military police collection assets.

2-44. As the operation continues, military police planners track the status of each collection task, analyze reporting, and satisfy requirements. They pay particular attention to assets not producing required results, which may trigger adjustments to the information collection plan. The staff assesses the value of the information from collection assets and develops or refines requirements to satisfy information gaps.

2-45. When reporting satisfies a requirement, the staff relieves the collection assets of further responsibility to collect against information collection tasks related to the satisfied requirement. The operations officer, in coordination with the staff, provides additional tasks to satisfy emerging requirements. The operations staff informs—

- The collection assets of the partially satisfied requirements to continue collection against, the collection tasks that remain outstanding, and what remains to be done to fulfill those requirements.
- The collection assets that are assigned new tasks designed to exploit opportunities or respond to changes in the situation.

Adjusting the Information Collection Plan

2-46. Building assessment and feedback mechanisms into the information collection plan allows military police the ability to adjust the information collection plan as necessary to ensure that military police collection efforts remain effective in accomplishing assigned collection tasks, continue to support collection objectives, and advance the effort toward achieving the commander's intent and desired end state. As the situation changes, staffs adjust the information collection plan to synchronize collection tasks. This optimizes collection capabilities. The staff constantly updates requirements to ensure that information-gathering efforts synchronize with current operations and support future operations planning. As collected information answers requirements, the staff updates the information collection plan.

2-47. Updating the information collection plan includes—

- Maintaining information collection activities synchronized to operations.
- Cuing assets to other collection requirements.
- Eliminating satisfied requirements.
- Developing and adding new requirements.
- Retasking assets.
- Transitioning to the next operation.

2-48. Each action requires collaboration among the staff. In military police organizations, the operations and intelligence staff work together to modify the information collection plan. In brigade combat teams and echelons above brigade, military police staff support the intelligence staff during continuous planning requirements and assessing the collection of military police collection assets. See ATP 2-01 for further details on planning requirements and assessing collection.

This page intentionally left blank.

Chapter 3

Collect and Process

This chapter describes step two of the PIO framework: collect and process. This step focuses on providing timely and relevant police information to produce police intelligence products that influence current and future operations. This chapter begins by reviewing the roles and authorities of military police to collect police information. Next, it describes how military police collection assets collect and process police information by using diverse methods, sources, and techniques.

COLLECTION ROLES AND AUTHORITIES

3-1. *Information collection* is an activity that synchronizes and integrates the planning and employment of sensors and assets as well as the processing, exploitation, and dissemination systems in direct support of current and future operations (FM 3-55). Police information collection consists of activities conducted during military police operations that may be used to drive police, detention, investigative, and security and mobility support mission planning. Collected police information may also be fed into the integrating processes as a component of the commander's overall information collection effort.

3-2. During police information collection, it is important for military police to be cognizant of the inherent roles, authorities, and limitations of collection during police operations, detention operations, and security and mobility support. In general, military police and USACIDC personnel are authorized to collect information related to law enforcement. However, for criminal investigative purposes, there are significant limitations on traditional military intelligence personnel collecting such information except as authorized by applicable laws and regulations. Collection on U.S. persons implicates many legal considerations and restrictions. Judge advocates should be consulted during the planning and collection of police information to ensure adherence to legal requirements.

3-3. PIO conducted in support bases and base camps in the United States and its territories must be conducted within legal and policy restrictions. 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 (an offense that has been committed or evidence which indicates that a crime that has a military connection may be committed) exists. 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 military intelligence personnel or military police during unified land operations outside the continental United States that deal with non-U.S. persons.

3-4. The collection and management of police information are enabled by, and subject to, laws, regulations, and policies. These documents ensure the proper conduct of PIO. Although restrictions may be present in an operational area where police collection assets seek to collect information on individuals other than U.S. persons, the ability to collect and share police information in such environments is generally less restrictive. Restrictions and guidance regarding the collection of police information are described in the references listed in table 3-1, page 3-2. See appendix A for detailed descriptions of the most relevant references and their applicability to PIO.

Table 3-1. Regulation, policy, and laws relevant to police information collection

- AR 190-5
- AR 190-24
- AR 190-30
- AR 190-45
- AR 190-47
- AR 190-53
- AR 195-2
- AR 380-13
- AR 381-10
- AR 381-12
- AR 525-13

- EO 12333
- DODD 2310.1E
- DODD 3025.18
- DODD 5200.27
- DODD 5240.01
- DODI 2000.12
- DODI 3025.21
- DODI 5505.17
- DODI 5525.18

- U.S. Code Titles 10, 18, 22, 32, and 50
- 28 CFR Part 23 (criminal intelligence)
- 18 USC 1385 (*Posse Comitatus*)
- MCM (UCMJ)/AR 27-10
- U.S.-host nation agreements/SOFA
- DOD Law of War Manual/FM 27-10
- International treaties, such as the Hague Convention (1899 and 1907), the Geneva Convention (1949), and Protocol I to the Geneva Convention (1977)

Legend:

AR	Army regulation	FM	field manual
CFR	Code of Federal Regulations	MCM	Manual for Courts-Martial
DOD	Depart of Defense	SOFA	status-of-forces agreement
DODD	Department of Defense directive	UCMJ	Uniform Code of Military Justice
DODI	Department of Defense instruction	U.S.	United States
		USC	United States code
EO	executive order		

3-5. Military police Soldiers and USACIDC special agents are the primary collectors of police information. Military police collect police information while conducting tasks across the three military police disciplines:

- **Police operations.** Military police collect police information while conducting police operations, which includes—
  - Law enforcement.
  - Criminal investigations.
  - Forensic analysis and biometric identification support.
  - Customs support.
  - Support to civil security and civil control.
  - Traffic management and enforcement.
  - Civil disturbance control.
  - Police engagement.
  - Support to civil law enforcement.
  - Evidence response team support.
- **Detention operations.** Military police collect police information while conducting detention operations, which includes—
  - U.S. military prisoner confinement.
  - Detainee operations.
  - Host-nation corrections training and support.
- **Security and mobility support.** Military police collect police information while conducting security and mobility support, which includes—
  - Support to mobility.
  - Area security.
  - Reconnaissance and surveillance.
  - Antiterrorism support.
  - Physical security.
  - MWD support.

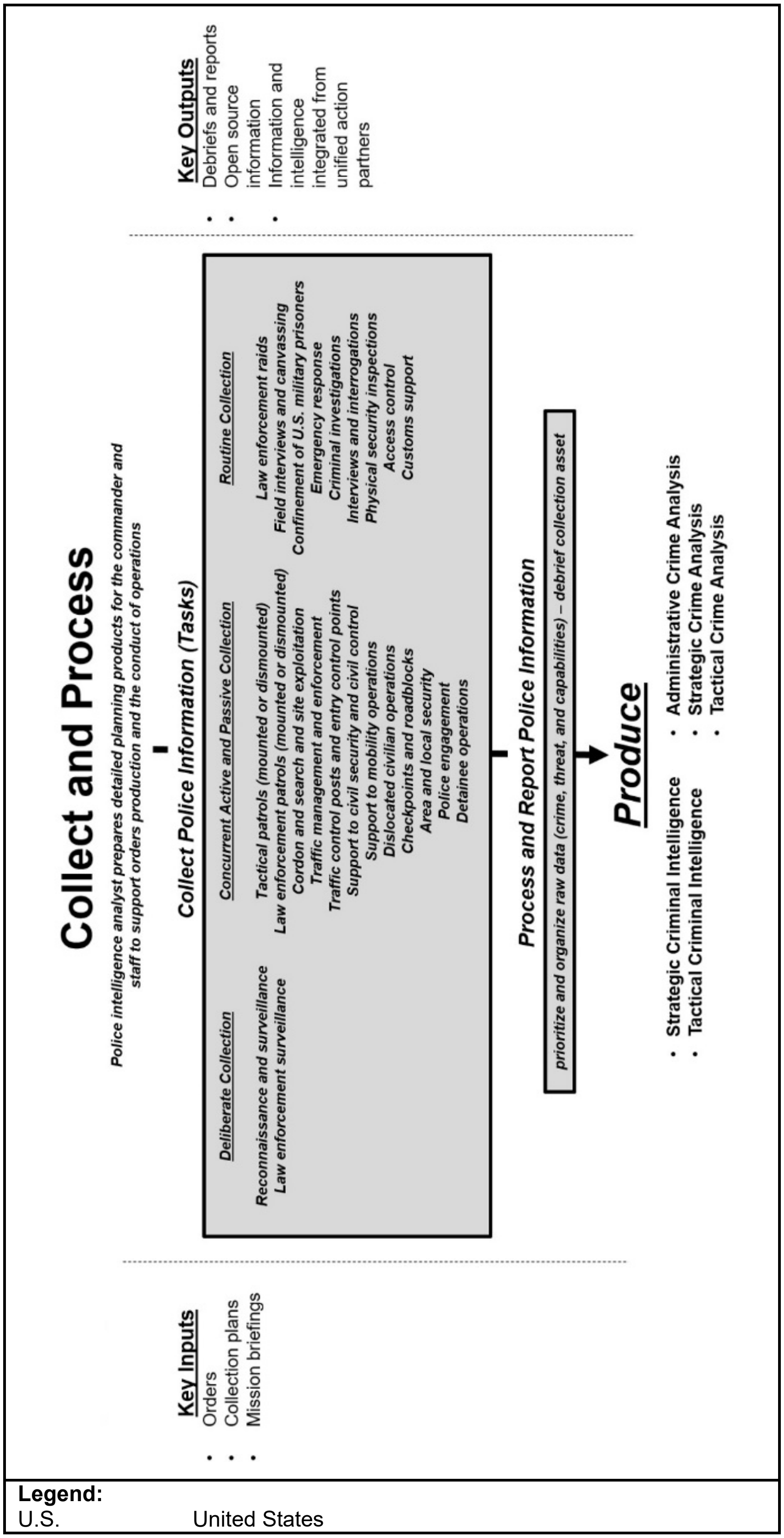
    - Support to populace.
    - Resources control.
    - Logistics security.

3-6. Besides police information collected directly through the conduct of military police operations, military police collection assets also receive information from interaction and coordination with unified action partners, including—

- Higher echelon S-2/G-2 personnel.
- Military information support operations units.
- Host-nation police.
- Domestic law enforcement agencies.
- Joint and multinational partners.
- The staff judge advocate.
- Higher echelon battalion or brigade civil affairs operations staff officer (S-9)/assistant chief of staff, civil affairs operations (G-9) personnel.
- The civil-military operations center.
- Civil affairs teams.
- Force protection officers.

3-7. As necessary, information obtained from unified action partners is assessed for apparent or intuitive links, connections, or associations with other police information to integrate multiple sources into the criminal and crime analysis process while adhering to legal and policy guidelines regarding the use of such information, depending on the operational environment in which military police are operating.

3-8. A primary concern of military police and USACIDC personnel collecting police information across the military police disciplines is abiding by constitutional, legal, and regulatory requirements to protect the rights and privacy of those subject to criminal investigation, apprehension, or confinement. This emphasis places significant responsibilities on those authorities overseeing police information collection, storage, and dissemination to protect privacy and rights and to prevent violations of U.S laws and regulations pertaining to military intelligence collection against U.S. persons. See appendix A for further details regarding the authority to collect information against U.S. persons for law enforcement and criminal investigative purposes. Figure 3-1, page 3-4, depicts the collect and process step of PIO.


Key Inputs
• Orders
• Collection plans
• Mission briefings
Collect and Process
Police intelligence analyst prepares detailed planning products for the commander and staff to support orders production and the conduct of operations
Collect Police Information (Tasks)
Deliberate Collection
Reconnaissance and surveillance
Law enforcement surveillance
Concurrent Active and Passive Collection
Tactical patrols (mounted or dismounted)
Law enforcement patrols (mounted or dismounted)
Cordon and search and site exploitation
Traffic management and enforcement
Traffic control posts and entry control points
Support to civil security and civil control
Support to mobility operations
Dislocated civilian operations
Checkpoints and roadblocks
Area and local security
Police engagement
Detainee operations
Routine Collection
Law enforcement raids
Field interviews and canvassing
Confinement of U.S. military prisoners
Emergency response
Criminal investigations
Interviews and interrogations
Physical security inspections
Access control
Customs support
Process and Report Police Information
prioritize and organize raw data (crime, threat, and capabilities) – debrief collection asset
Produce
• Strategic Criminal Intelligence
• Tactical Criminal Intelligence
• Administrative Crime Analysis
• Strategic Crime Analysis
• Tactical Crime Analysis
Key Outputs
• Debriefs and reports
• Open source information
• Information and intelligence integrated from unified action partners

Legend:	
U.S.	United States

Figure 3-1. Collect and process police information

COLLECT POLICE INFORMATION

3-9. Police information collection follows the collection tasks established by the information collection plan. A successful information collection effort results in the timely collection, processing, and reporting of relevant and accurate information, which supports the analysis, production, and dissemination of police intelligence products. To be effective, collection efforts follow the operations process as collection assets plan, prepare, execute, and assess collection. The collection efforts must remain focused on achieving the objectives established by the information collection plan to ensure that the effort and risk assumed by collection assets are balanced by the collection efforts and their contributions to fulfilling the CCIR, intelligence requirements, or investigative requirements. See FM 3-55 for an additional discussion of information collection techniques and activities.

3-10. Collected police information focuses on the aspects of the operational environment that are causing or are influencing crime, disorder, and the fear of crime within a population. This step (along with the plan and direct step) corresponds to the scanning step in the scanning, analysis, response, and assessment model. Within the scanning, analysis, response, and assessment model, this process focuses attention on collecting police information through a myriad of methods to understand and develop effective policing responses to specific crime problems within the operational environment.

3-11. As military police collect police information, they must constantly assess the reliability of the information collected. This is discussed in greater detail below as police intelligence analysts evaluate collected police information for value, reliability, and credibility. It is important for military police collection assets to remember that they are collecting police information because it can shape awareness of potential problems with the sources of police information early in the analysis process and may shape the methods and techniques that military police employ to obtain the most accurate information possible. For example, awareness of a person's suspicious behavior or indicators of deception may lead to follow-up questions of a witness, victim, or subject during a field interview that may produce additional police information. This awareness is especially critical when dealing with individuals providing information, regardless of the operational environments.

3-12. 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 (real or perceived) to slight, hurt, or anger them. These are not all-inclusive of the possible factors that may motivate people to come forward with information to police personnel.

3-13. 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 previously mentioned 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 defeated, civil violence, or natural disasters. In these examples, victims may see the United States as a liberating or humanitarian force. 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. Some may hope for money or material support. In all environments and circumstances, military police collection assets 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

3-14. Police information can be collected through active or passive collection efforts during the conduct of military police operations. Passive or routine collection is the compiling of data or information gathered while engaged in routine policing, detention, and security and mobility support missions. During passive collection, military police personnel are not on a dedicated reconnaissance, assessment, or collection mission. Passive collection occurs every time military police engage with or observe the people with whom, or the environment in which they operate. Examples of passive collection include establishing rapport with the local population by implementing and maintaining contact; maintaining efforts to clarify and verify information already obtained through observations or other means; or observing activity, a lack of activity, or other variations from the norm.

3-15. 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 they may be linked directly to specific criminal investigations. This required information is generally briefed to military police forces as part of their patrol or mission briefing before mission execution.

3-16. Military police typically do not perform active or passive collection in isolation, but they often perform concurrent collection that combines active and passive methods. In concurrent collection, military police are assigned deliberate collection tasks as part of another tactical task to accomplish. Military police perform the tactical tasks and collect the police information necessary to support and implement into the intelligence requirements. In addition to those collection tasks specified in a mission order or brief, military police employ passive collection to gather information that may not be specified but is important to understand, such as aspects of the crime environment or criminal activity. For instance, a military police patrol is tasked to establish a traffic control post to control traffic along a main supply route to ensure freedom of movement for friendly forces. Within the mission order to perform this task, the CCIR provide the military police patrol PIR and FFIR to deliberately collect while the patrol also pays attention to other indicators within the operational environment that may be relevant to decision makers or police effectiveness.

3-17. Collection is integrated throughout all military police operations. During the conduct of military operations, military police patrols and specialty military police collection assets are arrayed across the area of operations to perform a variety of policing, detention, security, and mobility tasks. Military police collect information as a deliberate collection task or concurrent with the conduct of other military police missions or tasks. Police information can be collected actively through direct observation and engagement with targeted personnel or passively by observing and listening to the surrounding environment and the interactions of people. Due to the methods that military police employ and the policing focus on countering crime and criminal actors, military police provide a unique collection capability that generates police information for criminal and crime analysis and for immediate dissemination to relevant unified action partners to support situational awareness, protection efforts, and decision-making processes.

Police Information Collection Tasks and Sources

3-18. The development of a viable information collection plan, including the management and supervision of collection tasks and sources, is critical to successful police information collection. Military police, USACIDC, or other police collection assets collect information and data about criminal or other irregular threats and police systems, infrastructure, processes, capabilities, and resources. Collection may also target and answer intelligence requirements concerning environmental and geographic characteristics, cultural and ethnic norms, formal and informal authority structures, and other factors affecting policing activities and the crime environment. Successful PIO is dependent on the execution of collection tasks to generate timely, relevant, and accurate police information.

3-19. Military police Soldiers operate throughout the area of operations during the execution of military police operations. The diverse tasks that military police perform often put them in advantageous places across the area of operations to collect information from a variety of sources. This section discusses several of the most common tasks that military police use to collect police information. This does not preclude collection by other means. These common collection tasks and sources are—

- Reconnaissance, surveillance, and assessments (technical and threat assessments).
- Military police patrols.
- Cordon and search and law enforcement raids.
- Site exploitation and evidence collection.
- Forensic analysis and biometric identification support.
- Law enforcement investigations (criminal and collision [traffic accident] investigations).
- Interviews and law enforcement interrogations.

- Police engagement with populations, community leaders, unified action partners, informants, and law enforcement sources.
- Traffic management and enforcement.
- Physical security and access control.
- MWD support.
- Detention operations (confinement of U.S. military prisoners and detainee operations).
- Dislocated civilian operations.
- Data mining, database queries (law enforcement and intelligence), reachback (such as the Defense Forensic Science Center), and open-source data reviews.

3-20. Military police obtain police information from a myriad of sources during the execution of military police operations. The versatility of military police and their dispersion across the area of operations enable them to engage diverse populations to obtain the information needed to answer information and intelligence requirements related to crime, disorder, fear of crime, destabilizing factors, and police effectiveness in providing safe and secure environments. These sources of police information are essential to developing a clear picture of the networks, trends, patterns, and associations that are critical to combating criminal and other irregular threats. Sources of police information also allow military police to identify and mitigate organizational, system, and infrastructure shortfalls affecting police, detention, and investigative missions.

3-21. Military police and USACIDC special agents collect and analyze information in response to requests for information, reviews of records and reports, assessments and inspections, complaints, criminal statistics, incidents, inquiries, biometric data, forensic evidence, and surveys of police and criminal environments. USACIDC specifically leverages access, networks, and expertise to obtain information from the following specific sources:

- The Combating Terrorism Program, as outlined in AR 525-13.
- Law enforcement agencies.
- Intelligence agencies.
- Personal security vulnerability assessments.
- Criminal threat analysis.
- Logistics security threat assessments.
- Criminal investigations.
- Interviews and law enforcement interrogations.

Military Police Reconnaissance, Surveillance, and Assessment

3-22. Military police reconnaissance, surveillance, and assessment assists in collecting police information required to enhance situational understanding; plans, prepares, executes, and assesses missions in support of decisive action; and compiles the critical information and evidence required to prosecute criminal offenders. Military police reconnaissance efforts conducted early in an operation establish the baseline of knowledge and understanding required to perform subsequent missions. Military police focus reconnaissance on understanding crime environments, police and detention capabilities, and destabilizing elements within society to support U.S. force stability operations and efforts to consolidate gains following large-scale ground combat. This specialized policing focus enhances the ability of U.S. forces and unified action partners to achieve objectives focused on building the HN police and corrections institutions necessary for an effective criminal justice system under the rule of law.

3-23. *Reconnaissance* is a mission undertaken to obtain, by visual observation or other detection methods, information about the activities and resources of an enemy or adversary, or to secure data concerning the meteorological, hydrographic, or geographic characteristics of a particular area (JP 2-0). *Surveillance* is the systematic observation of aerospace, cyberspace, surface or subsurface areas, places, persons, or things by visual, aural, electronic, photographic, or other means (JP 3-0).

3-24. While surveillance is considered part of reconnaissance, a key difference between surveillance and reconnaissance missions is that surveillance is systematic, is usually passive in information collection, and may be continuous. Reconnaissance is typically more limited to the duration of an assigned mission, is active in information collection of information, and usually includes human participation rather than purely technical means. Reconnaissance is a focused collection effort that employs many tactics, techniques, and procedures throughout the course of the mission, one of which may include an extended period of surveillance. See FM 3-90-2 for an additional discussion of reconnaissance in greater detail.

3-25. Military police employ reconnaissance, surveillance, and assessment capabilities as the primary means to perform deliberate information collection. When performing reconnaissance in tactical environments, military police primarily focus on determining the presence of criminal, terrorist, or other irregular threats in an area of operations. Reconnaissance tasks are typically completed by military police patrols trained in combat skills and policing techniques. This form of reconnaissance supports situational awareness of threats targeting main supply routes, lines of communication, and critical infrastructure in echelon support areas (bases, base camps, and command posts). Military police patrols also collect information regarding police and crime throughout an area of operations, specifically, locations of HN police stations, prison facilities, and general population attitudes toward the police. Military police reconnaissance patrols can satisfy multiple CCIRs for an area of operations and intelligence requirements specific to police infrastructure or criminal threats.

3-26. Law enforcement reconnaissance and surveillance requires specialized technical training and experience to navigate legal and policy restrictions, protect rights and privacy concerns, and employ advanced law enforcement surveillance technology. Law enforcement reconnaissance and surveillance tasks are typically performed by specially trained personnel (special reaction teams, military police investigators, USACIDC special agents). Specific types of reconnaissance, surveillance, and assessments that military police conduct across operational environments include the following:

- Reconnaissance: route, zone, and area.
- Surveillance: general surveillance, early warning, and law enforcement surveillance.
- Assessments: threat and technical.

Military Police Reconnaissance

3-27. *Route reconnaissance* is a directed effort to obtain detailed information of a specified route and all terrain from which the enemy could influence movement along that route (ADP 3-90). Military police performing route reconnaissance focus on developing an understanding the routes, trafficability, and traffic flows necessary to enable effective traffic management and enforcement and route or convoy security missions.

3-28. *Zone reconnaissance* is a form of reconnaissance that involves a directed effort to obtain detailed information on all routes, obstacles, terrain, and enemy forces within a zone defined by boundaries (ADP 3-90). A zone reconnaissance may include several routes or area reconnaissance missions assigned to subordinate units. Typically, military police conduct zone reconnaissance when they first move into a new area of operations or law enforcement jurisdiction to gain an understanding of the critical locations (key police and corrections infrastructure, ingress and egress routes for potential criminal actors, and general routes, terrain features, critical locations to enable rapid emergency or response forces).

3-29. *Area reconnaissance* is a form of reconnaissance that focuses on obtaining detailed information about the terrain or enemy activity within a prescribed area (ADP 3-90). The area may consist of a single point, such as a house, where criminal activity is suspected or of an area, such as the immediate area surrounding a HN police station. Because the area is smaller, an area reconnaissance typically takes less time to complete than zone reconnaissance. Area reconnaissance is the most common technique employed by military police because it supports specific mission planning and focuses on the specific places where crimes have occurred or are likely to occur or where crime-conducive places presenting opportunities for criminals to exploit.

Military Police Surveillance

3-30. General surveillance employs multiple forms of sensors to develop the general understanding of crime environments and criminal threats. This may include dispersed surveillance cameras or sensors at locations across an area of operations or jurisdiction. General surveillance at places such as transportation hubs, recreational facilities, parking lots, barracks, financial institutions, markets or commercial establishments, and other commonly transited locations provide general deterrence of criminal activity. Such general surveillance also supports crime analysis following the commission of crimes to determine who, what, when, and where crime or crime patterns occur to support the investigation and prosecution of a specific crime or enhance crime prevention efforts to reduce the attractiveness of a place to criminal activity.

3-31. Early warning employs sensors in positions or locations likely to attract criminal activity or other threats. These sensors deter crime, monitor criminal activity, and create video evidence for the prosecution of crimes. The most common places for early warning sensors are checkpoints and entry control points, critical sites, controlled access facilities, and other places requiring technical physical security measures to protect critical property or assets. Early warning surveillance is critical to performing military police tasks, (crime prevention, physical security, antiterrorism, base and base camp defense, critical asset security, the enablement of timely and effective emergency response).

3-32. Law enforcement surveillance involves the employment of sensors, surveillance personnel, and technology to observe specific criminal or threat targets and to gather required police information. Law enforcement surveillance may be required to confirm suspected criminal activity, attribute suspected criminals to a specific time and place, or confirm associations between persons, groups, or entities. Surveillance may be physical observation of a person or place, visual surveillance by remote video equipment, or audio surveillance via a myriad of technologies employed to intercept audio evidence. Law enforcement surveillance is typically associated with specific criminal investigations or the production of criminal intelligence. However, law enforcement surveillance may also be performed to conduct assessments (traffic studies, physical security assessments, other security and protection requirements). See AR 190-53 and ATP 3-39.12 for details on law enforcement surveillance.

3-33. In an operational area, military police may be tasked to conduct surveillance of specific populations, locations, or facilities to satisfy CCIR that have been identified and disseminated through the operations process. Military police units conduct surveillance to gain information to help guard against unexpected threat attacks in an area of operations or to gain information critical to understanding, planning, and executing missions in support of decisive action. When surveillance is required in populated areas, military police patrols may be more acceptable collection assets because military police are perceived as a law enforcement organization rather than solely as a combat element.

3-34. Commanders and staffs must fully understand the capabilities and limitations of available military police assets. This prevents collection asset tasking that does not match capability at a particular echelon or organization. Some reconnaissance and surveillance requirements demand special equipment, training, or expertise to complete the mission successfully. This may require specific requests for technical capabilities not present in baseline military police organizations. Understanding the capabilities and limitations of various military police organizations is critical to planning and requesting the appropriate echelon and type of military police technical capability to meet mission requirements. See FM 3-39 for additional information on different military police organizations and their technical capabilities.

Military Police Assessments

3-35. Military police assessments conducted early in an operation greatly enhance efforts to consolidate gains during later phases by establishing a baseline knowledge and understanding of crime environments, criminal threats, and police and corrections institutions responsible for deterring crime and controlling criminal populations. Military police and USACIDC support situational understanding by providing the following assessment capabilities:

- 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.

3-36. Threat assessments integrate criminal threat analysis with criticality and vulnerability assessments required for the prioritization of assets by commanders and provost marshals to counter threat activities and associated risks. Vulnerability and criticality information helps police intelligence analysts 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 and interests or indirect threats that can disrupt operations. Threat analysis 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.

3-37. Technical assessments help leverage the unique professional skills that military police and USACIDC personnel possess in the core competencies of policing, corrections/investigations. This expert professional knowledge in two (policing and corrections/investigations) of the three pillars of the criminal justice sector (judicial being the third) provide commanders and staffs vital collection capabilities to understand police and prison institutions present in an operational area. Such technical policing, corrections, and investigative-focused assessments provide expert knowledge while evaluating the crime environment, police and prison infrastructure, systems, personnel, training, manning, and capabilities and capacities of police and prison institutions to enforce the law and control criminal populations. See FM 3-39 for a full listing of military police and USACIDC elements and for additional information on their specific technical capabilities that may be leveraged to support technical assessments.

Military Police Patrols

3-38. Typically, military police patrols are arrayed across the area of operations during the conduct of their assigned missions across the military police disciplines. The dispersion of military police patrols (single teams, law enforcement units, or squad- or platoon-size elements) makes them effective collection assets. Observation and evaluation skills are inherent in police training, which further enhances the capabilities of military police patrols to contribute to the collection effort in support of PIO and other requirements.

3-39. Military police Soldiers regularly observe and interact with the people and environments in which they operate. This regular contact and interaction with the population and environment make military police patrols effective in concurrent 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 information and intelligence requirements applicable to the entire area of operations or discover information that was not requested but has recognized value. That information is provided to commanders and staffs, along with the contextual details and circumstances of the discovery.

3-40. Military police patrols use several patrol methods. These various patrol methods allow military police to adapt and employ the best method to effectively collect police information based on the circumstances. When operating in a densely populated area (urban environment or special event), military police may opt for a foot or dismounted patrol to enable direct interaction, observation, and police engagement with populations that may report relevant information about crime or criminal threats. In circumstances with a rapidly developing situation for which gaining information requires mobility (combat or active-shooter situation), military police may opt for the greater mobility, communication, and protection offered by vehicle or mounted patrols. The versatility to adjust patrol methods rapidly to effectively meet information collection requirements makes military police ideal collection assets to employ in uncertain, dynamic, and rapidly evolving situations. See ATP 3-39.10 for additional details on patrol methods.

3-41. Military police patrols are often directed to conduct a deliberate collection mission to obtain specific information about an area or target. These requests are tied to a commander's PIR, the provost marshal's intelligence requirements regarding the area of operations, or specific police investigations. Intelligence requirements are generally briefed to military police Soldiers as part of their patrol briefs before mission execution. Deliberate preparation, specifically for the mission, is required. Postmission debriefs are critical to ensure that information collected by military police patrols is received by the appropriate staff elements for timely analysis and dissemination.

Cordon and Search and Law Enforcement Searches and Raids

3-42. *Cordon and search* is a technique of conducting a movement to contact that involves isolating a target area and searching suspected locations within that target area to capture or destroy possible enemy forces and contraband (FM 3-90-1). Cordon and search operations take place throughout the range of military operations. Commanders conducting a cordon and search organize their units into four elements—command, security, search or assault, and support. The security element must be large enough to establish an inner and outer cordon around the target area of the search. See FM 3-90-1 for additional information on cordon and search operations.

3-43. In operational areas, military police typically conduct cordon and search at the company level and below when performing area security tasks. Information, documents, media, other material or observations, and detainees obtained during cordon and search provide relevant police information for immediate dissemination (time-sensitive) or for use during criminal and crime analysis to produce police intelligence. The police information obtained during cordon and search operations is critical to effectively disrupting criminal activity, furthering investigations, and providing evidence for use in prosecution under the rule of law.

3-44. Maneuver formations typically conduct cordon and search at the maneuver battalion level and below. Military police attached or supporting maneuver commanders may provide critical assistance, typically by supporting the security or search element. Military police assets are especially valuable in providing support to the search element. Advanced technical capabilities that may be provided by military police to support combined arms cordon and search operations include evidence response teams, MWDs, detention specialists, and forensic experts. All military police Soldiers receive law enforcement training and have a greater general awareness when protecting crime scenes, collecting forensic materials, and processing evidence according to the stringent evidentiary standards that support cordon and search operations.

3-45. Law enforcement searches and raids are conducted by trained law enforcement officers (military police Soldiers, Department of the Army civilian police, and USACIDC special agents). Law enforcement officers execute searches to secure evidence for judicial proceedings or to recover stolen property. They execute raids to apprehend offenders, obtain evidence of illegal activity, or confiscate illegal weapons and contraband. Due to the inherent danger of high-risk searches and raids, investigative units often request special reaction team support in the execution of such missions. Special reaction teams are suited for high-risk law enforcement raids in high-threat environments. See ATP 3-39.11 for additional information on special reaction teams and law enforcement raids.

3-46. Law enforcement searches entail more than simply locating evidence or criminal subjects. They require procedures that preserve the legality of the search and present the best possible case for a prosecutor. To conduct a search, law enforcement may need a search authorization or warrant supported by a finding of probable cause that the person, property, or evidence sought after are located in the place or area to be searched. A search authorization is express permission issued by a competent military authority; a search warrant is issued by a competent civil authority to search and/or seize a person, property, or evidence. Failure to execute a search properly, or without authority, may result in the loss or inadmissibility of any evidence collected in a court-martial or in a federal judicial proceeding under the exclusionary rule. Evidence derived from an exploitation of an illegal act may also be inadmissible under the Fruit of the Poisonous Tree doctrine. Military police performing a law enforcement search must exert every effort to remain within the scope and limitations outlined in the search authorization or they risk undermining the value of the police information or evidence obtained. See ATP 3-39.10 for additional details on search and seizure during police operations.

3-47. Law enforcement raids are used to execute searches or apprehensions when numerous subjects are involved or when there is a potential for a high degree of resistance. Requests for special reaction team support for raids usually occur in conjunction with ongoing law enforcement activities by USACIDC special agents who are skilled in conducting raids and apprehensions and are familiar with evidence collection and preservation. Law enforcement raids often result in an abundance of police information collected through active and passive methods resulting from actions and statements of an apprehended criminal subject, forensic evidence, media devices, photographic or audio recordings, and statements by witnesses or bystanders at the scene.

Site Exploitation and Evidence Collection

3-48. *Site exploitation* is the synchronized and integrated application of scientific and technological capabilities and enablers to answer information requirements, facilitate subsequent operations, and support HN rule of law (ATP 3-90.15). A site is a location designated by a commander as potentially having materiel pertinent for collection and for the positive identification of persons. Site exploitation contributes to exploitation, which in the context of information collection consists of taking full advantage of information that has been obtained for tactical, operational, or strategic purposes.

3-49. Site exploitation is guided by the information collection plan. The information collection plan enables the commander to focus assets on collecting information to answer specific information requirements. When the commander designates a site for exploitation, the staff establishes an objective and specific tactical tasks that support the information collection plan. The plan also ensures that the staff requests and integrates the necessary enablers before site exploitation. See ATP 3-90.15 for additional information on site exploitation.

3-50. Evidence collection entails collecting a wide array of physical objects, testimonies, electronic data, and analyses; it is an essential task in successful military police operations. 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. If a site is suspected to be or has been a place of detention for captured or detained personnel, investigators and evidence collectors should be aware that detained personnel often leave proof of life at their place of detention. 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 tools required to collect evidence properly. Evidence collection should be performed as a deliberate and methodical process unless the 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.

3-51. 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 trained 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 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.

3-52. The continuous growth in electronic devices (cellular telephones, digital cameras, 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 (CD/DVDs, 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 HN security forces, including manned or unmanned aircraft.

Note. Information extracted from electronic devices, photographs, video and audio recordings, and written or printed (hardcopy) documents related to law enforcement investigations can be exploited by trained digital forensic examiners assigned to USACIDC formations. If the information contained within these items does not have applicability to law enforcement investigations, the items should be forwarded to document and media exploitation teams (if allowed by appropriate laws and policy) to support intelligence analysis (see ATP 2-91.8).

3-53. 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 to the system used or to the age of the document. Word choices and spelling may provide clues to a person's background and education. Handwriting analysis may give investigators another means of identifying a specific individual.

Lists kept near the computer may be valuable because 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 documents, 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 additional information on evidence collection.

Forensic Analysis and Biometric Identification Support

3-54. Forensic analysis and biometrics identification support through numerous modalities have significantly increased the ability of USACIDC investigators and police intelligence analysts to add clarity to understanding events and to attribute individuals involved in those events. Biometrics identification tools and forensic capabilities can be significant assets used distinguish between friendly, neutral, and threat forces and to deny anonymity and impunity to criminals, terrorists, and other irregular threat actors. Forensic and biometric 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 subject'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 on bases and base camps or in support of decisive action.

3-55. Biometrics collection capabilities require—

- Approved biometrics collection devices that are capable of collecting fingerprints, iris images, and facial photographs according to DOD standards.
- Personnel who are trained on how to operate biometrics collection devices.
- Collection and storage capability and manipulation software for the comparison and analysis of biometrics samples.
- Biometrics watch list training enables the local commander to build local watch lists of high-value individuals and to enable local forces to search for national/regional/global high-value individuals in the local area of responsibility.

3-56. Forensic 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 collected materials.

Biometrics

3-57. *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 is collected and personal behavioral traits are identified for future comparison.

3-58. 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 databases. During screening, military police compare the claimed identity of a subject with the database to verify the identity, discover the identity, or enroll it as a new identity. This data includes biometrics data (fingerprints, voiceprints, facial photographs, iris images, DNA).

3-59. Military police, USACIDC personnel, and investigators, and police intelligence analysts can leverage biometrics data to develop trends, patterns, and associations between individuals. Biometrics data that results in the identification or confirmation of an individual's presence at specific times and places, and in the determination of truthfulness or deception can be extremely useful in building singular associations to linking groups, cells, or organizations. Linking biometrics data with the forensic analysis of evidence collected at the scene of a crime or an attack can assist law enforcement personnel in criminal investigations or directly feed the targeting process for commanders conducting decisive action. Coordinating with the S-2/G-2 to nominate persons of interest to the biometrics watch lists enables law enforcement personnel to expose persons of interest to global tracking and enables biometrically equipped unified action partners to positively identify persons of interest during battlefield encounters.

> ***Note.*** Biometrics data 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 or legal and policy restrictions, every effort should be made to share this data with military intelligence (see ATP 2-22.85).

Forensics

3-60. Forensics is the application of multidisciplinary scientific processes to establish facts. The collection of forensic material enables the methodical analysis of evidence to establish 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 prosecutions. Additionally, forensic analysis is used to answer CCIRs, provide situational awareness, influence criminal and crime analysis, and support other mission requirements as part of decisive action.

3-61. USACIDC supports Army forensics requirements through the Defense Forensic Science Center. The Defense Forensic Science Center facility is stationary due to the nature of the equipment required and other operational requirements. The Defense Forensic Science Center deploys forensic exploitation teams with trained examiners to support operational commanders in the field. This expeditionary capability enables timely forensic analysis across a broad range of forensic capabilities, to include latent fingerprints, toolmarks, firearms, DNA, digital forensics analysis, and explosive and drug chemistry. 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.

3-62. Forensic analysis expands the ability of police intelligence analysts to establish trends, patterns, and associations by providing scientific facts of relationships between persons, objects, or data. Criminals, terrorists, or other threat actors tend to operate in predictable ways. The analyses and comparisons of fragments left at the scenes of improvised explosive device bombings or incident sites in an area of operations can identify similarities in materials used, the construct of the trigger device, and other variables (see FM 4-30 for additional information on explosive ordnance disposal). 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 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 in developing targeting strategies.

3-63. 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 or when collecting material at an incident site. See ATP 3-39.12 for detailed information on evidence collection and preservation.

Law Enforcement Investigations

3-64. 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. 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 perpetrator, and collect and process evidence to enable a successful prosecution.

3-65. 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. Law enforcement investigations fall into two primary categories—criminal investigations and collision (traffic accident) investigations.

3-66. Military police Soldiers are trained to conduct preliminary investigations as the first law enforcement officer at the scene of a crime or traffic accident. Military police investigate incidents by identifying, collecting, and preserving potential evidence; observing physical characteristics of locations and items; and conducting interviews with potential witnesses, victims, suspects, and technical experts. Specially trained military police investigators and USACIDC special agents conduct most of the formal criminal investigations in the Army. These investigators are trained in technical investigative techniques, to include evidence identification, processing, and preservation critical to successful criminal investigations. USACIDC maintains purview over criminal cases as outlined in AR 195-2.

3-67. A collision investigation is the process of the observation, collection, and documentation of evidence (including physical measurements of objects, markings, and vehicles) and the analysis, preparation, and preservation of physical and testimonial evidence to determine the cause or causes of a collision or mishap involving a vehicle. Collision investigations are typically conducted by trained traffic management and collision investigators; however, any military police patrol may be required to conduct investigations of minor traffic incidents or to assist in major incidents or complex collision investigations.

3-68. Typically, criminal intelligence associated with criminal investigations is law enforcement-sensitive and remains within law enforcement channels; however, depending on the environment and mission, criminal intelligence may be directly integrated into the operations process as discussed in chapter 5. PIO can provide significant, relevant, and timely criminal intelligence derived from U.S. and HN criminal investigative efforts focused on active criminal, terrorist, and irregular threats against U.S. and HN assets and interests. See ATP 3-39.12 for additional information on law enforcement investigations.

Interviews and Law Enforcement Interrogations

3-69. Although physical evidence, records, and recordings often provide critical bits of information about an incident, there is usually a significant benefit in asking questions of persons who have some direct 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, which are used by military police and USACIDC personnel to obtain relevant police information. The third is intelligence interrogations and is only conducted by trained and certified military intelligence personnel.

Law Enforcement Interviews

3-70. Interviews are conducted by law enforcement personnel to gather information and determine facts about a crime or incident. Interviews are characterized by the questioning of a person who is cooperative and freely provides information. They are used for fact finding and are probative in nature. During interviews of potential suspects, a reasonable suspicion of guilt may not initially be established. Persons being interviewed are typically not under apprehension and may depart the area at any time. If a statement is made during the interview of a victim, witness, or potential suspect that raises a reasonable suspicion that the individual committed a crime, questioning must cease until the suspect is advised of his rights under Article 31(b) of the uniform code of military justice or *Miranda versus Arizona*, 1966. Interview questions may only continue if the subject waives his right against self-incrimination and legal counsel. This should be documented on DA Form 3881 (*Rights Warning Procedure/Waiver Certificate*). See ATP 3-39.10 and ATP 3-39.35 for additional information on interview procedures.

3-71. The following are the four main interview categories that law enforcement investigators use to learn more about crimes or incidents:

- **Canvass.** Canvass interviews offer the opportunity to talk to large numbers of people quickly to determine if they are aware of the incident or if they 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 often works to establish a 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 are designed to obtain information from people who saw, heard, or know about information of value concerning an incident. Many of the same factors that cause victim interviews to be unreliable are also present during witness interviews.
- **Suspect.** Suspect and subject interviews are conducted with persons who are suspected of committing a crime or who caused an incident with persons who are charged with a criminal offense. All factors for obtaining accurate reports from witnesses and victims apply during interviews with suspects.

3-72. 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 suspect and the ability of the suspect 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 seek answers to typically open-ended questions. The guilt or innocence of the person being interviewed is generally unknown.

Law Enforcement Interrogations

3-73. A *law enforcement interrogation* is the systematic effort by law enforcement investigators to prove, disprove, or corroborate information relevant to a criminal investigation using direct questioning in a controlled environment (ATP 3-39.10). A law enforcement interrogation is conducted by trained law enforcement personnel—typically military police investigators or USACIDC special agents. Law enforcement interrogations are employed when a reasonable suspicion of guilt is known. Law enforcement interrogations are generally more confrontational than interviews. The law enforcement interrogation is conducted in a controlled and structured environment using direct, close-ended questions designed to obtain an admission of guilt or a confession. An admission is a self-incriminating statement that falls short of a complete acknowledgement of guilt; a confession results when the whole truth has been disclosed by the subject, including the acceptance of responsibility for his actions.

3-74. 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. 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 concerning the use of polygraphs in criminal investigations. The Army Deputy Chief of Staff for Intelligence provides policy guidance for the use of polygraphs in intelligence and counterintelligence applications (see AR 195-6 and AR 381-10).

3-75. Intelligence interrogations are only conducted by DOD trained and certified interrogators. Military police perform security, guard, and escort tasks during detainee operations, but they do not participate in or set conditions for intelligence interrogations (see FM 3-63).

> ***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, AR 195-2 and ATP 3-39.12.

Police Engagement

3-76. Police engagement is the foundation for successful long-term police operations. Successful police organizations interact and establish trust with the populations they serve. This is 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 when military police and USACIDC personnel interact with residents, HN police and security forces, media personnel, and unified action partners. Routine engagement with diverse organizations and people allows military police to gain valuable police information about criminal threats and criminal activity in an area of operations. See ATP 3-39.10 for details on police engagement.

3-77. Police engagement is an activity with several distinct purposes. Police engagement is used to inform the populace (or other agencies and organizations) of specific data points and themes to persuade the population to cooperate with civil and military authorities; mitigate present or potential discontent; 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 police information from the population, other police agencies, or other external organizations. It is enhanced by regular police contact and the subsequent development of trust based on ethical, professional, and effective policing.

3-78. Police engagement is a specific type of Soldier and leader engagement; it occurs between police personnel, organizations, or populations to establish trust, maintain social order, and uphold the rule of law. Military police and USACIDC personnel engage local, HN, and multinational police partners; police and law enforcement agencies; community leaders; and local populations to obtain critical police information that may influence military operations or potentially destabilize an area of operations. The goal of police engagement is to develop a routine and reliable police intelligence network through which police information can flow to military police and USACIDC personnel and into the operations process. Based on the situation and information requirements, police engagement can be formal or informal.

- **Formal.** Formal police engagement is generally conducted as part of a deliberate military police or USACIDC Soldier and leader engagement strategy to gain support or information or to convey a message. This activity requires preparation, coordination, and proper reporting after a police engagement activity. Formal police engagement often aligns with deliberate or active police information collection methods (such as attending town hall meetings or key leader engagements with local leaders).
- **Informal.** 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 and personnel outside the military police unit has the potential to be an informal police engagement. Individual military police Soldiers and teams interacting with the population conduct the bulk of police engagement activities. Building rapport with the community establishes avenues for military police forces to obtain valuable police information. Informal police engagement typically aligns with routine or passive collection methods.

Populations

3-79. Police engagement is the primary method through which military police interact with and build trust, legitimacy, and public support with the populations they are responsible for policing, protecting, and serving. Trust encompasses several aspects that enable the effective collection of police information. Trust may reflect the population’s belief that the police enforce laws in an impartial, unbiased, and equal manner that is untainted by prejudice or corruption. Trust may also reflect the confidence the population has in the capability and capacity of the police to provide effective protection, enforcement, and civil order. Legitimate police who cannot uphold the rule of law or protect the population may lose trust and public support based on the inability to maintain civil order. Trust also reflects the faith people have that reporting information will not endanger themselves or their families, their privacy will be protected, and the information will be processed and used to serve the good of the public. When people perceive that reporting information will not contribute to apprehending criminal offenders, improving the crime environment, or reducing the fear of crime in society, they are unlikely to accept the risk of potential retribution or social isolation by reporting information to the police. In these ways, trust is the bedrock of successful police engagement and police information collection among populations.

3-80. Military police and USACIDC personnel can gain a significant amount of police information from initial complaints or calls for response or assistance due to specific emergencies or incidents. The initial contact with complainants or individuals at the scene of an incident (witnesses, victims, and potential suspects) can result in acquiring 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 results 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 police information is critical to the development of accurate assessments and analysis by military police, USACIDC personnel, and police intelligence analysts.

Community Leaders

3-81. Community leaders can be valuable sources of police information specific to their areas of influence. They typically have historic knowledge of persons and activities in their cities, towns, neighborhoods, or bases. Information received should be confirmed and vetted; however, community leaders can provide military police and USACIDC personnel with valuable information regarding the criminal history and variations in their area (persons or groups, new individuals or groups, activities and observations that are out of the norm). These leaders can also provide insight into the opinions of the population (public perceptions and levels of trust or hostility) on the police in the area.

3-82. Community leaders may include—

- Local government officials.
- Installation or base commanders and staffs.
- School officials.
- Business owners or managers.
- Neighborhood mayors and watch leaders.
- Religious and tribal leaders.
- Informal leaders.

3-83. Community leaders in another culture may require time and effort by military police and USACIDC personnel to build a level of trust that results in the 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. Military police assessments should be made early in an operation to determine the appropriate level of police engagement required in a particular area of operations.

Unified Action Partners

3-84. 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, and HN governments). 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 collection efforts. Unified action partners may include—

- Host-nation police, corrections personnel, or criminal justice sector officials.
- Civilian law enforcement agencies (local, state, and federal).
- Multinational police forces.
- U.S. governmental agencies (Department of State, Department of Homeland Security [DHS]).
- Nongovernmental organizations (American Red Cross, Doctors Without Borders).

Informants and Law Enforcement Sources

3-85. In some circumstances, military police and USACIDC personnel may attempt to gain recurring access and insight into the workings of a criminal network. At other times, they seek similar access to an organization that may knowingly or unknowingly provide support to criminals. Army law enforcement personnel frequently obtain police 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 are known to the law enforcement investigator and may be willing to provide additional information, including information that they obtain specifically at the request of an investigator or police intelligence analyst.

3-86. 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 they 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 normally coordinates and deconflicts their law enforcement 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.

3-87. 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, avoid being targeted, or direct prosecution or attacks against their rivals. Still, others are motivated by feelings of patriotism or a sense of justice or to support U.S. values and ideals. Some informants and law enforcement sources are motivated by feelings of revenge toward the organization they are reporting against. It is important for law enforcement investigators and police intelligence analysts to understand these motives. At a minimum, this understanding provides insights into biases and potential areas of informant law enforcement or source unreliability that may make information suspect or warrant deliberate corroboration.

Traffic Management and Enforcement

3-88. Military police conduct traffic management and enforcement across the range of military operations. Traffic management and enforcement are critical to maintain freedom of movement for military and civilian traffic. Due to the dispersed nature of road networks spread throughout the area of operations or on bases and base camps, military police conducting traffic management and enforcement are perfectly suited to perform active or passive information collection while performing traffic-related tasks. Performing traffic control places military police in regular contact and interaction with local populations that may provide relevant information. During large-scale ground combat operations, the movement of dislocated civilian populations may be monitored, and variations or indicators may contribute to the overall situational understanding of the commander.

3-89. While conducting traffic control, military police establish traffic control posts from which they may perform reconnaissance and surveillance tasks to fulfill deliberate information collection objectives. *A traffic control post* is a manned post that is used to preclude the interruption of traffic flow or movement along a designated route (FM 3-39). Deliberate information collection at traffic control posts enables military police to contribute to answering commander PIRs focused on criminal and other irregular threats in support or consolidation areas. Locations of traffic control posts established on main supply routes and lines of communication put military police in a unique position to monitor and report information regarding friendly forces to influence the commander's FFIR. Information may include a changed route status, situation reports on friendly force convoy status, unanticipated obstacles, hazards, collisions creating traffic congestion or impacting movement schedules, and other mobility-related information reported through traffic control posts that may not be reported through other channels.

3-90. An important part of traffic enforcement is the use of checkpoints. Checkpoint operations conducted by military police are command-authorized inspections. The purpose of checkpoint operations, within the context of traffic enforcement, is to create a deterrent effect (perception of increased risk of detection, citation, and possible apprehension for traffic-related violations). Checkpoint operations allow military police to employ random antiterrorism measures, probable cause searches, and the employment of technical capabilities, such as MWD or biometrics to identify known criminal offenders, reveal contraband or illicit materials, and discover indicators of criminal activity. The ability of military police to conduct inspections and search persons and vehicles at checkpoints (depending on policy, standard operating procedures, and local guidance based on the operational environment) enables them to collect illegal material, collect evidence of criminal activity, and obtain police information to fulfill deliberate collection objectives or passively as part of routine observations and interactions with persons transiting the checkpoint.

Physical Security and Access/Entry Control

3-91. Military police employ several diverse capabilities to implement physical security measures, control access to areas such as bases and base camps, or regulate the entry to places such as critical sites or at border crossing sites. Similar to the level of interaction, inspection, and observation present during checkpoint operations, military police collect police information while performing physical security, access control, and entry control by using active and passive methods that employ a mixture of technological and human sensors. This mixture of sources enables military police to obtain a comprehensive understanding of the security environment, criminal and other irregular threats to U.S. forces and operations, and routine patterns of daily activity that may provide indicators of increased threats, criminal activity, or public discontent.

3-92. *Physical security* is that part of security concerned with physical measures designed to safeguard personnel; to prevent unauthorized access to equipment, installations, material, and documents; and to safeguard them against espionage, sabotage, damage, and theft (JP 3-0). (See AR 190-13 and ATP 3-39.32 for additional details on physical security.) Physical security measures are applied in depth as a critical aspect in applying security and antiterrorism measures on static locations. They are key in preventing unauthorized access to restricted, controlled, or vulnerable areas. Physical security measures must be prioritized based on vulnerability and threat assessments to protect critical sites, personnel, and equipment. Physical security measures employ combinations of human and technical sensors that collect an abundance of police information that is immediately accessible to military police and USACIDC personnel. This information may be disseminated as needed to influence situational awareness, or it may be analyzed by police intelligence analysts to develop criminal intelligence or crime analysis that guides law enforcement investigative or policing approaches. Different types of relevant sources of police information can be implemented to increase physical security measures, including video cameras, intrusion detection devices, and security guard personnel.

3-93. The purpose of an access control point is to prevent unauthorized access to Army installations, bases, and base camps, while maximizing traffic flow. The difference between access control points and entry control points is that access control points are those points along an installation boundary that represent an initial security screening point for vehicles and, in some cases, pedestrians entering the installation, base, or base camp. See TC 19-210 for information on access control.

3-94. Those facilities or locations within the boundary of an installation or base that require restricted entry are referred to as entry control points. Entry control points are generally located at airfields, ammunition supply points, high-security areas, and command posts. Entry control points are also used to describe efforts to regulate, monitor, and enforce laws, customs, or policy at border crossing sites, border security checkpoints, and customs checkpoints. Military police provide support to customs and border security through the operation and execution of entry control points and security checkpoints.

3-95. Military police are well positioned when manning access and entry control points due to the intrusive nature these security checkpoints may entail. During access and entry control, security guards observe and engage individuals who may—

- Voluntarily provide information.
- Show signs of discomfort or nervousness while attempting to hide criminal or terrorist activity.
- Be identified by devices connected to a biometrics watch list or law enforcement databases as a wanted criminal subject or known terrorist actor.
- Attempt to smuggle contraband or illegal substances across jurisdictions (from a state to an Army installation or across international borders).
- Display probable cause or evidence of criminal activity (for example, slurred speech and the presence of an alcoholic-like odor may give military police a reasonable suspicion to perform a field sobriety test for suspected driving under the influence, or a random inspection may reveal evidence of illegal activity, such as human, arms, or drug trafficking).

3-96. Access and entry control points present likely avenues of approach for criminals and terrorists seeking to infiltrate or attack U.S. forces. These points present threats with an opportunity to combine mobility and surprise during an attack due to the trafficability of routes and the ability to blend in with routine traffic. They also present the opportunity for adversarial personnel to attempt to gain access to a base, country, or facility by concealing their identity or their hostile intentions (for example, insider threats with valid access who are motivated to violate the law or conduct an attack). The use of biometrics, identification procedures, trained security guards, and military police often causes access and entry control points to be the first sensors capable of detecting potential threat reconnaissance and surveillance, indicators of an attack on U.S. forces and bases, and criminal activity (smuggling, trafficking, illegal substance abuse). This is true whether these tasks are performed to control access at home station or to control entry to secure facilities or whether they are deployed in support of decisive action. Information collected through such means should be immediately assessed to ensure that relevant and time-sensitive information is reported through the proper channels immediately.

Note. Observations and information related to potential threat activity at home stations should be immediately reported to counterintelligence personnel.

Military Working Dogs

3-97. The MWD teams provide a variety of unique capabilities that contribute to the collection of police information. MWDs range from single-purpose canines that are trained on one specialized task to dual-purpose canines that are capable of performing several complex tasks (scouting, patrolling, detecting explosive and narcotic scents). Those missions that include reconnaissance often find MWD teams to be a valued asset, although their value to surveillance missions may be limited. MWD teams provide patrol and explosive detection and tracking capabilities that enhance reconnaissance operations. Due to their ability to detect beyond the capacity of human senses, MWDs are well suited to complement military police information collection by detecting explosive, narcotics, and other indicators of criminal or terrorist activity. See ATP 3-39.34 for more information on MWD.

Detention Operations

3-98. Detention involves the detainment of a population or group that poses some level of threat to military operations. Detention operations are conducted by military police to shelter, sustain, guard, protect, and account for populations (detainees or U.S. military prisoners) as a result of military or civil conflict or to facilitate criminal prosecution. Detained persons are frequently sources of information pertaining to other investigations or prosecutions due to their direct or indirect connections with crime, criminal activity, or other criminals within or outside a detention facility.

3-99. Military police responsible for guarding detained personnel continuously employ passive collection techniques to gather information about the population of U.S. military corrections and detention facilities in support of unified land operations. This passive collection stems from observing the activities, routines, and interactions of detained populations in detention or corrections facilities. Military police personnel conducting detainee operations use observation and listening techniques to gain and maintain situational awareness critical to the protection of the guard force and facility population. Passive collection requires significant attention to detail and continuous attention from military police guard forces. Information collected by guard personnel is passed through the chain of command to the echelon S-2/G-2 using established debriefing procedures, when authorized by appropriate laws and policy.

3-100. 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 detention facility. Regular debriefings for guard personnel operating in close proximity to the facility population can provide military police staff and police intelligence analysts with the information necessary to develop and identify the formation of disruptive trends, patterns, and associations in the facility.

3-101. Detained 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 is the chain of command; in a deployed operational environment, it is the S-2/G-2. The external element may also require additional intelligence or law enforcement interrogations or interviews. FM 3-63 contains additional information concerning detainee operations and associated PIO.

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

Dislocated Civilian Operations

3-102. Military operations that are conducted across the range of military operations often require the temporary movement of civilian populations. Military police provide support to dislocated civilian operations, which includes establishing and operating facilities and supporting civil affairs efforts to ensure that routes remain open and clear to the maneuver commander. Dislocated civilian operations are conducted by military police to shelter, sustain, guard, protect, and account for civilians that are dislocated as a result of military or civil conflict or natural or man-made disasters. The level of control is typically drastically different than during detainee operations. Detainee operations involves a high level of control and supervision based on the security risk. During dislocated civilian operations, dislocated civilians are allowed freedom of movement as long as such movement does not impede military operations.

3-103. Despite the differences between detainee and dislocated civilian operations, any facility housing large numbers of persons for significant periods of time is prone to unrest, the presence of criminal activity, and the formation of (or infiltration by) criminal elements. Some of the same passive information-gathering techniques employed to identify and mitigate disruptive or criminal activities within a detention facility may be required in a dislocated civilian facility. The collection of police information during dislocated civilian operations is critical to understanding the threat of crime within the population and may help answer information and intelligence requirements because of the dislocated civilians' unique knowledge of the places, people, and networks operating in areas disrupted by military operations.

Other Sources of Police Information

3-104. Besides the police information collected during the conduct of military police operations, there are several additional tasks and sources that military police and police intelligence analysts may use to collect the police information necessary for criminal and crime analysis.

Database Queries and Searches

3-105. Police intelligence analysts conduct searches and queries of databases to obtain relevant information that may be combined with collected police information to create situational understanding or influence the criminal and crime analysis processes. Because databases (Army law enforcement databases, federated law enforcement enterprise databases, or intelligence databases) are compartmentalized and often run on separate systems or classification levels, police intelligence analysts must carefully plan and prepare for searches and queries to ensure that they access the appropriate systems and networks for the data they seek to obtain.

> ***Note.*** Special care must be given to handling data, information, or intelligence on different systems and networks. Each network possesses its own classifications and information protection considerations. Police intelligence analysts must remain cognizant of the classification level and release criteria of the information they are handling to ensure that privacy-protected or law-enforcement-sensitive information is not improperly shared outside law enforcement channels and classified information is not exposed. See AR 25-22 for handling privacy information, AR 190-45 for handling law enforcement-sensitive information, and AR 380-5 for handling classified information.

Data Mining

3-106. Data mining uses data to discover previously unknown, valid patterns and relationships in large data sets. Data mining analyzes data from different perspectives and summarizes it into useful information. It finds correlations or patterns among multiple fields in other large relational databases. Data mining can help organize the mass of collected data. Data mining consists of more than collecting and managing data; it also includes analysis and prediction.

Reachback

3-107. *Reachback* is the process of obtaining products, services, and applications, or forces, or equipment, or material from organizations that are not forward deployed (JP 3-30). Reachback capabilities allow military police and USACIDC personnel to leverage national-level capabilities to support operations in theater. When deployed, one of the most important reachback capabilities that military police and USACIDC personnel have is access to the Defense Forensic Science Center. The Defense Forensic Science Center maintains its primary forensic laboratory at a stationary location due to the nature of the equipment required. While the Defense Forensic Science Center provides forward-deployable forensic expeditionary laboratories, advanced technical forensics analysis may require reachback support from the Defense Forensic Science Center to provide advanced forensic support in latent fingerprints, tool marks, firearms, DNA, and explosive/drug chemistry. This combination of an on-site and reachback capability allows the forensic expeditionary laboratory to prioritize in-theater capabilities while ensuring comprehensive forensic analysis support through reachback.

Crime Statistics and Surveys

3-108. There are several sources of crime data that police intelligence analysts may use to generate police information for use in criminal and crime analysis. At the national level, sources include the Federal Bureau of Investigation (FBI) Uniform Crime Report, National Incident-Based Reporting System, and National Crime Victimization Survey. At the Army strategic level, similar crime statistics are generated annually in the Office of the Provost Marshal General's Army Crime Report and the emerging Army Crime Victimization Survey and via a direct link to the Defense Incident-Based Reporting System. The Defense Incident-Based Reporting System is the DOD centralized reporting system to the FBI National Incident-Based Reporting System (see DODI 7730.47). Besides national and Army-wide data, police intelligence analysts can produce local installation crime statistics and leverage police intelligence networks with local law enforcement agencies to gather crime data and statistics. Appendix C provides Web site links to the following various crime statistics sources:

- Uniform Crime Report.
- National Incident-Based Reporting System.
- National Crime Victimization Survey.
- Army Crime Report.
- Army Crime Victimization Survey.
- Defense Incident-Based Reporting System.
- Local crime statistics.

Open Source and Public Information

3-109. 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, social media sites, chat rooms, and other printed or digital publications). With the proliferation of information 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 through online sources. Individuals, groups, and organizations regularly populate public sites, providing valuable information about their associations, organizations, motivations, and other aspects of their operations and activities.

Operational Contract Support

3-110. 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 ATP 4-10). Contracted support often includes traditional goods and services; but it may also include interpreter communications, infrastructure, security, and other technical support. 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.

3-111. 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 the HN, U.S. military, multinational, intergovernmental, or nongovernmental personnel. Military police and USACIDC personnel should not overlook contractors as a possible source of information.

PROCESS POLICE INFORMATION

3-112. Military police process collected police information before reporting it. Processing converts information into a form through which it can be used for reporting and analysis. This usually involves placing the information in a standard report format (such as a military police report). Military police initially process collected police information into manageable portions and prioritize the collected information according to current collection requirements. Before reporting collected police information, military police ensure that the information is timely, accurate, precise, and relevant to the intelligence and information requirements established by the information collection plan. Military police also highlight newly identified crime and criminal activity and established patterns, trends or associations within the area of operations that are readily apparent. Military police collection assets reporting may report that collection occurred but that they did not observe any activity that satisfied the information collection requirements.

3-113. Systematically recording and cataloging information obtained by assigned collection assets and routine patrols are critical to the PIO process and may fill important knowledge gaps in the overall situational understanding. Police information may be recorded manually or inputted directly 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 a rapid analysis of the information is identified, it is fed directly 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 operating in the United States and its territories.

POSTMISSION DEBRIEFINGS

3-114. The police intelligence debriefing is a process of collecting information of potential value by questioning military police elements returning from missions. The purpose of a debriefing is to identify and record data and information collected by the military police collection asset. This information may serve to identify collection tasks, additional information, and observations in the area of operations or to properly identify and record evidence gathered during the conduct of the mission.

Debriefing Collection Assets

3-115. Establishing debriefing procedures, including debriefing patrols with no deliberate collection mission to gain police information gathered through passive observations, is critical to the information collection effort. Properly conducted police intelligence debriefings ensure that available information is collected, collated, and assessed in an attempt to answer 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 extract information gained from observations made by military police to enhance situational understanding and fill gaps in current knowledge. Missions should not be considered complete and personnel should not be released until reports and debriefings are complete. When conducting debriefings, all mission elements should be debriefed, including—

- Leaders returning from operational liaison positions or meetings.
- Military police and other law enforcement personnel 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 police intelligence value.

3-116. The 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 the immediate recognition of CCIR. Time-sensitive information identified as exceptional should be immediately reported for action through the appropriate staff and command channels. The S-2/G-2, S-3/G-3, provost marshal section, or police intelligence analysts should—

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

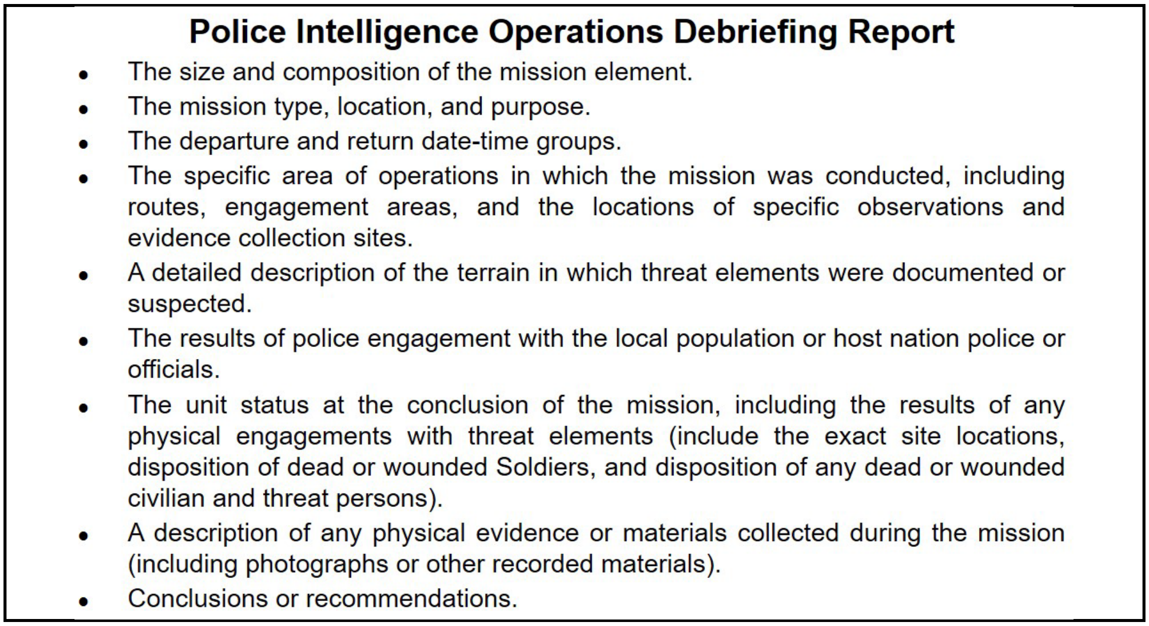
Debriefing Considerations

3-117. 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 an 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.

3-118. During the debriefing, avoid yes or no questions or questions framed in a way that leads the respondent to a particular answer. The goal of the debriefing is to gain information from the military police collection asset 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, staffs, and investigators with critical pieces of information. 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 or lack of sounds?”

3-119. At the conclusion of the debriefing, document collected observation and material evidence. A PIO debriefing report should be completed. Include, at a minimum, the items listed in figure 3-2, page 3-26.



Police Intelligence Operations Debriefing Report

- 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.

Figure 3-2. Example of a police intelligence operations debriefing report

EVALUATE POLICE INFORMATION

3-120. Military police staffs and police intelligence analysts evaluate police information for relevancy, reliability, and timeliness. Evaluating police information includes determining whether the information is relevant to existing information requirements and if pieces of the police information are related. Initially, information may seem irrelevant; however, it should be indexed, queried, and periodically reviewed in future analyses. When reevaluated, fragmentary pieces of information may be fused with additional data and information to provide an understanding that may not be achievable when analyzed as a singular piece of data. Additionally, police information must determine whether the information is reliable for presentation or if additional confirmation is required. Collected police information must be assessed for urgency to decide whether the information impacts time-sensitive operations and should be immediately shared or whether it should be routed for deliberate analysis.

3-121. Processing police information includes the evaluation of initial information to reduce raw data into manageable portions for analysis and production. During processing, police information and subsequent police intelligence are prioritized according to current collection and production requirements. Military police and USACIDC personnel responsible for managing police information and police intelligence—

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

Evaluating Data and Information Value

3-122. Police intelligence analysts must weigh the value of data and information to decide what is credible and relevant for analysis. The following five aspects determine the value of police information:

- **Validity.** Is the information a correct representative of what it is believed to signify? Do not produce police intelligence before validity is confirmed.
- **Relevance**. Is the information relevant to the mission or investigation? Is the data a logical connection to the priority of effort?

- **Timeliness.** Is the information 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 information. 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.
- **Legality.** Illegally collected information will risk tainting all work and expended resources. An analyst must ensure that information is obtained within legal guidelines.

Evaluating Information Source Reliability

3-123. Information sources should be evaluated for reliability. Military police conducting PIO must conduct continuous evaluations to ensure that police information used in their analysis does not lead to false assumptions and conclusions due to problems with the information source. Military police staffs, USACIDC personnel, and police intelligence analysts use an information source reliability scale (see table 3-2) to establish the level of reliability of an information source.

Table 3-2. Information 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.

Evaluating Information Credibility

3-124. Information must be evaluated for credibility. Military police conducting PIO must continuously evaluate information to ensure that analysis does not lead to false assumptions and conclusions due to credibility issues. Military police staffs, USACIDC personnel, and police intelligence analysts use an information credibility scale (see table 3-3, page 3-28) to establish the level of credibility of provided information.

Table 3-3. 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.

Raw Data File

3-125. Raw data files are initiated to document collected information that may develop (or contribute to) a future criminal investigation or to support police intelligence products. The raw data files normally do not contain enough credible information, but they must be reviewed to determine if the data substantiates other collected information. Normally, the information in raw data files is too incomplete to justify initiating investigative activity, targeting, or reporting. If the information received is only for situational awareness and no investigative or notification activity is required, the information should be documented in the raw data file. However, when collected and carefully analyzed, some items of data that are individually of no value can often be assembled to form meaningful information and significantly contribute to a police intelligence product. The fact that this type of information is often fragmentary makes it important that the information is properly analyzed and that additional collection efforts are made, as needed, to corroborate the information. When several items of information are substantive enough to warrant an investigation, a target analysis folder is initiated.

Criminal Intelligence Collection Folders

3-126. Extensive working files should be created and maintained on persons, networks, or organizations that are the subject of criminal investigations on bases or base camps or are targeted by U.S. forces and unified action partners. Criminal intelligence collection folders contain background information, analysis, spot reports, bulletins, or other information required by a police intelligence analyst to develop a thorough understanding of potential criminal subjects and criminal organizations. These collection folders are created to establish and maintain graphic and documentary reference material and record analyses. The analyst uses collection folders to organize and compile information related to criminal threats, criminal offenders, and organized criminal activity needed to conduct criminal analysis and produce tactical or strategic criminal intelligence products.

3-127. Criminal intelligence collection folders should be maintained separately from law enforcement investigative files and other police intelligence products because they pertain directly to criminal offenders and organized criminal activity. Access to the folders should be controlled. Military police and USACIDC organizations maintaining criminal intelligence collection folders ensure that applicable laws, policies, and regulations are adhered to regarding the collection, storage, and maintenance of information and intelligence directly related to criminal offenders, networks, and organizations. See AR 195-2, DODI 5505.17, and DODI 5525.18 for additional information.

3-128. The baseline content of criminal intelligence collection folders should include—

- Names of suspected or known criminal offenders.
- Locations of crime incidents or repeated criminal activity.
- Threat indicators of criminal behavior.

- Threat signs and symbols.
- Threat effects.
- Source identification and where the specified information can most likely be obtained.

3-129. Critical information associated with a given criminal threat includes (at a minimum)—

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

3-130. Many ideologically motivated threat groups place great emphasis and importance on symbolism. This is also true of the gang culture in the United States. The following unique characteristics related to specific criminal threat groups should be included in working files:

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

Target Analysis File

3-131. A target analysis file is a criminal intelligence collection file initiated to document the criminal intelligence and crime analysis efforts related to the targeting of an area, individual, group, or organization. The target analysis file is initiated when substantive information is received or developed that warrants the active targeting of criminal activity of an individual or criminal activity within a specific area. See chapter 5 for additional information on targeting.

Report Police Information

3-132. Collected police information is useless unless it is provided to the appropriate personnel in a timely manner to facilitate decision making or to improve situational awareness of active threats. Following any collection effort, 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. Military police collection efforts executed through the conduct of military police operations must be documented and provided to military police, USACIDC personnel, and police intelligence analysts for further assessment and analysis.

3-133. If there is no operational requirement to withhold information after coordination with the supporting judge advocate, efforts should be made to report collected and processed information to other law enforcement agencies or other U.S. forces for inclusion into the intelligence 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 when it fulfills information or intelligence requirements. See chapter 5 for a more in-depth discussion of dissemination.

3-134. While it is important to conduct criminal and crime analysis to produce police intelligence products for dissemination, it is equally important to share raw police information when appropriate. The value of raw information should not be overlooked; 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 organizations 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 abbreviated information, it is important to provide contact information so that the receiving element can ask further questions and possibly receive additional information.

Police Information Reporting and Storage Systems

3-135. 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 have become a reality and a necessity to effectively manage the volume and types of available data. Databases serve as repositories for police information and analyzed police intelligence products. This data may be maintained by a local provost marshal office, military police and USACIDC units, or an Army or DOD command or agency (such as the U.S. Army Installation Management Command, the U.S. Army Crime Records Center, or the Defense Forensics and Biometrics Agency [DFBA]). Databases can be used during active investigations and as final storage locations for closed investigations and reports. It is imperative that military police, USACIDC personnel, and police intelligence analysts become familiar with the full host of available databases for data entry, storage, and retrieval.

3-136. Advances in database technology, combined with an increase in information sharing and networking among police agencies, have 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 they can also turn to databases containing fugitive information from corrections systems and terrorist threat information from DHS and FBI. The DOD proprietary automation system (ALERTS) greatly improves interoperability and eliminates gaps that criminal and other threats might otherwise exploit.

3-137. Depending on the operational environment in which military police and USACIDC personnel are operating and the type of information to be reported, there are several potential ways military police report collected and processed police information. While ensuring that appropriate legal, policy, and regulatory guidance is fulfilled, military police also ensure that they focus on accurate reporting; inaccuracies when entering data into databases may significantly impact later analysis due to data entry errors. The following are the potential databases through which military police may report police information:

- Centralized Operations Police Suite.
- ALERTS.
- DCGS-A.

Centralized Operations Police Suite

3-138. The Centralized Operations Police Suite is an information management system supporting worldwide military police operations that combines applications, such as the Vehicle Registration System, ALERTS, the Army Corrections Reporting System, the Detainee Reporting System, and a self-registration feature. The Centralized Operations Police Suite is capable of supplying a significant amount of statistical data to police intelligence analysts and provost marshal staffs, specifically through the ALERTS application. 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.

Army Law Enforcement Reporting and Tracking System

3-139. ALERTS replaced the Army Criminal Investigation/Intelligence system. A significant feature of the Centralized Operations Police Suite (the Military Police Reporting System) is becoming the primary case management system for all Army law enforcement professionals. This system provides the Army with an integrated case management system for law enforcement personnel. ALERTS streamlines the referral process and data flow from military police reports to reports of investigation, which prevents the duplicate reporting of the same criminal incidents. Additionally, external data reporting and sharing features, such as those for the Defense Data Exchange and the Defense Incident Base Reporting System, improve the ability of military police and USACIDC to share information with relevant stakeholders.

3-140. ALERTS is accredited for unclassified law enforcement-sensitive operations and uses private, network-based software applications. Military police and USACIDC personnel have local office and global access to most data in ALERTS. ALERTS helps analysts and investigators by providing a common reporting and storage database for police information. This allows stored police information to be retrieved, collated, and used for criminal and crime analysis across law enforcement and investigative organizations. (See chapter 4 for a discussion of ALERTS support to analysis.) ALERTS also allows for the rapid query of police information to meet immediate information requirements, inform key decision makers, or share with relevant and authorized stakeholders. (See chapter 5 for a discussion of ALERTS support to dissemination.)

Distributed Common Ground System–Army

3-141. The DCGS-A is the Army 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. DCGS-A facilitates the rapid conduct of operations and the synchronization of warfighting functions. This enables commanders to operate in the threat decision cycle and to shape the environment for successful follow-on operations. DCGS-A provides the following capabilities:

- Receives and processes select reconnaissance and surveillance sensor data.
- Facilitates the control of selected Army sensor systems.
- Facilitates 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.

3-142. In deployed environments, military police may report police information and police intelligence through S-2/G-2 channels using DCGS-A to meet information and intelligence requirements, support situational awareness, and influence and assist in establishing a common operational picture. When conducting law enforcement and criminal investigations, military police and USACIDC do not populate police information and police intelligence into DCGS-A to avoid violations of legal and policy restrictions. By maintaining separate law enforcement and investigation reporting and storage systems, military police prevent the sharing of police information and police intelligence that cannot be shared outside of law enforcement channels. When supporting decisive action overseas, military police and USACIDC personnel may report and store police information not related to U.S. citizens through DCGS-A to allow intelligence personnel to fuse that information with other information and intelligence to enhance situational awareness of threats to U.S. forces and operations.

Note. It is critical that the police intelligence reports that reside on DCGS-A are compliant with the legal and regulatory restrictions placed on the collection of information against U.S. persons by intelligence personnel. See appendix A for a discussion of legal authorities and restrictions.

This page intentionally left blank.

Chapter 4

Produce

This chapter describes step three of the PIO framework: produce. This step focuses on producing police intelligence products through the criminal and crime analysis processes. Police intelligence is categorized as administrative crime analysis, tactical crime analysis, strategic crime analysis, tactical criminal intelligence, or strategic criminal intelligence. Additionally, there are many types of products that may be produced and grouped for different dissemination purposes.

POLICE INTELLIGENCE PRODUCTION

4-1. Police intelligence production includes analyzing police information and presenting police intelligence products, conclusions, or projections regarding the operational environment and enemy forces in a format that enables the commander to achieve situational understanding. Police intelligence produced by police intelligence analysts, military police, and USACIDC personnel should allow stakeholders to gain a greater understanding of the operational environment and enable operational objectives. Police intelligence provides commanders, provost marshals, and law enforcement investigators with useful tools to form a holistic assessment of criminal threats and crime environments across the area of operations.

4-2. 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 decision making.
- **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 commander, provost marshal, or law enforcement investigator objectives and intent within the timeline required for certain operations or effects.

4-3. Production involves the analysis of collected police information and combines it with existing police intelligence to create accurate and complete police intelligence products. Police intelligence analysts create police intelligence products, conclusions, or projections regarding criminal threats or crime environments 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 staff members. Police intelligence products are used to revise military police running estimates, support the military decisionmaking process, and facilitate enhanced situational understanding.

4-4. Police intelligence production involves analysis of collected police information by using the criminal analysis and crime analysis processes. These analysis processes correspond to the analysis step in the scanning, analysis, response, and assessment model (see ATP 3-39.10 for a discussion of various policing models and strategies). Criminal analysis and crime analysis are interdependent, complementary, and overlapping analysis processes that allow military police to take a holistic approach in identifying and defeating criminal threats and environmental factors that promote crime, disorder, and fear of crime (see figure 4-1, page 4-2).

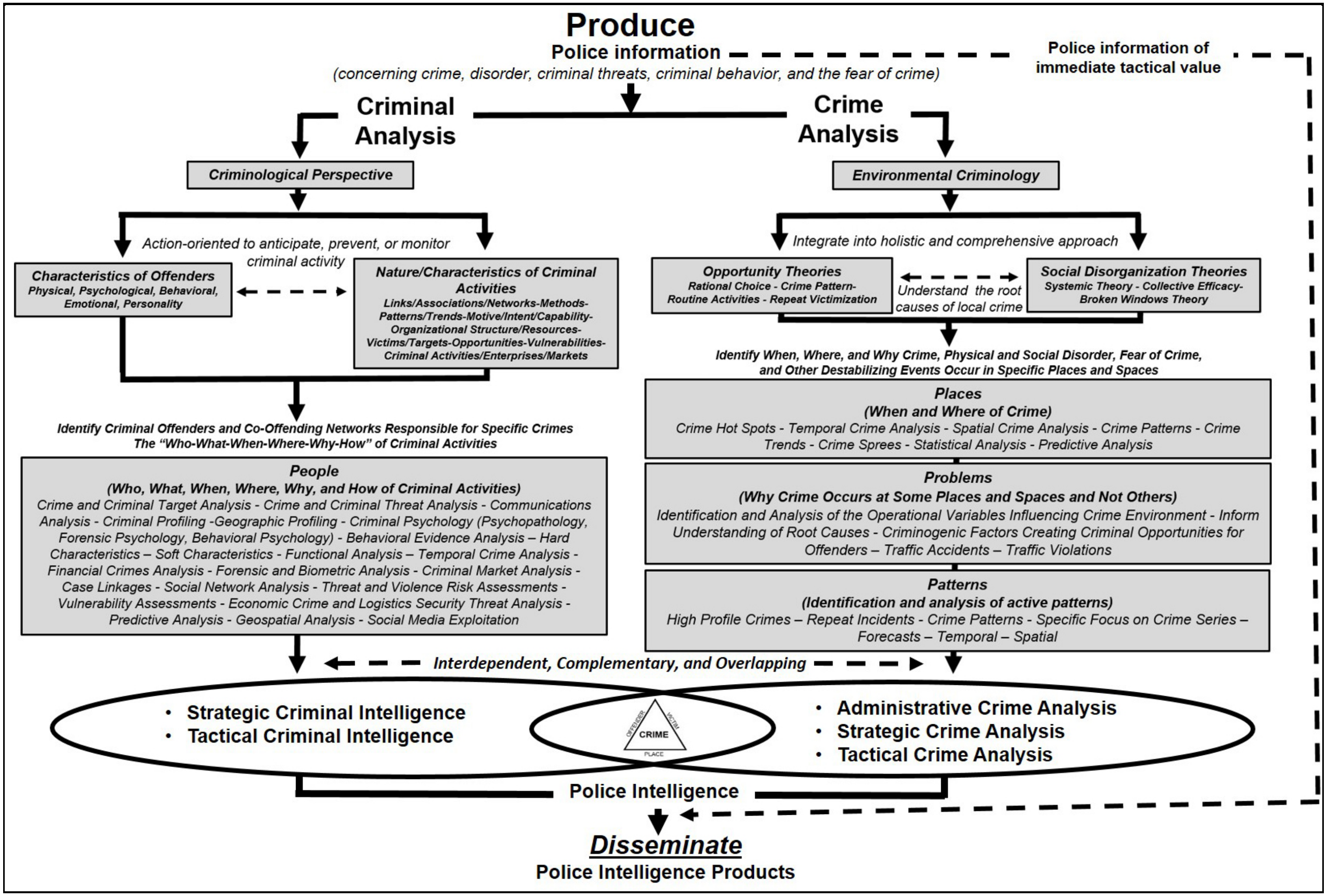

Produce
Police information
Police information of immediate tactical value
(concerning crime, disorder, criminal threats, criminal behavior, and the fear of crime)
Criminal Analysis
Crime Analysis
Criminological Perspective
Environmental Criminology
Action-oriented to anticipate, prevent, or monitor criminal activity
Characteristics of Offenders
Physical, Psychological, Behavioral, Emotional, Personality
Nature/Characteristics of Criminal Activities
Links/Associations/Networks-Methods-Patterns/Trends-Motive/Intent/Capability-Organizational Structure/Resources-Victims/Targets-Opportunities-Vulnerabilities-Criminal Activities/Enterprises/Markets
Integrate into holistic and comprehensive approach
Opportunity Theories
Rational Choice - Crime Pattern-Routine Activities - Repeat Victimization
Understand the root causes of local crime
Social Disorganization Theories
Systemic Theory - Collective Efficacy-Broken Windows Theory
Identify Criminal Offenders and Co-Offending Networks Responsible for Specific Crimes
The "Who-What-When-Where-Why-How" of Criminal Activities
Identify When, Where, and Why Crime, Physical and Social Disorder, Fear of Crime, and Other Destabilizing Events Occur in Specific Places and Spaces
People
(Who, What, When, Where, Why, and How of Criminal Activities)
Crime and Criminal Target Analysis - Crime and Criminal Threat Analysis - Communications Analysis - Criminal Profiling -Geographic Profiling - Criminal Psychology (Psychopathology, Forensic Psychology, Behavioral Psychology) - Behavioral Evidence Analysis – Hard Characteristics – Soft Characteristics - Functional Analysis – Temporal Crime Analysis - Financial Crimes Analysis - Forensic and Biometric Analysis - Criminal Market Analysis - Case Linkages - Social Network Analysis - Threat and Violence Risk Assessments - Vulnerability Assessments - Economic Crime and Logistics Security Threat Analysis - Predictive Analysis - Geospatial Analysis - Social Media Exploitation
Places
(When and Where of Crime)
Crime Hot Spots - Temporal Crime Analysis - Spatial Crime Analysis - Crime Patterns - Crime Trends - Crime Sprees - Statistical Analysis - Predictive Analysis
Problems
(Why Crime Occurs at Some Places and Spaces and Not Others)
Identification and Analysis of the Operational Variables Influencing Crime Environment - Inform Understanding of Root Causes - Criminogenic Factors Creating Criminal Opportunities for Offenders – Traffic Accidents – Traffic Violations
Patterns
(Identification and analysis of active patterns)
High Profile Crimes – Repeat Incidents - Crime Patterns - Specific Focus on Crime Series – Forecasts – Temporal – Spatial
Interdependent, Complementary, and Overlapping
• Strategic Criminal Intelligence
• Tactical Criminal Intelligence
OFFENDER
VICTIM
CRIME
PLACE
• Administrative Crime Analysis
• Strategic Crime Analysis
• Tactical Crime Analysis
Police Intelligence
Disseminate
Police Intelligence Products

Figure 4-1. Produce police intelligence products

ANALYZING POLICE INFORMATION

4-5. Military police staff and police intelligence analysts continuously analyze police information to generate understanding and produce police intelligence. The purpose of criminal and crime analysis is to answer PIR and other intelligence requirements and to produce police intelligence products that support decisive action, law enforcement, and investigative or detention missions. Analysis conducted as part of PIO is conducted from a policing viewpoint and focuses on police activities, systems, and capabilities and on the criminal aspects of the operational environment.

4-6. 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 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 make inferences and draw conclusions.
- Develop criminal threat courses of action.

4-7. The analysis of police information varies based on intelligence requirements and the purposes for which the analysis is meant to serve—such as identifying and apprehending a criminal offender, informing the public or population, or shaping crime prevention strategies to prevent and deter criminal activity. Police intelligence analysts use common analytical techniques and integrate criminal intelligence and crime analysis to answer requirements specific to policing organizations, the crime environment, and criminal investigative gaps and considerations.

4-8. 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 are 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.

4-9. Automation increases the capability to correlate large volumes of data and information from many sources and assists in the analysis process. The interpretation of information requires an analyst to develop search and file parameters. Analysis continues to be a human function—cognitive functions that manifest in reflective thinking. Police information is converted into police intelligence 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 requirements.

4-10. Access to local, theater, DOD, non-DOD, and commercial databases allows analysts to leverage stored knowledge on topics ranging from basic demographics to criminal threat characteristics. Access to military police databases, such as ALERTS, is typically granted when military police, USACIDC personnel, or police intelligence analysts are assigned to a position that requires access to perform assigned duties and responsibilities. A validated Defense Intelligence Agency customer number (acquired by the intelligence directorate of an echelon intelligence staff section S-2/G-2), in combination with SECRET Internet Protocol Router Network (SIPRNET) and Joint Worldwide Intelligence Communication System connectivity, can establish access to most intelligence databases.

4-11. The challenge for an analyst is to gain an understanding of the structure, contents, strengths, and weaknesses of a police database, regardless of the database type. These challenges require extensive training and familiarity with police databases. Additionally, the procedures are often difficult for extracting portions of data or downloading and transferring data to unit automated information systems. Commanders and staffs should consider allowing appropriate time, resources, and training to the analysts to ensure that they remain capable and proficient in navigating and leveraging available resources to maximize their potential.

CRIMINAL AND CRIME ANALYSIS PROCESSES

4-12. The criminal and crime analysis processes result in the production of police intelligence products. Although these products result from independent analysis processes, the two processes are overlapping, interdependent, and complementary to each other. Each process focuses on the specific aspects of crime inherent to the respective analysis process. Criminal analysis is designed to examine the criminal offender and specific criminal activities linked to the offender. It encompasses the who (a specific offender, organization, or network), the what (specific crimes attributed to the offender), the when and where of the crimes, how (methods) the crime was commited, and why or reason (motivations) the crime was committed. Crime analysis includes the when, where, and why of crime. It is not necessarily linked to a specific criminal offender, but it is derived from an environmental perspective in terms of understanding why crime occurs in some places and not in others. While each process is focused on producing specific desired outcomes, the two processes together generate a holistic understanding of crime problems by understanding the environmental aspects that create crime-conducive conditions and the offenders and networks who exploit available opportunities to commit crimes.

4-13. Police intelligence analysts employ various analytical techniques to analyze, synthesize, and develop products based on available police information. Analytical techniques use cognitive thought and reasoning to deduce, induce, and infer meaning from data and information while working toward conclusions that answer specific information or intelligence requirements. Depending on specific requirements and missions, categorizing the analysis effort helps to focus the analyst's efforts toward specific data, considerations, and results. While criminal and crime analysis are overlapping and interdependent, each is focused on different aspects of the crime to achieve different purposes.

4-14. The analytical techniques used during the criminal analysis process are focused analysis on producing criminal intelligence that supports decision-making processes by improving situational awareness of the characteristics of criminal offenders and the nature of criminal activities. Criminal analysis focuses on analyzing crime to understand criminal offender motivations, characteristics, methods, patterns of activity, and associations to gain knowledge of the people and networks posing a criminal threat. Techniques such as link analysis and association or network analysis are critical to linking individual criminal offenders to specific crimes and to linking co-offending criminals to the broader criminal networks to which they are affiliated with or support. This produces criminal intelligence that is predictive in nature, allowing commanders to anticipate, prevent, and monitor potential criminal activity.

4-15. The analytical techniques used in the crime analysis process focus analysis on generating an understanding of the environment, its spatial-temporal nature, and the opportunities creating conditions that are conducive to crime and disorder. Crime analysis generally focuses on crimes that have occurred and the patterns they establish to understand a specific crime incident or evaluate situational factors contributing to crime and disorder. Techniques such as crime pattern analysis are critical to identifying patterns of crime distribution in time and space that allow identification of crime concentrations. This focus on the environmental causes of crime supports proactive and preventative policing by supporting the investigation and apprehension of criminal subjects; recommending environmental changes to reduce crime-conducive conditions; and supporting policing strategies aimed at preventing, deterring, and reducing crime.

4-16. While some analytical techniques are more common or relevant to one analysis process over the other, several techniques may be applied during either analysis process based on the focus given to analysis and the desired results to be achieved. Police intelligence analysts determine their approach to analysis and the techniques to be employed, depending on specific information and intelligence requirements to produce clear and purposeful analytical results that are categorized, packaged, and disseminated to influence decisions. Three analytical techniques that are foundational and common to the criminal analysis and crime analysis processes are statistical analysis, trend analysis, and predictive analysis.

STATISTICAL ANALYSIS

4-17. Statistical data is raw data that may be organized, packaged, and disseminated for an array of purposes, such as identifying crime frequencies, trends, and distributions. Statistical data can be drawn from diverse sources and depicted in numerous manners, but the data also has limitations. Police intelligence 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 is often presented in charts to display—

- Frequencies using bar, pie, and Pareto charts. (A Pareto chart is a type of chart that contains both bars and a line graph, where individual values are represented in descending order by bars, and the cumulative total is represented by the line.)
- Trends using bar and line charts.
- Distributions using geographic information system, trend lines, or other formats.

4-18. Data requires different types of statistical tools to present effective information in a clear and understandable manner. For example, military police staff and police intelligence analysts may depict larceny offenses over the course of a year to identify seasonal variations in a particular crime. A pie chart may help show a commander the types of crimes that are most prevalent within their formation. The staff or analyst may depict these statistics on a frequency chart in bar graph format to depict multiple crimes occurring during each quarter of a fiscal year. However, if a police intelligence analyst wants to portray how long this activity has been occurring or the trajectory information, they may depict aggregate annual crime data by using a trend line. The data presented in graphic form should also be tabulated so that the information is readily available to reinforce the chart and show how the data was tabulated. Supporting geospatial products may further enhance the presentation of statistical data. Figure 4-2 provides several different examples of graphical formats for displaying statistical data.

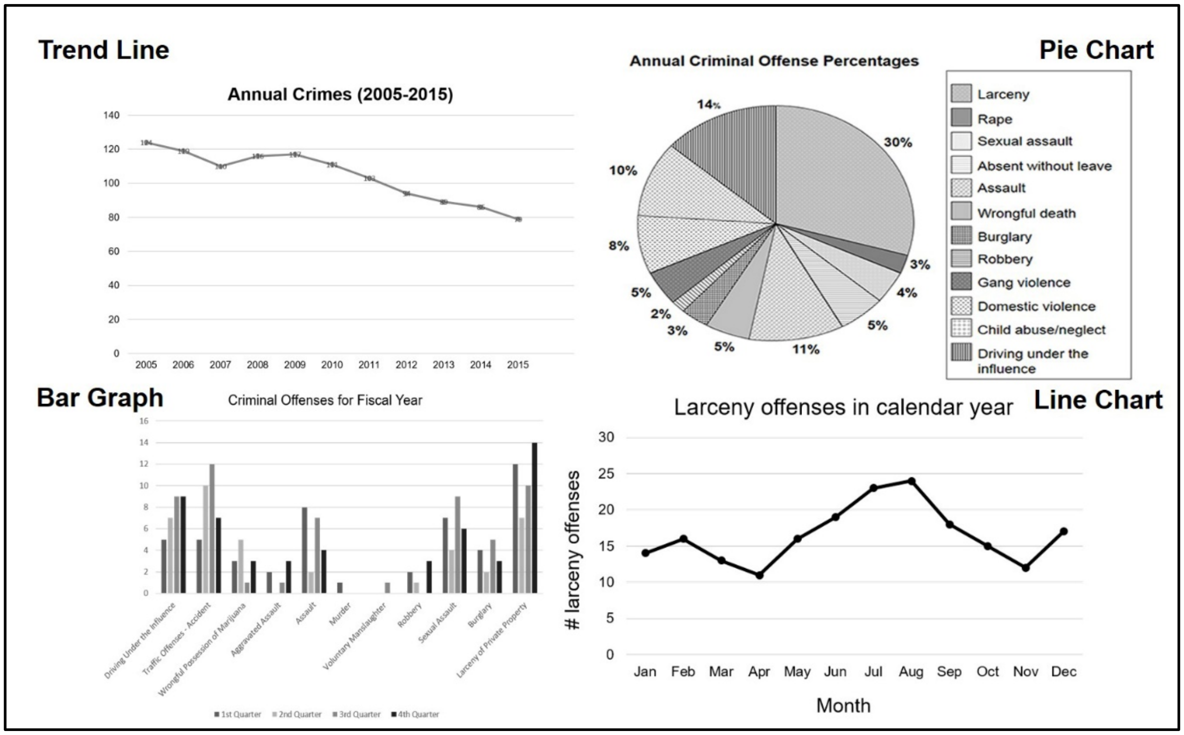


Figure 4-2. Examples of graphic representations of statistical data

TREND ANALYSIS

4-19. 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 activity in the past. Trend analysis uses statistical data to predict future actions or occurrences. This historical perspective provides continuous insights for developing coherent possible or probable courses of action for a criminal threat and for fostering the ability to predict specific occurrences. Trend analysis uses data collected from police reports, raw data files, and other assembled historical data to generate useable maps, geospatial products, charts, or graphs that indicate crime trends. This information must be maintained and updated to be effective.

4-20. Comparisons of recorded historical police and criminal incidents and the associated trends derived through trend analysis can provide clues to criminal and threat capabilities, modes of operation, and activities in relation to time and space. Police intelligence derived from trend analysis enables the redistribution of police assets to address specific crime problems. Trend analysis can also determine organizational problem areas and facilitate organizational adjustments or changes to improve police operations. Trend analysis is useful for establishing a baseline for police intelligence analysts and units to use as a statistical point of reference for future analyses. Trends can be depicted in many different formats, including—

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

4-21. Ideally, trend analysis should be depicted visually and in a report format. Trend analysis is extremely useful for depicting changes over time in—

- Specific occurrences of the types of crimes and safety issues (traffic collisions, driving under the influence of alcohol or illegal substances, juvenile crimes, assaults [simple, aggravated, domestic incidents], sex crimes, suicide, drug offenses, homicide, larcenies, gang activities, and 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.
- Traffic flow (specific intersections or roadways, entry control points and traffic control posts, traffic peaks [daily, seasonal, holiday, special events]).
- Numbers and types of citations (DD Form 1408 [*Armed Forces Traffic Ticket*], the Central Violation Bureau form, other locally used forms).
- Calls for service, assistance, or complaints against the police.
- Patrol response times.
- Special-event attendance statistics.

PREDICTIVE ANALYSIS

4-22. Predictive analysis employs multiple analytical techniques to analyze current and historical police information and police 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 be valuable in identifying crime trends to project future potential trajectories. The value in predictive analysis lies in enabling commanders and provost marshals to make informed decisions regarding criminal threat mitigation and interdiction. It enables commanders and provost marshals to make adjustments in task organization and asset distribution to counter crime-conducive conditions and factors contributing to instability and disorder.

4-23. Through analysis, police information becomes police intelligence. Analysis is based on critical examinations of available and relevant information to determine capabilities and trends and to develop predictive analysis for crime environments and criminal threats. Police intelligence supports predictive analysis to—

- Determine the identity of individual criminals, criminal groups, and applicable associations.
- Determine the course of action that a specific criminal threat is likely to take, enabling commanders, provost marshals, and investigators to identify possible friendly courses of action to counter the threat.

- Predict crime trends in an area of operations, based on the extrapolation of statistical crime data, enabling adjustments to patrol and distribution to counter criminal activity.
- Determine the 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.
- Identify the 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 HN legal systems, focusing on the police and prisons.
- Identify locations and contributing factors generating crime opportunities and crime-conducive conditions.

CRIMINAL ANALYSIS PROCESS

4-24. The criminal analysis process begins with the realization that criminals make decisions to commit crimes based on calculations (deliberate or intuitive) of perceived benefits versus the potential risks and costs of being caught and punished. From this premise, police intelligence analysts look at crime problems from the perspective of criminal offenders to understand the motivations and factors influencing offender decision making. Approaching criminal analysis from this perspective allows police intelligence analysts to recommend crime prevention and investigative measures that are designed to deny offenders the benefits they expect to gain (monetary gain) from criminal activity or to increase the perceived risks (risk of going to prison) and costs associated with committing crimes. This criminological perspective is essential to generating predictive criminal intelligence designed to anticipate and disrupt criminal activities before they produce effects that negatively impact military operations or readiness.

Criminological Perspective

4-25. Conducting criminal analysis through a criminological perspective allows police intelligence analysts to understand the characteristics of criminal offenders and the nature and characteristics associated with criminal activities.

Characteristics of Offenders

4-26. Military police, USACIDC personnel, and police intelligence analysts gain a basic understanding of criminal psychology, behavior, and characteristics through years of experience in dealing with criminals. They provide a unique policing perspective that allows analysis of the elements of crime (offender, victim, and place) from a criminal's perspective to understand criminal motivations and intentions. The cumulative knowledge, skills, and perspective generated from the daily engagement with criminal subjects or convicted prisoners give military police a unique understanding of the characteristics common to criminal offenders and of the nature of criminal activities.

Nature and Characteristics of Criminal Activities

4-27. Similar to understanding the characteristics of offenders, military police and USACIDC personnel gain valuable experience in understanding the nature and characteristics of criminal activities due to the knowledge, skills, and experience gained while monitoring, investigating, and controlling criminal activity. Common characteristics across various forms of criminal activity allow military police and USACIDC personnel to appreciate and form a particular perspective that permits them to interpret criminal incidents and activities through the prism of known criminal conventions. The following is a list of some of the areas in which military police possess unique knowledge and experience:

- Criminal motives and intents.
- Methods, techniques, and modus operandi.

- Links, associations, and networks of criminal offenders.
- Patterns and trends of criminal activity.
- Capabilities, organizational structures, and resourcing or criminal organizations.
- Victimology and criminal target/victim selection.
- Crime and criminal opportunities and impacts on criminal perceptions.
- Vulnerabilities and exposure to criminal activity.
- Illicit activities, enterprises, business, and markets.

People

4-28. The primary focus of criminal analysis is on the people who are responsible for committing crimes and are participating in organized criminal activity. The goal is to understand their capability, capacity, and intent to commit criminal acts or harm U.S. forces. This approach stems from using several different perspectives to scrutinize individuals who commit crimes so that holistic understanding of criminal offenders and criminal organizations is gained. These perspectives include examination through the lens of the criminal and the threat they pose to U.S. forces and interests; the psychological, behavioral, and cognitive characteristics of offenders; the connections and linkages among co-offending networks and organizations of criminals; and the way in which exposed vulnerabilities provide the crime opportunities upon which criminals act.

Communication Analysis

4-29. Communication analysis (also referred to as toll analysis) reviews 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. 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 allows police intelligence analysts to document incoming and outgoing calls, telephone locations (GPS tracking), dates and times of calls, call durations, and other communications data. This facilitates the identification of communication patterns and associations relative to specific communications equipment.

4-30. Communication analysis may be charted by using manual methods or advanced analytical software. The ability of information technology to improve the efficiency and effectiveness of analysis is readily evident in complicated career fields and data-intensive research techniques, such as communication analysis. Using advanced analytical software, police intelligence analysts can analyze large amounts of data related to communications and produce graphical charts that simplify the data and depict associations, directionality, and the volume of communications taking place within a given communication network. The greatest advantage of using information technology is the ability to filter and vary the amount of data depicted based on the level of detail a particular audience requires. A law enforcement investigator may require extremely comprehensive details, but high-level decision makers may be more interested in the broader patterns and connections such analysis may reveal. Communication analysis can be combined with other analysis techniques, such as geospatial analysis, to target communication networks on the understanding of the people using communication devices combined with the physical infrastructure that supports such communications. Appendix B provides an example communication or toll analysis product.

Financial Crimes and Criminal Market Analysis

4-31. The purpose of a financial crimes 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 for which money is a motivating factor. This type of analysis is focused 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 for which financial crime analysis is relevant include fraud (insurance fraud, contract fraud), bribery, embezzlement, theft (deception, product substitution), racketeering, and other economic crimes.

4-32. Criminal market analysis is used to examine beyond the financial crimes being committed within an area of operations so that an understanding of the markets and associated incentives for illicit goods is achieved. Understanding criminal markets is essential to not only stopping current criminal offenders but also for preventing future financial crimes by removing the mechanisms that give individuals incentives or facilitate their illicit financial crimes. When analyzing criminal markets, police intelligence analysts may use commodity flow charts. Commodity flow charts depict the directional flow of commodities (money, stolen property, or illicit drugs) between entities or within criminal networks. Commodity flow charts also provide basic association and contextual information as it pertains to the flow of commodities. Commodity flow charts can show details as precise as individual transactions or depict the totality of transactional events. Appendix B provides an example commodity flow chart.

Criminal Aspects of Corruption

4-33. Military police and USACIDC special agents conducting criminal analysis often gain insights and knowledge of criminal activities that are contributing to corruption. Criminal analysis enables military police to assist commanders in understanding the drivers of corruption and the subsequent impacts on public distrust or civil disorder. The civil institutions and personnel that U.S. forces rely on to translate operational success into enduring political solutions through the consolidation of gains are undermined by corruption that negates positive gains in civil security and order, governance, economic growth, and infrastructure development. The inability to stabilize security and civil environments undermines the government legitimacy and effectiveness that may be essential to achieving strategic and operational objectives.

4-34. While criminal analysis helps identify corruption by criminal elements, the analysis of corruption may uncover civil or police institutions linked to criminal activities, criminal organizations, or other irregular threats networks (terrorist or insurgent). Analysis of corruption is a continuous process that may reveal critical linkages, associations, patterns, and connections among people within or outside public institutions affiliated with crime or organized criminal activities. This understanding is essential for identifying criminal networks, conducting law enforcement investigations, and supporting the enforcement of anticorruption laws through the removal of corrupt officials. See ATP 3-07.5 for additional information.

Biometric and Forensic Analysis

4-35. Biometric and forensic analysis is critical to denying criminal and other irregular threats anonymity and impunity through scientific means of attribution. When people engage in criminal activity, they often leave biological materials at a crime scene or incident site. These traces of biological evidence may include an item containing blood, semen, hair, saliva, skin tissue, fingernail scrapings, bone, or other bodily fluids. Likewise, offenders may leave other physical evidence at a location, such as documents, electronic devices, firearms, bullet casings, tire or footprints, toolmarks, or trace evidence of substances such as drugs, gunpowder, fibers, glass, or soil. Biometric and forensic analysis can establish the presence of a person in time and space in relation to a criminal incident. It can also provide evidentiary insights into the criminal modus operandi, technique, or intent. Forensic analysis allows military police to scientifically establish facts or provide scientific evidence of various connections. Such connections allow military police and USACIDC special agents to identify, attribute, and connect criminal offenders to specific criminal incidents or criminal networks.

4-36. The DFBA is charged with executing the Secretary of the Army's Executive Agent responsibilities for DOD forensics and biometrics. In this role, DFBA leads, consolidates, and coordinates forensics and biometrics activities across DOD in support of the National Security Strategy. DFBA maintains the DOD authoritative biometrics repository and the DOD Automated Biometric Identification System, which includes fingerprints, palm prints, iris images, and facial images of 16 million encounters, the majority of which were collected by U.S. and coalition forces supporting the wars in Iraq and Afghanistan. Since 2005, the DOD Automated Biometric Identification System has made millions of biometric matches of non-U.S. citizens by using latent prints and facial and iris recognition to assist commanders in implementing force protection measures, target enemy combatants, identify improvised explosive device bomb makers, reduce green-on-blue attacks on U.S. and coalition forces, and identify known or suspected terrorists attempting to enter the United States.

4-37. DFBA collaborates continuously with interagency and intelligence community partners. Three key partners are DHS, FBI, and the Terrorist Screening Center. An example of DFBA interagency and intelligence community collaboration is the file sharing between DHS, FBI and Terrorist Screening Center databases, which supports a whole-of-government approach for identifying terrorists. Another example is DOD assisting DHS refugee vetting missions with analytic support to the biometric screening of applications.

4-38. The primary capability performing forensic analysis is the Defense Forensic Science Center. The Defense Forensic Science Center mission is to provide full-service forensic support (traditional, expeditionary, and reachback) to Army and DOD entities worldwide, provide specialized forensic training and research capabilities, serve as the executive agent for the DOD Convicted Offender DNA Databasing Program, and provide forensic support to other federal departments and agencies, when appropriate. The Defense Forensic Science Center is the DOD premier forensic center. Its subordinate units include the U.S. Army Criminal Investigation Laboratory, the Office of the Chief Scientist, the Forensic Exploitation Directorate, and the Office of Quality Initiatives and Training.

4-39. When USACIDC special agents require forensic analysis of evidence to support criminal investigations, they use the capabilities of the Defense Forensic Science Center to analyze forensic materials, access interagency databases (FBI Combined DNA Index System database for DNA profiles), and provide forensic analysis results and reports to USACIDC special agents to generate investigative leads, make conclusions regarding subject innocence or guilt, or provide evidence for prosecution. The Defense Forensic Science Center also provides forensic analysis support to deployed warfighters. In operational areas, Defense Forensic Science Center deploys the Forensic Exploitation Teams to provide in-theater forensic analysis support to operational and tactical commanders.

4-40. The forensic exploitation team is a deployable laboratory with adaptive forensic capabilities that enhances the exploitation of captured enemy materiel and evidence gathered supporting protection, targeting, sourcing, criminal prosecution, and mission success. Forensic exploitation teams provide a standardized exploitation process by integrating weapons technical exploitation capabilities, including explosive exploitation and electronic reengineering, with the teams inherent forensic disciplines of serology, DNA, chemistry, latent prints, and firearms/tool marks. Forensic exploitation teams support combatant commanders based on operational priorities. Forensic exploitation teams have on-site capabilities and the ability to obtain institutional support from the Defense Forensic Science Center through reachback. This combination of on-site and reachback capability allows the forensic exploitation team to prioritize in-theater capabilities while ensuring full forensic analysis support. Table 4-1 shows forensic exploitation team capabilities.

Table 4-1. Forensic exploitation team capabilities

Latent Prints	*DNA*
• Provide latent print exploitation. • Research unknown-latent-print-to-known-record comparison/identification. • Administer record-to-record comparison (identification confirmation). • Prepare latent-to-latent comparison. • Rapidly deploy latent print experts with forensic disciplines at FXD. • May work in unclassified or classified environments (support prosecution or intelligence).	• Is able to process samples and report results in 72 hours. • Follows FBI Quality Assurance Standards. • Conducts known and questioned sample processing, to include Touch DNA. • Is involved with advancing DNA technology (Rapid DNA, Next Generation Sequencing). • Is capable of submitting DNA results for prosecution by local governments. • Supports intelligence and LE communities.

Table 4-1. Forensic exploitation team capabilities (continued)

Chemistry	*Firearms & Toolmarks*
• Explosives analysis: organic explosives; inorganic explosives; improvised explosives; controlled substances; and organic and inorganic fuels. • Trace characterization: improvised explosive device components; explosive residues; post blast components; and unknown materials	**Firearms** • Determines countries of origin. • Determines if a specific suspect firearm fired the bullet/cartridge case. • Links multiple shooting incidents. **Toolmarks** • Determines if a specific suspect tool made the toolmark damage/construction of an IED. • Links various incidents or items of evidence back to a single tool or origin.

Legend:

DNA	deoxyribonucleic acid	IED	improvised explosive device
FBI	Federal Bureau of Investigation	LE	law enforcement
FXD	forensic exploitation directorate		

Link Analysis

4-41. 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 locates people; identifies the ownership of assets; and determines 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. See ATP 2-33.4 for additional information on link analysis.

4-42. Link analysis is made possible by the diverse identities and social connections humans possess. A person may simultaneously identify and maintain connections with legitimate or criminal networks based on a particular part of their identity and values. While one part a person's identity and values may draw them toward legitimate enterprises, another part of their identity and values may draw them toward criminal enterprises. For example, one individual may possess moderate political and social values but associate with or facilitate criminal or terrorist networks based on financial incentives or interests. On the contrary, another individual may perform a similar task but have stronger ideological or religious beliefs that connect them to a criminal or terrorist organization on a much deeper level. Understanding the motivating factors behind various connections, links, or affiliations with irregular threat networks is crucial to determine the strength of connections between individuals and networks. Figure 4-3, page 4-12, demonstrates the diverse identities and social links of individuals.

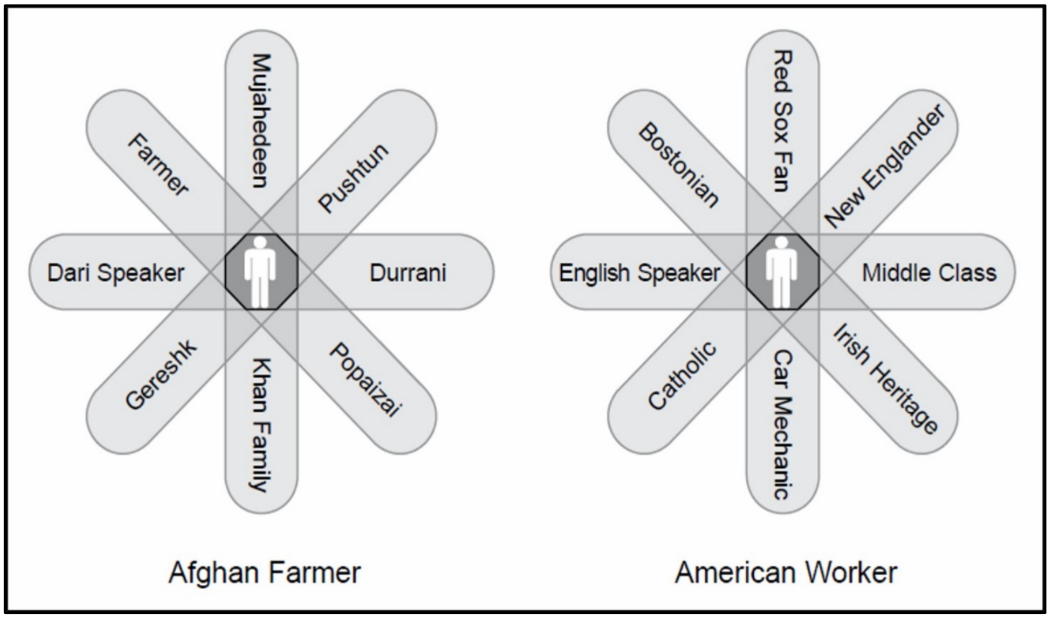


Figure 4-3. Personal identities and social links

4-43. 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 networks of complex and dynamic relationships 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. Link diagrams provide useful depictions of associations and relationships between people, places, things, and organizations. Along with the association, link diagrams can often provide contextual information explaining the nature of the association (relationship) between linked entities. 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 4-4 shows a basic example of a link diagram and standard link analysis symbology. Appendix B provides additional link analysis products generated using automated analytical software.

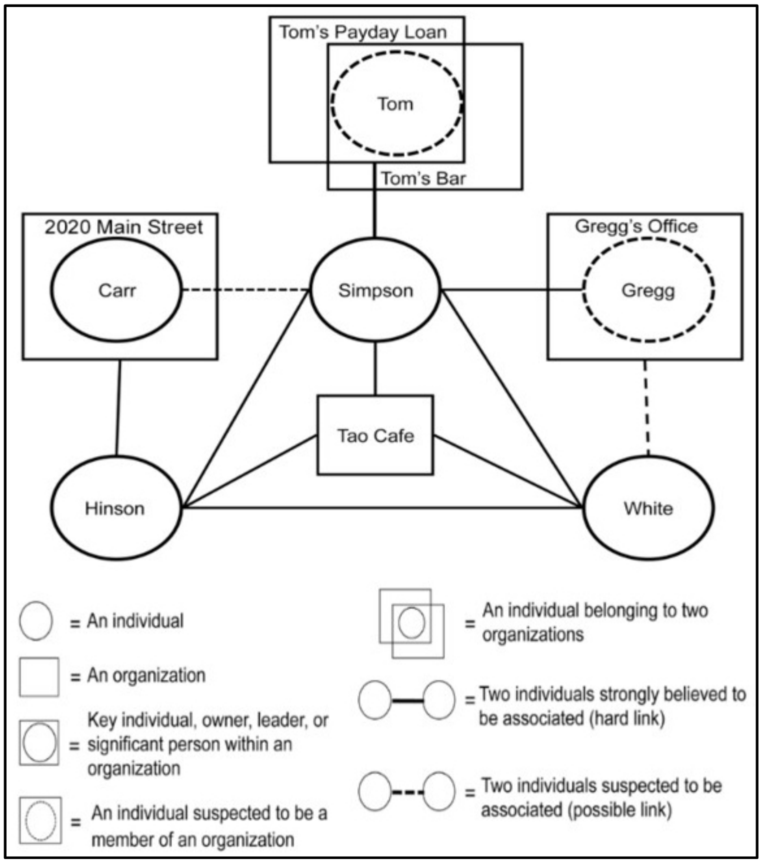

Tom's Payday Loan
Tom
Tom's Bar
2020 Main Street
Carr
Simpson
Gregg's Office
Gregg
Tao Cafe
Hinson
White
= An individual
= An organization
= Key individual, owner, leader, or significant person within an organization
= An individual suspected to be a member of an organization
= An individual belonging to two organizations
= Two individuals strongly believed to be associated (hard link)
= Two individuals suspected to be associated (possible link)

Figure 4-4. Example of a link diagram and symbology

4-44. A link analysis assists a police intelligence analyst with—

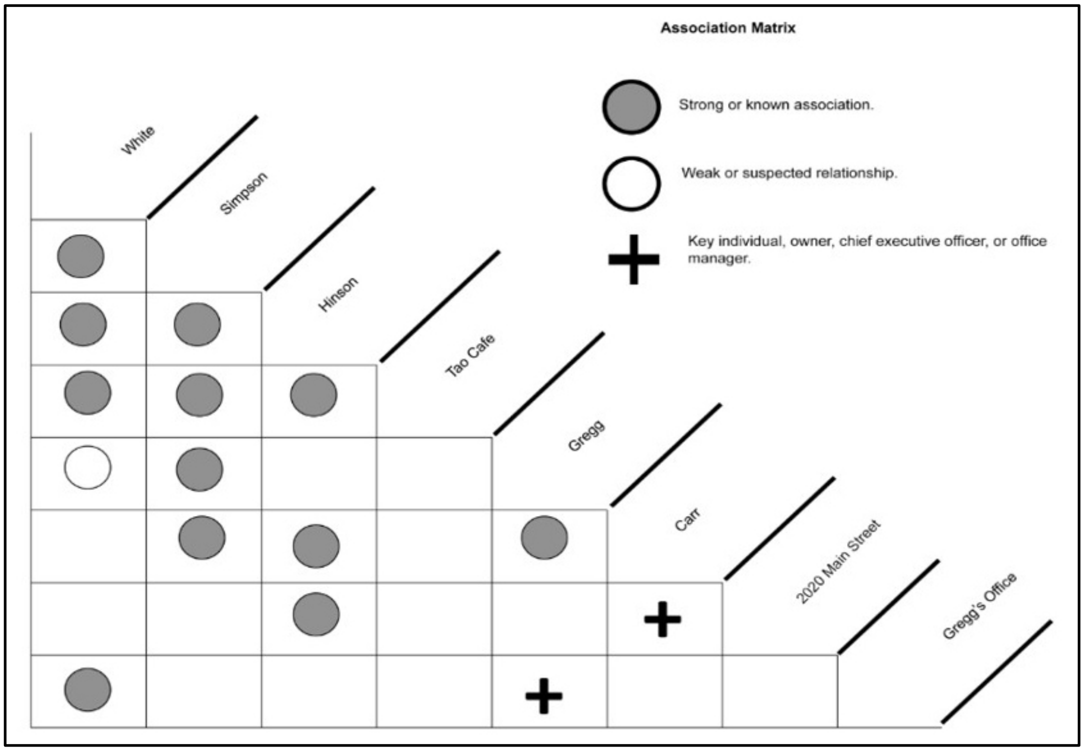
- **Determining the focus of analysis.** The focus may be on an individual, organization, business, location, or other entity. The analysis attempts to answer if—
  - Possible associations or relationships exist among the entities of interest.
  - Patterns or trends are apparent.
  - Information can 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 status-of-forces agreements (SOFA) in the HN. 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 law enforcement 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 Matrix

4-45. 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 4-5 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. This graphic may depict associations (such as weak or unconfirmed, strong or confirmed, or a significant member of an entity or group).



Association Matrix

● Strong or known association.

○ Weak or suspected relationship.

+ Key individual, owner, chief executive officer, or office manager.

	White	Simpson	Hinson	Tao Cafe	Gregg	Carr	2020 Main Street
Simpson	●						
Hinson	●	●					
Tao Cafe	●	●	●				
Gregg	○	●					
Carr		●	●		●		
2020 Main Street			●			+	
Gregg's Office	●				+		

Figure 4-5. Example of an association matrix

Network Analysis

4-46. Network analysis is an analytical technique used to exam dynamic, multilink human networks characterized by varying degrees of centrality, scale, and complexity. Unlike conventional military hierarchies, criminal organizations (and other irregular threat organizations) often operate through relatively decentralized networks that are cellular and distributed across time and space. Part of the challenge in countering these types of organizations is their constant evolution and adaptation to gain a relative advantage. Central to overcoming this challenge is understanding how criminal organizations are organized, how they carry out operations, and what factors are critical to holding the organization together.

4-47. Police intelligence analysts must understand the linkage or connection between components of a system or group performing identical, similar, related, or complementary activities or functions. Viewed as a system, a network is an interconnected or interrelated group or chain—a functionally, physically, and/or behaviorally related group of regularly interacting or interdependent elements—that forms a unified whole. Network analysis involves evaluating the various components of a network to identify critical nodes or vulnerable points to influence, target, or exploit the vulnerabilities of networked organizations.

4-48. A network consists of individuals (or other elements) and the connections between them. Individuals in a network are called nodes. A node may also be a nonperson point at which subsidiary parts of the system originate or center (such as the command node of a terrorist cell). A critical node is an element, position, or command and control entity whose disruption or destruction immediately degrades the ability of a force to command, control, or effectively conduct operations. Network analysis evaluates how nodes of a designated system function in relation to one another. It can help commanders identify systems or networks, the system's subsystems or components, and critical nodes of a subsystem for potential targeting.

4-49. Network analysis enhances understanding of criminal networks to help commanders determine the best approach to counter the network. Network analysis focuses on identifying individuals, groups, and subgroups or cells that comprise the network's structure. Police intelligence analysts analyze the criminal network structure to determine the existence and strength of relationships (links or ties) between people, groups, or organizations (nodes or actors). They evaluate key nodes in a criminal network by using network diagrams to assess varying types of centrality (degree, closeness, betweenness, and eigenvector). Figure 4-6 depicts a networked organization with various types of structures. While baseline network diagrams are an essential starting point to determine the importance of the various components of a network based on physical attributes (number of links, position of nodes), assessing the social aspects of a network (human motivations and criminal motives behind various actor behaviors) adds significant qualitative value to network analysis that can enhance the ability to counter criminal networks. See ATP 2-33.4 for additional information on network analysis.

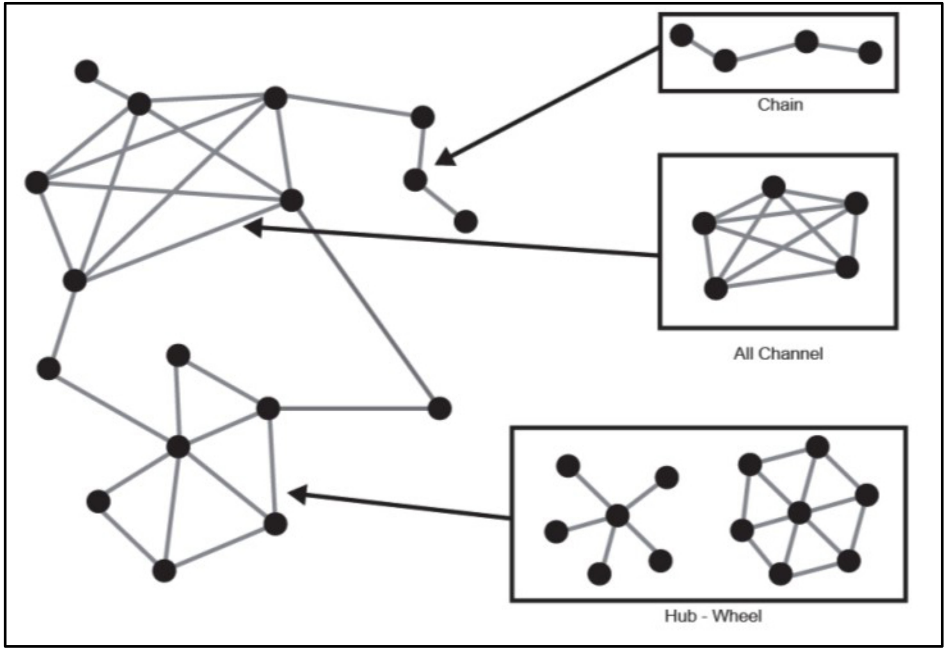


Figure 4-6. Network organization and structures

Social Network Analysis

4-50. Social network analysis (also called sociometrics) is a tool that police intelligence analysts may use to understand the organizational dynamics of a criminal network and how best to exploit it. This type of analysis involves the mathematical measuring of variables related to the distance between nodes and the types of associations required to derive meaning from the network diagram, especially about the degree and type of influence one node has on another. Social network analysis—

- Allows analysts to identify and portray details of a network structure.
- Shows how a networked organization behaves and how that connectivity affects its behavior.
- Allows analysts to assess a network's design, how its members may or may not act autonomously, where the leadership resides or how it is distributed among members, and how hierarchical dynamics may mix or not mix with network dynamics.
- Differs from network analysis in that it focuses on the individual and interpersonal relations within the network.
- Supports a commander's requirement to describe, estimate, and predict the dynamic structure of a criminal organization.
- Provides commanders a useful tool to gauge an operation's effectiveness in countering crime and criminal threats.
- Allows analysts to assess a criminal organization's adaptation to operational environments and friendly operations.

4-51. Understanding criminal networks allows commanders to visualize the individual people within these networks to determine the actors who are the most influential, powerful, or critical to the organization's function and operations. This enables commanders to develop a concept of operations for countering criminal networks and influences targeting priorities to achieve the most effective results by focusing on defeating the most critical capabilities or actors holding the network together. This may not always be the immediately obvious prediction based strictly on network analysis, but analyzing the social aspects of a network to understand human motivations, behavior, and intent may provide significantly greater analytical results based on qualitative analysis.

4-52. As an example, network analysis may reveal an actor with links to nearly all other actors in the network, possessing a high degree of centrality. This may initially seem important and lead one to believe that the destruction of this actor will significantly disrupt the network, but that may not be the case. Based on an understanding of the individual's position and motive (facilitates logistical movements and smuggling of contraband through a port for financial bribes), an analyst may determine that the individual is replaceable and has the most links with others in the network simply because of their facilitation activities and not because of their standing or importance in the organization. Given this understanding, the response may significantly differ. Rather than eliminating this single actor (who may just be replaced by another facilitator susceptible to bribes), the commander may determine the best approach is to interview, interrogate, or attempt to turn the individual into an informant based on the person's knowledge of the network's key operators, logistical movement routes, and types of illicit materials being smuggled. See JP 3-25 for additional details on social network analysis and countering threat networks.

Social Media Analysis

4-53. Human social networks have existed as long as human civilization and can be facilitated through any medium of communication (face-to-face, telephonic, digital, social media). However, the extensive use of modern social media to connect networks of people has greatly accelerated the pace of communications and the reach of potential threat networks. Social media analysis is an extension of communication analysis discussed above, but it may extend beyond mere analysis of communications due to the multiple functions or purposes for using social media. Social media may provide sources of data related to communications (posts, comments, Tweets), networks (friends, groups, memberships), activities (liking, sharing, following), affiliations (pictures with criminal gang symbols or signs), or locations (picture geotagging, location data). These various sources of data may provide evidence of affiliation with violent extremist groups, geographic movement patterns, or indications of criminal motive and intent that can influence criminal analysis.

4-54. Criminals may use social media as a tool to facilitate many different types of crimes. Besides enabling communications between individuals in criminal networks, social media may be used to facilitate cyberspace crimes, financial crimes, or other types of criminal activity. Social media analysis helps unveil those crimes that are facilitated by social media technology and it complements other analysis techniques discussed in this chapter, such as financial crimes analysis, criminal market analysis, or functional analysis.

Functional Analysis

4-55. 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 and certain actions or functions must be implicitly performed to accomplish those operations or tasks. 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 enables police intelligence 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.
- Functions to be performed to accomplish the identified threat objective.
- Capabilities available to perform each function.

Flowcharting

4-56. 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 criminal activities. Flowcharting allows a police intelligence analyst to isolate associations and patterns identified through previous analysis techniques to depict a specific person, organization, entity, association, or activity without extraneous information. The flowchart may also show accountable gaps in time. When combined with other analysis (link analysis or communications analysis), a flow chart can assist an analyst in understanding relationships and where involved associates fit into the scheme of a criminal enterprise.

4-57. 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 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.
- **Timelines (time-event) and theme lines.** These techniques are used to depict sequences of events in chronological order (timeline), or chronologically depict events as they pertain to a specific entity (theme line). Timelines and theme lines are used individually to assess the actions of a given entity or they can be used in conjunction with additional timelines or theme lines to conduct comparative analysis of relationships to given events. 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 4-7, page 4-18, shows an example of a basic time-event flowchart and symbology. See appendix B for more advanced and complicated examples generated by using automated analytical software.
- **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. See appendix B for an example.

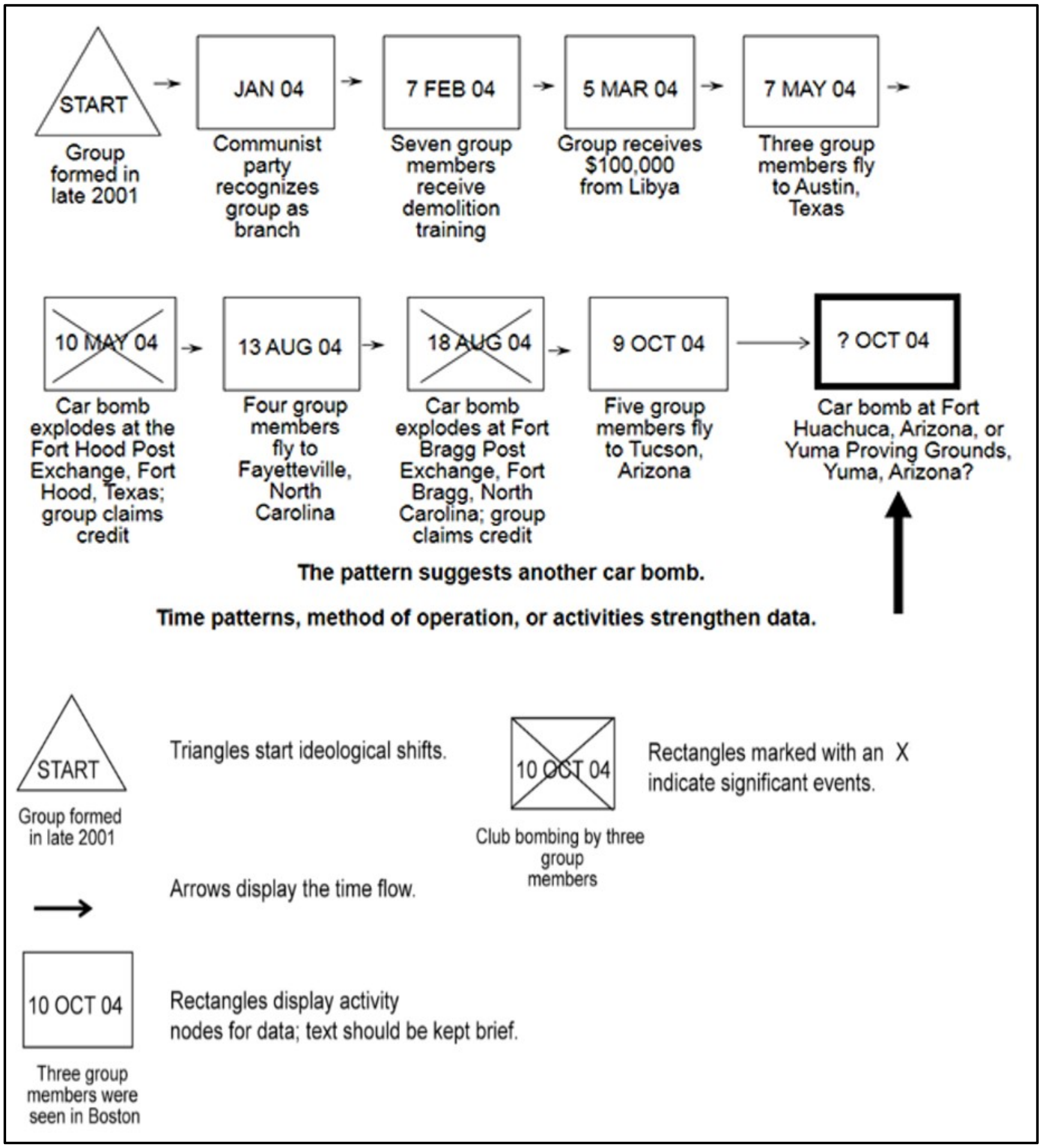

START
Group formed in late 2001
JAN 04
Communist party recognizes group as branch
7 FEB 04
Seven group members receive demolition training
5 MAR 04
Group receives $100,000 from Libya
7 MAY 04
Three group members fly to Austin, Texas
10 MAY 04
Car bomb explodes at the Fort Hood Post Exchange, Fort Hood, Texas; group claims credit
13 AUG 04
Four group members fly to Fayetteville, North Carolina
18 AUG 04
Car bomb explodes at Fort Bragg Post Exchange, Fort Bragg, North Carolina; group claims credit
9 OCT 04
Five group members fly to Tucson, Arizona
? OCT 04
Car bomb at Fort Huachuca, Arizona, or Yuma Proving Grounds, Yuma, Arizona?
The pattern suggests another car bomb.
Time patterns, method of operation, or activities strengthen data.
START
Group formed in late 2001
Triangles start ideological shifts.
10 OCT 04
Club bombing by three group members
Rectangles marked with an X indicate significant events.
Arrows display the time flow.
10 OCT 04
Three group members were seen in Boston
Rectangles display activity nodes for data; text should be kept brief.

Figure 4-7. Example of a timeline flowchart

Case Linkages

4-58. The connections revealed through different criminal analysis techniques (link, association, network analysis) allow military police, USACIDC special agents, and police intelligence analysts to make linkages between criminal investigations and cases. This expands the understanding of criminal threats from individual criminal offenders to broader criminal networks and organizations. The linkages among criminal cases allow for broadening the focus from individual criminal incidents to broader patterns of criminal activity. This technique is critical for connecting criminal incidents to determine if patterns of criminal activity are part of broader networks and organizations that constitute a criminal threat. See appendix B for a combined chart that leverages multiple types of analysis using automated information technology to greatly enhance the ability to understand diverse and overlapping relationships between people, places, things, and organizations.

Criminal Threat Analysis

4-59. Criminal threat analysis is a continuous process of compiling and examining available information concerning potential criminal threats. Criminal and terrorist threats may target U.S. military organizations, elements, installations, or personnel. A criminal threat analysis reviews the operational capabilities, intentions, and activities of threat groups and the operational environment in which friendly forces operate. Criminal threat analysis is an essential step to identify and describe the threat posed by specific criminal groups or individuals. Criminal threat analysis supports the production of threat assessments and provides the criminal intelligence necessary to influence targeting processes that seek to defeat criminal actors or disrupt criminal activities within the area of operations. Criminal threat analysis techniques are regularly applied to enhance antiterrorism, physical security, and crime prevention efforts.

4-60. Existing criminal information, criminal intelligence, threat information, and asset vulnerabilities are considered when conducting a criminal threat analysis. Criminal information and criminal intelligence provide insights on the goals, methods, techniques, and targets of individual criminals and criminal networks. Threat information can lead to the identification of threats of unknown criminals or criminal groups. Criminal threat analysis must continuously account for changes in the operational environment. As vulnerabilities are reduced in some areas or as security is improved, threats may focus on other areas where there are potential vulnerabilities or where criminal activity is least expected. Transitions between missions, tasks, and personnel often present opportunities for criminal threats to capitalize on gaps and seams that are exposed during transition periods. Criminal threat analysis is only valid as long as a threat still actively seeks to target a particular vulnerability. Failure to keep pace with adaptive criminal threats may result in security postures that no longer protect vulnerable assets.

4-61. Criminal threat analysis focuses on evaluating the following factors:

- **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.
- **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—
  - HN 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.** Geopolitical factors refers to war, instability, economic turmoil, status of local government, environmental stress.

Criticality and Vulnerability Assessments

4-62. An integral part of assessing criminal threats is understanding the criticality and vulnerability of friendly assets to the effects of criminal activity. 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 details on criticality and vulnerability assessments.) This process helps the staff identify critical assets to prioritize for the commander’s protection efforts. Critical assets may include personnel, equipment, stockpiles, buildings, recreation areas, communication, or transportation systems that are deemed critical.

4-63. The criticality of an asset typically depends on the—

- Value of an asset to a mission or population.
  - **Importance.** The importance of an asset determines the value of the asset located in the area, taking into consideration the function, inherent nature, and monetary value.
  - **Effect.** The effect an asset has on a mission or population measures the ramification of a criminal or terrorist incident in the area, taking into consideration psychological, economic, sociological, and military impacts.
  - **Recoverability.** The recoverability of an asset 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 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.

4-64. 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. The use of these tools is based on the premise that by looking at friendly forces from the threat's perspective, it becomes apparent whose assets are most critical or most likely to be targeted by threat forces. For military police and USACIDC personnel using these tools, the results can be used to develop protection strategies and defeat criminal threats.

4-65. The most commonly used analytical tools are the mission, symbolism, history, accessibility, recognizability, population, and proximity and criticality, accessibility, recuperability, vulnerability, effect, and recognizability models. (See ATP 2-33.4 and ATP 3-37.2 for details on the use of these analytical tools.) Efforts to assess criticality and vulnerability are often performed by multifunctional teams that provide contributions from different perspectives. These task-organized teams may include expertise in engineering, signal and network communications, medical support, special operations, legal support, and law enforcement. This multifunctional approach incorporates considerations from a vast array of technical specialties to produce a holistic assessment that supports a comprehensive and layered protection effort.

Criminal Threat Assessment

4-66. Criminal threat assessments integrate criminal threat analysis with criticality and vulnerability assessments to help commanders prioritize protection assets to defeat criminal or terrorist threat activities. Criminal threat analysis is essential to determine the level of threat posed against specific U.S. interests (material, structure, organization, installation, unit, population). Vulnerability and criticality assessments build on criminal threat analysis to help identify weaknesses and vulnerabilities that existing criminal threats may target. Understanding the level of threat posed by criminal actors and potential friendly vulnerabilities allows police intelligence analysts to produce criminal threat assessments that enable commanders and provost marshals to prioritize efforts and assets to counter criminal or other irregular threats posing the greatest threat to friendly forces or operations.

4-67. Based on the factors evaluated during criminal threat analysis and criticality and vulnerability assessments, criminal or terrorist threats 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., HN, 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 HN elements.
- **Low.**
  - There are no indications of a threat presence.
  - There is no threatening activity present in the area of operations.

Economic Crime and Logistics Security Threat Assessments

4-68. The economic crime threat assessmentand logistics security threat assessment are critical elements of the Army crime prevention program. USACIDC elements typically perform these specific threat assessments. These two assessments focus on analyzing economic crime potential and vulnerabilities of bases, base camps, and lines of communications (including intertheater and intratheater). USACIDC personnel work closely with logistics unit commanders to identify and mitigate these vulnerabilities within the logistics enterprise. Military police and USACIDC personnel must closely communicate and collaborate on significant items in the economic crime threat assessment and logistics security threat assessment to ensure multilayered protection of the commander's logistics pipeline. For instance, while USACIDC special agents typically perform economic crime threat assessment and logistics security threat assessment, military police typically provide support to securing the bases, base camps, lines of communications, and critical logistics nodes that USACIDC personnel assess. Effective collaboration allows for proactive and preventive policing approaches across all military police assets operating within an area of operations. The following describes economic crime threat assessment and logistics security threat assessment:

- **Economic crime threat assessment.** Economic crime threat assessment is a review 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 related to economic crimes.
- **Logistics security threat assessment.** Logistics security threat assessment is a review 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. Logistics security threat assessments can serve as substantial internal and external operational planning tools.

Crime and Criminal Target Analysis

4-69. Crime and criminal target analysis enables military police staffs and police intelligence analysts to identify criminal threats and crime-conducive conditions for targeting. A key aspect to performing crime and criminal target analysis is the determination of the effects desired and the optimal method of targeting. 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 by military police may range from police engagements to the application of nonlethal and lethal force, depending on mission and operational variables. Key objectives of crime and criminal target analysis are the determination of timing and the synchronization of operations, the prioritization of targets to be engaged, the desired effect, and the optimal method of targeting.

4-70. The results of crime and criminal target analysis directly inform military police and USACIDC efforts to protect friendly installations, personnel, and resources through the prevention, deterrence, and apprehension of criminal threats that impact friendly force safety, security, or readiness. The results of crime and criminal target analysis may also contribute to decisive action by aiding to the development of criminal and other irregular threat targets for commanders. Criminal intelligence generated by crime and criminal target analysis provides valuable information to commanders for enabling effective targeting.

4-71. As operations transition from large-scale ground combat to the consolidation of gains, crime and criminal target analysis grows in importance for commanders seeking to eliminate or reduce criminal and other disruptive elements that undermine the establishment of civil order and enforcement of the rule of law. Given the instability and disorder commonly followed by destructive large-scale ground combat, HN capabilities may be limited or nonexistent when identifying criminal actors, investigating crimes, and implementing an effective criminal justice system under the rule of law. This transition often requires increasing restraint in targeting operations as the situation stabilizes and use of lethal force is constrained. The ability to identify criminal actors within a population and target them with nonlethal police and investigative techniques is critical to defeating criminal threats without resorting to excessive lethal force that may provoke retaliatory violence or contribute to an adversary’s narrative.

4-72. Crime and criminal target analysis and subsequent military police support to operations occur in all environments. The ultimate goal of crime and criminal target analysis is to—

- Identify criminal threat persons, networks, or organizations.
- Develop investigative leads that guide or influence criminal investigations.
- Identify places with crime-conducive conditions that may be targeted to prevent future crimes from occurring.
- Make targeting recommendations to address the people and places contributing to crime.

CRIME ANALYSIS PROCESS

4-73. Eliminating criminals from the battlefield is essential to successfully address immediate criminal threats, but it is ineffective in the long-term if the conditions and environments that gave rise to those criminals are not also addressed. Without addressing the factors that create crime-conducive conditions and underlying problems which generate crime opportunities, people will continue to choose to engage in crime. The crime analysis process identifies when, where, and why crime, social disorder, fear of crime, and other destabilizing events occur in specific times and places and across broad spaces. Crime analysis focuses attention on places, patterns, and problems to determine the root causes of crime, the drivers of instability and disorder, and the relevant factors generating crime-conducive conditions that create crime opportunities. While crime analysis does not focus on the who of crime in the same sense as criminal analysis (such as attributing a specific offender to a crime incident), it provides insights into the types of people choosing to offend, the types of victims being targeted, and the methods being used by those committing those crimes. The crime analysis process results in the production of administrative, tactical, and strategic crime analysis that influences decisions and actions to prevent crime, address crime patterns, and solve underlying crime problems.

Environmental Criminology Perspective

4-74. Crime analysis is enabled by the unique professional training, knowledge, and experience of military police, USACIDC special agents, and police intelligence analysts. In the course of interacting with and analyzing crime environments, military police gain a unique appreciation and perspective that allows them to perceive crime from an environmental criminology viewpoint. Environmental criminology has a long history dating to the early twentieth century and includes two main theoretical perspectives for understanding crime: opportunity theories and social disorganization theories.

Opportunity Theories

4-75. Opportunity theories approach crime from the perspective of understanding the situational conditions and factors influencing individuals to commit crimes. To understand crime, this broad approach relies on several different types of opportunity theories within the field of environmental criminology. Descriptions of several of these theories are provided in table 4-2. Despite different focuses, these opportunity theories rely on two common assumptions: crime is driven by individual perceptions and choices that satisfy a person's needs without being caught, and offender perceptions are highly dependent on situational factors and conditions within their social and physical environment.

Table 4-2. Opportunity theories

Theory/Perspective	*Description*
Rational Choice Theory (Derek Cornish and Ronald Clarke)	Those who use the Rational Choice Theory view crime as a result of rational choices made by potential criminals based on available information in their social and physical environment. This theory suggests that criminals make decisions to engage in criminal acts based on assessing the expected gains against the risks of being caught and the severity of the ensuing punishment.
Routine Activities Theory (Lawrence Cohen and Richard Felson)	Those who use the Routine Activities Theory view crime as an extension of regular human activities that follow distinct patterns in time and space. As people go about their daily lives, they gain spatial awareness of vulnerable victims or property that may fulfill their needs and desires. This theory evaluates how the routine patterns of daily life impact and contribute to crime when a potential offender and suitable victim/target converge at a place and time absent a guardian.
Crime Pattern Theory (Paul and Patricia Brantingham)	Those who use the Crime Pattern Theory combine elements of rational choice and routine activities by viewing the patterns criminal offenders display as they move through time and space during their daily lives. This theory includes such concepts as awareness, space, action space, and cognitive maps. This theory suggests that crime occurs where suitable victims/targets intersect with a potential offender's awareness space and provides the person a rational choice to commit a crime.
Crime concentration • Repeat offending • Repeat victimization • Hot spots, products, and facilities	The 80/20 rule of crime concentration is the principle derived from the statistical analysis of crime data across multiple focus areas that finds distinct concentration patterns related to crime. Research suggests that approximately 5% of offenders account for 50% of crime, 4% of victims account for 40% of victimization, 5% of locations account for 50% of crime incidents, and some products or facilities show exponential crime rates compared to other products or facilities.

Social Disorganization Theories

4-76. Social disorganization theories focus on how areas, neighborhoods, communities, and social structures influence crime. There are three prominent social disorganization theories of crime that all focus on different aspects of the social and physical environment. These three perspectives are discussed in table 4-3, page 4-24. While each theory relies on common foundations in searching for the social aspects of disorder among communities that results in higher crime, each focuses on different aspects of social systems. The understanding of social disorganization theories is especially important when evaluating dense urban environments where systemic conditions may greatly magnify the effects of disorder and social disorganization.

Table 4-3. Social disorganization theories

Theory/Perspective	*Description*
Systemic Theory (Berry and Kasarda)	The Systemic Theory is focused on the networks, relationships, and complex systems that people develop within social environments that impact their ability to control crime. This theory suggests that formal and informal association ties, friendship networks, the collective control of teenagers, and participation in neighborhood organizations significantly influence criminality.
Collective Efficacy (Sampson and Colleagues)	Collective Efficacy is defined as the social cohesion among neighbors combined with their willingness to intervene on behalf of the common good. Social cohesion is a measure of the trust and shared behavioral expectations that exist within a community that enable informal social control and collective action.
Broken Windows Theory (Wilson and Kelling)	The Broken Window Theory suggests that people's willingness to engage in informal social control is influenced by environmental cues. When people perceive the environment as orderly and clean, they are more likely to intervene to prevent disorder, and potential criminals are less likely to commit crimes. When the environment is disorderly and neglected, no one is willing to intervene, and criminals are no longer constrained by informal social control.

Places

4-77. Places provide the setting and context for legal and illegal actions. Police intelligence analysts, when given a broader understanding that is enhanced by an environmental criminology perspective, can better analyze crime by considering the setting and context in which crime occurs and by understanding the factors that contribute to crime, the environmental vulnerabilities that produce opportunities for crime, and the common features of places that may be changed to reduce crime-conducive conditions. Closely related to the idea that crimes must occur at places (and may extend from physical places into virtual spaces such as cyberspace) is the idea that crime also occurs in time. Evaluating crime through an analysis of the spatial and temporal aspects of crime settings allows police intelligence analysts to identify situational factors relevant to solving criminal investigations and addressing crime-conducive conditions.

Spatial-Temporal Analysis

4-78. Spatial-temporal analysis uses spatial concentrations (hotspots) and temporal concentrations (hot times) to evaluate patterns in space and time that enable the prediction of crime. Spatial-temporal analysis relies on effective crime mapping and the subsequent identification of hotspots, hot times, and hot routes. These foundational techniques allow police intelligence analysts to translate raw crime data into useable depictions of crime in space and time that are essential to deriving meaning from crime patterns, drawing conclusions, and making recommendations. Given the concentrations of crime at places and times, this type of crime analysis can help focus police deterrence efforts and assist in the prioritization of limited police capabilities.

4-79. The following is an example of spatial-temporal analysis: Spatial analysis shows a neighborhood that is adjacent to a school and has a concentration of housebreaking offenses. Temporal analysis shows that these housebreakings are concentrated on weekdays during a one-hour period immediately following the release of students from that school. Spatial-temporal analysis puts the two analysis techniques together to draw the likely conclusion that students are released from school and, while on their way home, are discovering opportunities to break into unguarded and unobserved houses along the route. This conclusion informs police and influences police responses by recommending that a concentration of law enforcement patrols be placed in the neighborhoods around the school during the time period that students walk home to deter potential offenders from committing crimes.

Crime Mapping

4-80. Crime mapping uses location data (address, X-Y coordinates) to graphically depict crimes or other incidents on a map. Crime maps document cumulative crime incidents that have occurred in the area of operations. Crime maps are critical tools in geographic distribution analysis and crime pattern analysis because the visual depiction of crimes and their uneven distribution results in identifiable patterns that police intelligence analysts can use to deduce meaning. Crime mapping has been around since the early twentieth century and was often conducted using paper maps and pushpins until the advent of information systems that are capable of generating crime maps. Geographic information system tools greatly assist criminal and crime analysis by producing crime maps with advanced layering or filtering features. Crime maps may also be called incident maps, coordinate maps, or pushpin maps—depending on what type of data it is depicting or by what means. Figure 4-8, page 4-26, displays an example of a crime map.

Note. Several information systems and software programs support the techniques of crime mapping. The following example reflects software applications being fielded at various Army installations, appendix B provides examples built with i2Analyst Notebook™, and DCGS-A includes ArcGIG© software that is also capable of performing crime mapping and other spatial-temporal analysis techniques.

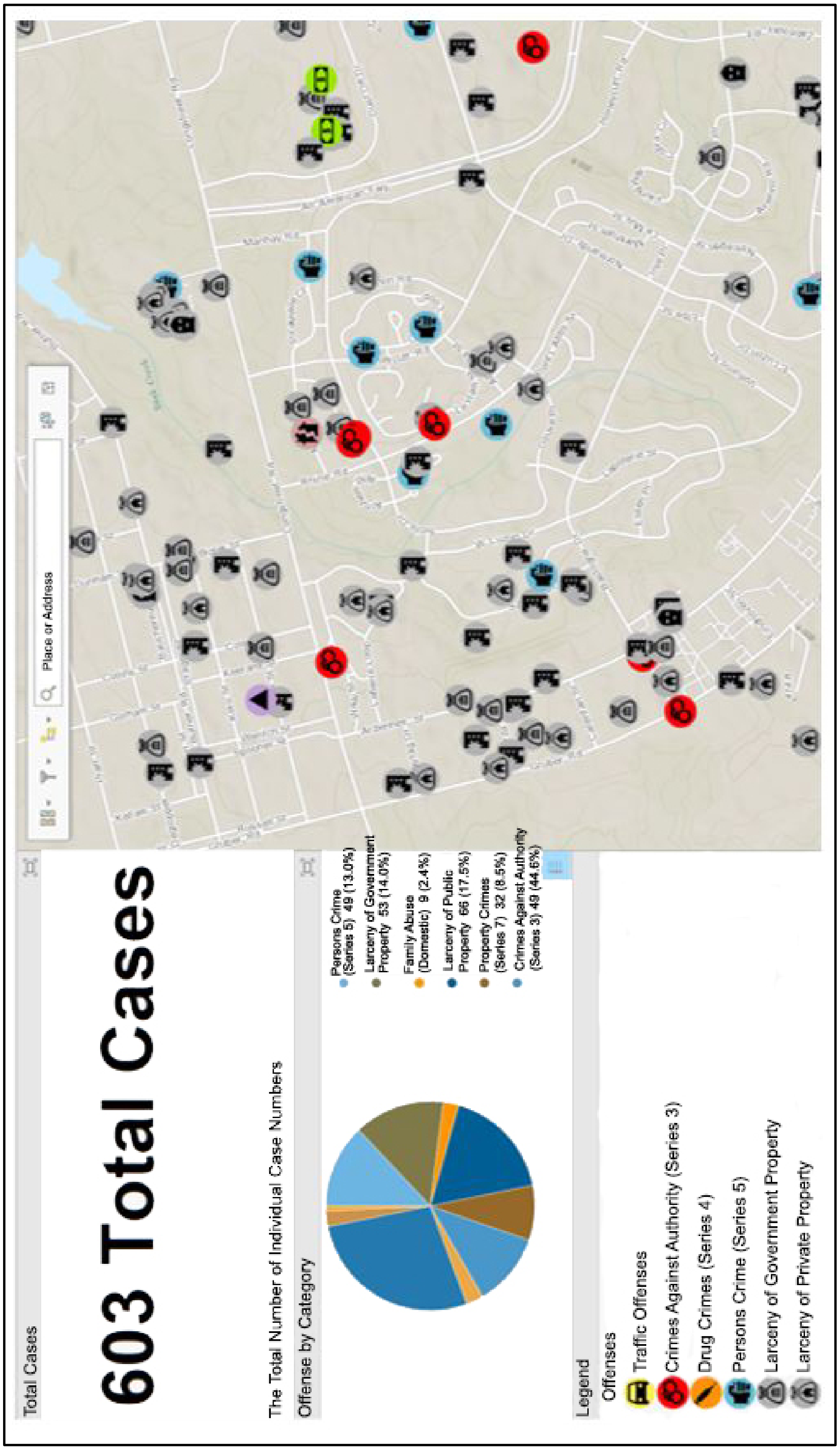

Place or Address
Total Cases
603 Total Cases
The Total Number of Individual Case Numbers
Offense by Category
Persons Crime (Series 5) 49 (13.0%)
Larceny of Government Property 53 (14.0%)
Family Abuse (Domestic) 9 (2.4%)
Larceny of Public Property 66 (17.5%)
Property Crimes (Series 7) 32 (8.5%)
Crimes Against Authority (Series 3) 49 (44.6%)
Legend
Offenses
Traffic Offenses
Crimes Against Authority (Series 3)
Drug Crimes (Series 4)
Persons Crime (Series 5)
Larceny of Government Property
Larceny of Private Property

Figure 4-8. Example of a crime map

Hotspots

4-81. When crime is mapped, the distribution of crimes often results in identifiable patterns and concentrations at or surrounding specific places. The places at which crimes concentrate are known as crime hotspots. When crime mapping reveals crime hotspots, police intelligence analysts can begin to understand the factors contributing to crime across a particular area of operations by seeking to understand the conditions, situational circumstances, and environmental factors of those hotspots to determine why crime is occurring at those places but not at others. Understanding the specific factors that generate crimes, attract potential criminal offenders, or facilitate the ability of offenders to commit crimes at a specific place is an essential precondition to developing effective policing strategies and responses to prevent and reduce crime.

4-82. Crime hotspots often result from different types of factors that influence criminal perceptions and shape decisions to commit crimes (see figure 4-9 for additional information on crime hotspots). These factors (or facilitators) include—

- **Crime generators.** Crime generators are places at which large numbers of people go without intending (or without being initially motivated) to commit crimes. Because of the scale of human interactions and the large number of potential victims, these places generate opportunities for potential offenders to commit crimes where they converge in time and space with many potential victims. Examples of these places include large shopping areas, markets, transportation hubs, festivals, or sporting events.
- **Crime attractors.** Crime attractors are places that offer many crime opportunities and are attractive to potential offenders who deliberately seek to engage in criminal activity. These areas attract similar persons who may be motivated to engage in similar types of criminal activity. Examples may include areas in which individuals are known to engage in crimes, such as drug use or prostitution.
- **Crime enablers (or facilitators).** Crime enablers are places where the lack of management, regulation, or enforcement enables or facilitates criminal activities. These places may include areas where property owners allow crimes to occur without intervention; locations where there are no effective guardians present to control potential offenders; or areas where guardians are present, but lack the capability, capacity, or will to enforce the law. Examples may include bars or nightclubs that do not control or suppress excessive alcohol consumption, drug use, or other criminal activity on their property.

Hotspot Type	*Cause*	*Questions to Answer*	*Potential Reponses*
Crime Generator	Many unprotected people	What vulnerabilities exist at this place? What actions can be done to reduce vulnerabilities of people and property at this place?	Reduce place vulnerabilities or increase protection
Crime Attractor	Attracts offenders	What is attracting offenders? What can be changed to reduce the attractiveness of this place to those offenders?	Eliminate the conditions that are attracting offenders
Crime Enabler	Erosion of controls	Who is responsible for controlling behavior at the place? Why are they unwilling or unable to prevent crimes there?	Restore proper management and guardianship over place

Figure 4-9. Understanding crime hotspots and forming a response

Hot Times

4-83. Crime concentrates at specific places during certain times. The patterns of routine activities that shape daily life often impact patterns of criminal activity. Hot times frequently vary by different types of crimes based on the type of environment that is conducive to that particular crime. For instance, daytime housebreaking may occur while residents are at work because there is an absence of guardianship over the property, while assaults or driving under the influence offenses may occur most frequently in the late evening hours after potential offenders are intoxicated and bars are overcrowded. Crime analysis of hot times combined with an understanding of hotspots assists military police not only by isolating the places at which to concentrate prevention and enforcement efforts, but also by suggesting the times during which to do so to be the most effective.

4-84. Police intelligence analysts use several techniques to analyze temporal aspects of crime to determine hot times that enable the focusing of limited policing resources and operational capacity. Two prominent techniques are histograms and heat matrices. Appendix B provides an example histogram and heat matrix.

- **Histograms.** Histograms are used to depict a type of event, such as a type of crime or incidents, based on its occurrence during a given interval of time. Histograms assist in assessing when crime is taking place and are effective tools for managing manpower and resources to prevent and deter crime.
- **Heat Matrices.** Heat matrices are used to depict the frequency of an event, such as a type of crime or incident, based on its occurrence during a specified interval of time. Each period of time is assigned a color based on the number of incidents that occur during that time. The higher the number of incidents, the brighter the color. This type of matrix provides an easy tool for visually assessing historical incidents of crime and reviewing when they took place to provide focus to police operations.

Hot Routes

4-85. Hot routes are another variation of crime concentration. While hotspots focus on geographic areas or points at which crime concentrates, crime often does not evenly distribute only to specific areas or points. For certain crimes, especially those that involve trafficking or smuggling, crime concentrations may extend over broad areas but concentrate along certain routes called hot routes. In these situations, rather than attempting to graphically represent the concentration of crime across all areas it crosses, a police intelligence analyst can identify the hot routes across which crime concentrates and visually depict movement, smuggling, or distribution patterns. For example, drug trafficking into the United States often originates from places in Mexico or beyond but follows certain hot routes into and throughout the United States to transport and distribute drugs from production centers to dealers and users.

4-86. Identifying the hot routes criminals rely on to move personnel or distribute illicit materials influences potential prevention and response approaches that decision makers can adopt. To enforce the rule of law and apprehend criminals offenders for prosecution, some situations may necessitate that deliberate checkpoints be established along hot routes to interdict offenders participating in criminal trafficking or smuggling. Other situations may use the understanding of multiple hot routes to determine the common origins or distribution points at which multiple hot routes converge. This type of approach may allow for a more significant disruption to a criminal network's distribution and smuggling activities than that of the simple interdiction of individual criminal elements. These examples demonstrate approaches and solutions that various crime analysis techniques can influence. They are linked to, and depend on, the purpose of the analysis and its end state, which is why the analysis was created. In these examples, if the objective is to portray to the community that the police are actively enforcing the law and aggressively reducing the number of criminal offenses, the first approach (concentrated enforcement along a hot route) may be the appropriate choice. However, if the intent is to disrupt and defeat a criminal network, the latter approach may be a better alternative.

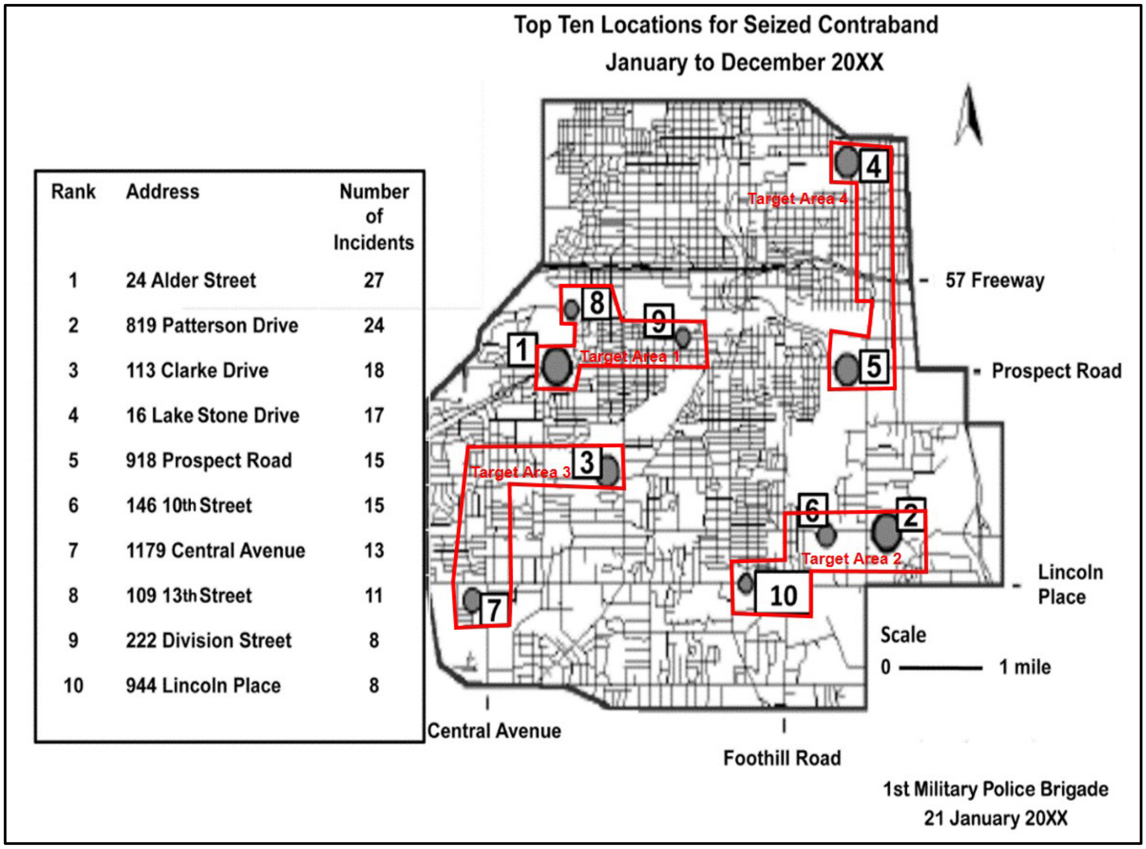
Terrain and Geospatial Analysis

4-87. Terrain analysisis conducted to understand the effects of terrain on operations. A terrain analysis in police operations has the same primary objective as it does in 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, and 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 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 for additional information of geospatial analysis.

4-88. Geospatial technology can greatly enhance the ability of police intelligence analysts to perform crime mapping. Leveraging such techniques allows for a clear and comprehensive depiction of crimes or other incidents by location, time, type, modus operandi, or other geospatial-enabled information such as physical infrastructure, political characteristics, or ethnic distributions. The programs used for geospatial analysis vary greatly in their ability to map, measure, compare, and analyze geospatial and temporal information; however, most rely on traditional geographic measures to provide map incidents, such as addresses, global positioning system coordinates, decimal-degree coordinates, or military grid reference system coordinates. Appendix B provides an example police intelligence product generated by using geospatial technology.

Geographic Distribution Analysis

4-89. Geographic distribution analysis is designed 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 police intelligence analyst to identify hot spots and facilitates geographic profiling to predict likely places for crime to occur. Geographic distribution analysis can also display locations of connected crimes, enabling the determination of probable bases of operation, offender residences, or other key locations. Geographic distribution analysis tools vary from incident mapping (using a physical map and colored pins, stickers, or other methods to identify specific occurrences 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. Figure 4-10 shows an example of the geographic distribution of crime hotspots that support why target areas were created and help focus law enforcement patrols conducting preventative police operations.



Top Ten Locations for Seized Contraband

January to December 20XX

Rank	Address	Number of Incidents
1	24 Alder Street	27
2	819 Patterson Drive	24
3	113 Clarke Drive	18
4	16 Lake Stone Drive	17
5	918 Prospect Road	15
6	146 10th Street	15
7	1179 Central Avenue	13
8	109 13th Street	11
9	222 Division Street	8
10	944 Lincoln Place	8

1st Military Police Brigade
21 January 20XX

Figure 4-10. Example of a geographic distribution of crime hotspots

Patterns

4-90. As humans interact through the routine activities of life, they establish patterns of behaviors, activities, and associations. Police intelligence analysts seek to understand the patterns of human activity that relate to or impact crime and criminal activity. They use several analytical techniques to achieve this understanding. These techniques are not used as singular methods, but they are often used concurrently with other techniques to complement and enhance each other. These techniques rely on qualitative and quantitative data. Qualitative data refers to nonnumerical data that lends itself to content analysis and the identification of patterns and associations. Quantitative data is typically numerical and statistical in nature and facilitates trend analysis. The techniques used by police intelligence analysts to understand patterns of human activity that impact crime and criminal activity include pattern analysis, crime pattern analysis, and understanding high-profile crimes, repeat incidents, crime series, and crime sprees.

Pattern Analysis

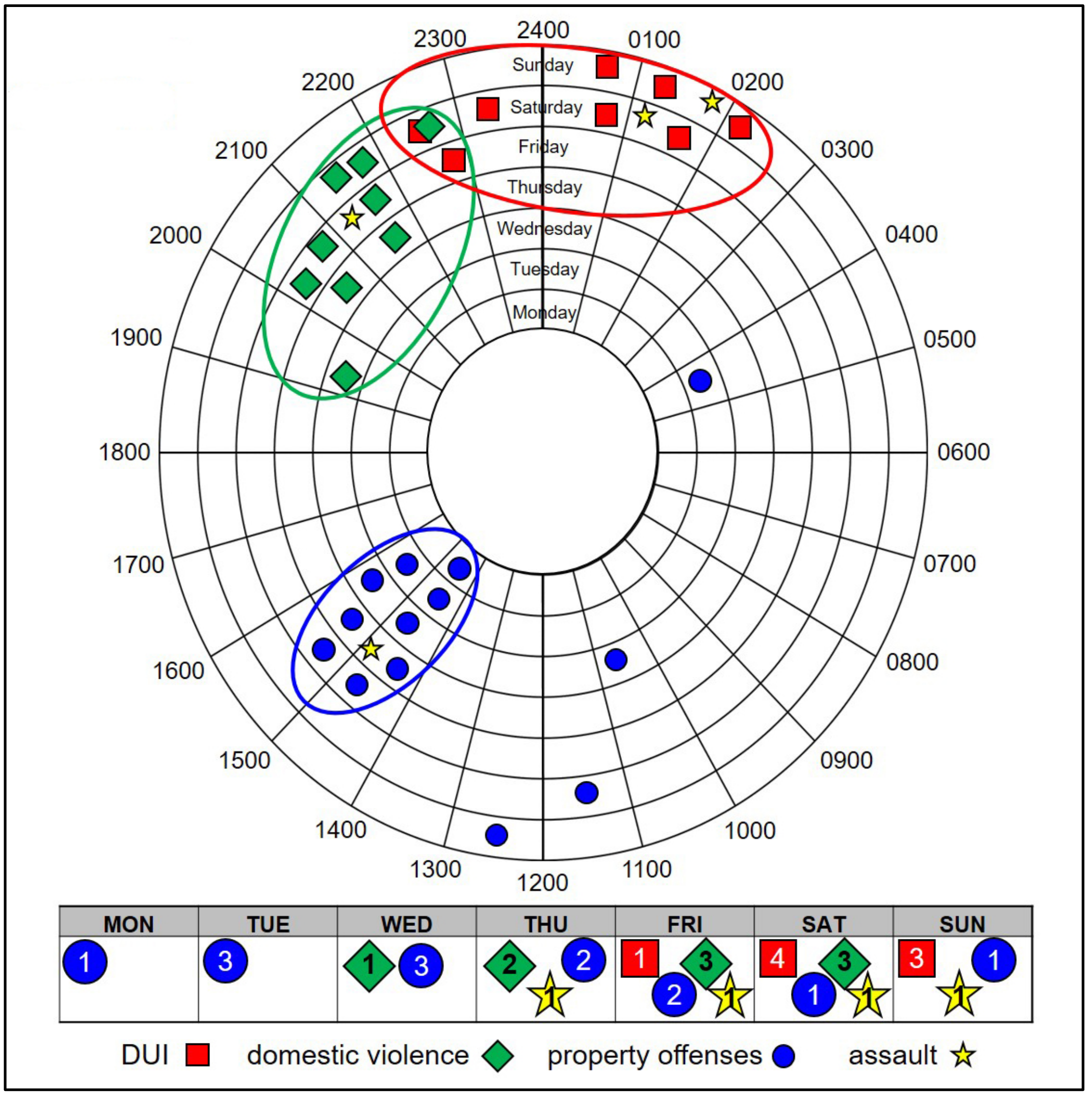
4-91. Pattern analysis is the process of identifying patterns of activities, associations, and events. A basic premise of pattern analysis is that these activities, associations, and events develop identifiable characteristics that can be used to produce meaning through analysis. A thorough analysis 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. Pattern analysis helps an analyst identify indicators of threat activity. See ATP 2-33.4 for additional information on pattern analysis.

Crime Pattern Analysis

4-92. While pattern analysis techniques can be used to analyze patterns across any type of human activity or association, crime pattern analysis specifically evaluates those patterns that people and networks establish which are relevant to understanding patterns of crime and criminal activity. Crime pattern analysis looks at the components of crime 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 criminal threats. Crime pattern analysis can be employed by using several different analytical methods discussed in this chapter (analysis of patterns, trends, networks, and the data association and flowcharting [time, event, and theme line charts]).

4-93. Police intelligence analysts use crime pattern analysis to generate police intelligence products that interpret crimes currently occurring; identify likely locations and times vulnerable to crime; and anticipate when, where, and what type of future crimes may occur. The predictive nature of crime pattern analysis helps military police and USACIDC personnel perform proactive crime prevention and police deterrence activities as part of their policing strategies. When coupled with S-2/G-2 efforts supporting decisive action, crime pattern analysis may support the identification of broader patterns across the operational environment (such as patterns of interaction or linkage between criminal and other threat groups) that may impact the common operational picture.

4-94. Figure 4-11 portrays a pattern analysis plot sheet depicting the analysis of four types of crimes spanning a weeklong timeframe. This pattern analysis plot sheet displays three kinds of information in one graphic display. The circular matrix is built concentrically into seven rings. Each ring identifies a different day of the week. The matrix is then divided into sections coinciding with the times of day. Lastly, the different types of crimes are depicted with different symbols. This tool is useful in identifying crime patterns because multiple types of information are displayed simultaneously in one graphic, allowing a police intelligence analyst to identify connections across different types of crime, times of day, and days of the week.



MON	TUE	WED	THU	FRI	SAT	SUN
● 1	● 3	◆ 1 ● 3	◆ 2 ● 2 ☆ 1	🟥 1 ◆ 3 ● 2 ☆ 1	🟥 4 ◆ 3 ● 1 ☆ 1	🟥 3 ● 1 ☆ 1

DUI 🟥 domestic violence ◆ property offenses ● assault ☆

Figure 4-11. Example of a pattern analysis plot sheet depicting crime patterns

High-Profile Crimes

4-95. High-profile crimes often have their own defining characteristics that make them stand out from other crimes. High-profile crimes may include murder, active-shooter events, or terrorism. These types of events attract significant media attention and may be perpetrated specifically for the perceived notoriety gained from such a crime or to advance a political or ideological narrative. Typically, high-profile crimes exhibit their own forms of patterns associated with their deliberate design to elicit media coverage or public attention. Because of the media attention given to high-profile crimes, they may inspire other offenders to imitate the crime for their own notoriety. Analysis of patterns of high-profile crimes can assist military police and USACIDC personnel in predicting what types of places or victims criminals may seek to target based on their ability to garnish high visibility or media attention, or they may seek to symbolically attack friendly vulnerabilities. Focusing crime analysis on these types of crimes can enhance vulnerability assessments and influence crime prevention, antiterrorism, and physical security efforts aimed at protecting vulnerable populations or hardening symbolically valuable targets.

Repeat Incidents

4-96. Repeat incidents occur when the same people, places, or activities occur that are nearly indistinguishable from each other. When an offender uses the same methods (or modus operandi), targets the same place, or victimizes the same person in multiple criminal incidents, the similarities in method, place, or victim may be analyzed to identify potential subjects or to protect the place or person being repeatedly targeted. For instance, crime analysis of multiple larceny offenses in an area may reveal patterns in the characteristics of places targeted (motorpools with poor lighting, no personnel present, and an abundance of landscaping offering concealment around access points) as opposed to the characteristics of those places not targeted (abundant lighting, rotational guards or staff duty personnel inspections, and no landscaping obscuring observation near access points) and show a common modus operandi (such as a lock on a gate cut with bolt cutters). Such specific patterns established across multiple separate criminal incidents suggest linkages and may result in the identification and apprehension of a subject or provide specific recommendations to the commander responsible for the place to enhance the crime prevention program.

Crime Series

4-97. A crime series occurs when two or more similar crimes are committed by the same individual (or group of co-offenders) against various victims or targets. Criminal offenders who succeed in a criminal act without being caught or punished are often emboldened to continue committing that crime. While a crime series may result from an offender's ongoing perception of the risk of being caught versus the reward of the crime, the patterns that emerge offer police intelligence analysts the opportunity to alter the situation by using crime analysis. For example, an offender may perpetrate a sexual assault by intoxicating a victim with the help of a group of accomplices. Given the fear, embarrassment, or reluctance of the victim to report the crime, the offender or co-offender may deem the effort successful and employ the same methods to commit a series of similar offenses. Analyzing the patterns associated with the crime series, such as similar places, methods, or victims, assists military police and USACIDC personnel in preventing and investigating such crimes.

Crime Sprees

4-98. A crime spree is a specific type of crime series that is characterized by such a high frequency of criminal incidents or activity that it appears almost continuous. It involves the same offender and usually occurs over a short period of time, but it may extend over a longer period of time when not addressed. Crime sprees typically occur in close proximity to a specific place and time and use similar methods that suggest that one offender is responsible for committing a series of crimes due to the similarity in location and techniques. An example of a crime spree may be when one offender commits multiple armed robberies across a small area that uses the same method (armed with semiautomatic pistol) and appears to be following a distinct pattern or route, suggesting the movement of an individual committing multiple crimes. When responding to a highly dynamic and unfolding crime spree, such as an active-shooter event, military police are often required to collect, process, and analyze incoming information intuitively to stop the perpetrator as rapidly as possible. Police intelligence analysts capable of rapidly analyzing and disseminating information to responding law enforcement patrols can greatly assist by shifting the cognitive burden of analysis in an ambiguous and time-constrained environment.

Problems

4-99. Crime analysis includes looking at crime through all possible stakeholder perspectives to understand the nature and causes of crime from the most holistic perspective possible. As part of this, crime analysis complements criminal analysis by integrating an analysis of all potential factors that may be creating crime problems, including population or societal problems, lack of policing capability or capacity to enforce the law or maintain order, and competing interests of relevant actors. The ability to generate crime analysis products to support problem solving greatly enhances the ability of military police commanders and staffs to solve crime problems through policing approaches and strategies, such as problem-oriented policing. See ATP 3-39.10 for a discussion of problem-oriented policing.

4-100. Crime problems may manifest themselves from simple to complex; therefore, organizational responses to crime problems are often dictated by the complexity of the crime problem at hand. At its most basic level, a single crime incident may involve relatively little complexity and be solvable by responding military police patrol, direct leadership (patrol supervisor, desk sergeant, watch commander), or law enforcement investigator (military police investigators, traffic management and collision investigator, or USACIDC special agent) based on purview. This level is the most direct and relies on professional techniques and procedures to collect evidence, conduct interviews and law enforcement interrogations, and derives conclusions based on specific evidence and information related directly to the criminal case.

4-101. At the next level, repeat incidents or multiple crimes across time and space may begin to exhibit patterns or connections that increase the complexity of solving the crime problem. The level of complexity within this space may range from connecting and linking multiple crimes by a single or multiple co-offenders to solve specific criminal cases, or it may extend across broader time and space horizons to indicate broader patterns of criminal activity. The range and scope determine the likely response. For multiple linked criminal incidents or repeat offenses, military police investigators or USACIDC special agents are the primary organizational levels solving the criminal incidents. However, as the scope and scale of crime patterns increase in time and space, the planning of military police and provost marshal staffs and the analysis of crime by police intelligence analysts become more critical. Crime pattern analysis uses aggregated data and pattern analysis techniques to make conclusions that address the factors influencing broader crime patterns.

4-102. The most complex aspects of solving crime problems are understanding and engaging to solve the underlying causes that produce or contribute to a crime incident and patterns. The fundamental root of crime problems is often impacted by factors outside the direct control of military police organizations. Therefore, as more complex factors contribute to problems, the commander or provost marshal (supported by staffs and police intelligence analysts) plays a more critical role in police engagement to coordinate police responses with external organizations and individuals to address the root causes of a crime problem. For instance, when crime continues to occur within an Army formation, issues internal to that organization (leadership, morale, discipline, the implementation of military justice) are crucial contributions to those crime problems. Military police commanders and provost marshals cannot solve these problems for an organization; however, they can contribute to the commander’s awareness and understanding of the problem to help supported commanders address the drivers of crime within their organization. Furthermore, crime problems often extend beyond the reach of military authorities entirely when the problem is generated by factors within civilian communities or in areas under civilian jurisdiction (inside or outside the United States). When this is the case, the requirement to engage, synchronize, or integrate the efforts of various unified action partners greatly increases the complexity of the problem and requires increased involvement by key organizational leaders and decision makers. See figure 4-12.

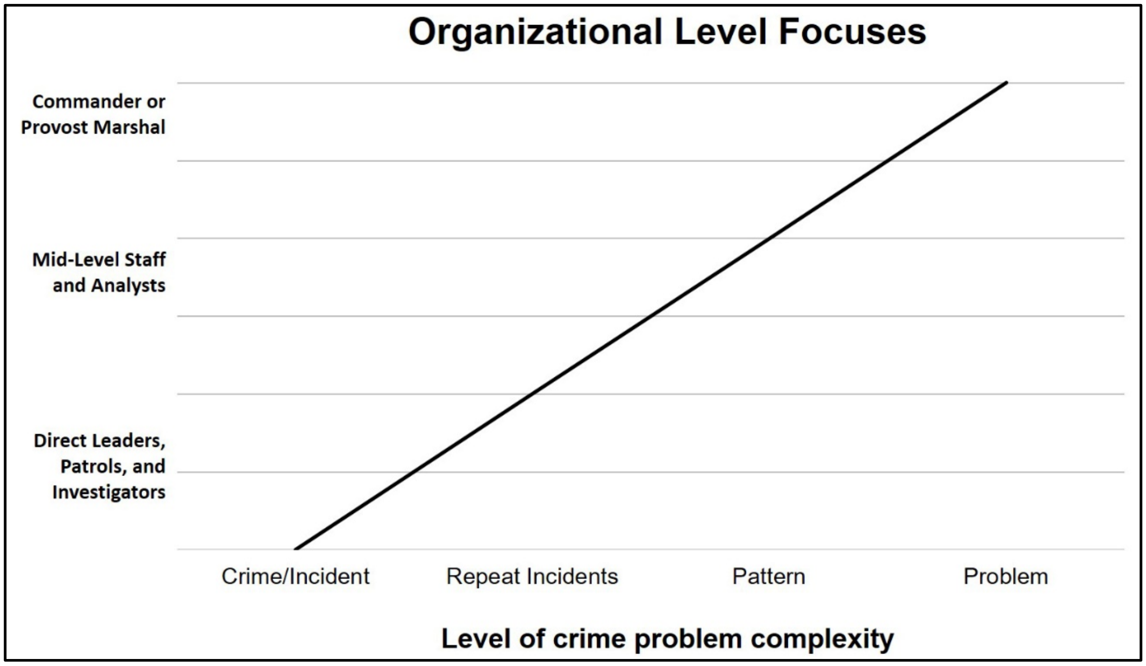


Figure 4-12. Organizational-level focuses based on the complexity of crime problems

Problem Analysis (Understanding the Root Causes of Crime)

4-103. Analyzing crime problems begins with an analysis of the criminogenic factors creating crime opportunities. Often crime is the surface symptom of deeper structural or environmental problems. By evaluating the conditions and situations that are causing crime rather than simply evaluating the incidence and effects of crime, police intelligence analysts can begin to understand the root causes of crime. Although it is essential to act on the symptoms of crime (respond to crime incidents, apprehend criminal offenders, and conduct criminal investigations to support the prosecution of criminal offenses), relying solely on removing criminal offenders from society without solving the underlying problems that are influencing individuals' choices to commit crimes will not result in reductions in crime across an area or population. Only by addressing the conditions that produce opportunities for additional potential offenders to engage in crime can criminal activity be confronted and reduced.

Analysis of Variables Influencing Crime Environments

4-104. Military police commanders and staffs analyze the operational variables and civil considerations that influence crime environments by using existing analysis tools inherent in the Army's military decisionmaking process (see FM 6-0) and IPB (see ATP 2-01.3). While using these standard analysis tools to ensure common language and understanding, military police analyze the operational environment from a policing perspective while maintaining a deliberate focus on crime, criminals, police and corrections institutions, and the drivers of instability and disorder. Table 4-4 provides several questions that military police should consider when assessing the operational variables as they relate to crime.

Table 4-4. Analysis of variables influencing crime environments

Variables	*Areas*	*Structures*	*Capabilities*	*Organizations*	*People*	*Events*
Political	Are there ungoverned areas where criminals operate with impunity? What political factors limit or constrain police enforcement in these areas?	Does the government fulfill governance functions, or are informal or criminal power structures predominant? What structure exist for upholding the rule of law?	Is the criminal justice system legitimate and effective? How much power or influence are criminals able to exert over political processes?	What organizations have the ability to influence crime in the area of operations? Are they capable and willing to enforce criminal laws? Have politicians or political institutions been corrupted by criminal organizations?	Who are influential actors with control or influence in the criminal justice system? Are they performing their duties according to the rule of law?	What political events have the potential for attracting criminal activities? Are political protest or rallies generally peaceful or violent in nature?
Military	What military assets are most vulnerable or exposed to criminal activity? Do military bases in the area provide criminals sanctuary?	Have criminal elements infiltrated or co-opted elements of the armed forces? Are there military-like criminal structures in the area of operations?	Do criminals possess military-like capabilities, such as crew-served weapons or explosives? Do criminals have connections to security forces that enhance their capabilities?	Do criminal organizations in the area of operations actively cooperate or affiliate with military forces? Are criminal organizations capable of organizing into para-military units similar in size to military forces?	Are there overlaps in personnel between military and criminal organizations? Do high-ranking military leaders have connections with criminal elements?	What military events or operations are threatened or vulnerable to criminal activities? Are there gaps or seams during military transitions that are exploited by criminals?

Table 4-4. Analysis of variables influencing crime environments (continued)

Variables	*Areas*	*Structures*	*Capabilities*	*Organizations*	*People*	*Events*
Economic	Where do criminal markets thrive? Are there poverty-stricken or depressed areas that may see high-levels of crime concentration?	Do illicit black markets exist outside the formal economy? Are there viable oversight structures in place to control illicit economic activity?	How do criminal organizations generate their profits? Do criminal organizations have control or influence over local front businesses, banks, or financial institutions?	Are banking or financial institutions corrupted or influenced by criminals? Do major corporations or companies have links to criminal organizations?	How does illicit money change hands between people? Are legitimate people or enterprises leveraged to launder or move illicit funds?	Do seasonal variations such as harvest seasons impact criminal activity? What economic events or activities are highly visible and offer opportunities to criminals?
Social	What impact does local culture and social demographics have on the level of crime in an area? Where do people concentrate their daily activities?	Are local social structures capable of controlling deviant behavior through informal social control?	Do informal mechanisms exist for settling disputes and grievances? How much social cohesion and collective efficacy exists in the society?	Do community or local social organizations exist to provide social goods? Do social or welfare organizations have connections or affiliations with criminal organizations?	What norms and values do people follow to gain honor, prestige, or acceptance in local communities? Are there local leaders or informal icons that people follow?	What types of events bring people together in daily life? Do criminals have influence or control over socially organized events?
Information	Do criminals have influence or control of radio, television, or other media platforms? Are there areas that facilitate criminal communication, such as street gathering points or graffiti markings?	What structures exist for criminals to spread their narratives or messages? Do criminals use methods, such as word- of-mouth, gang signs, or symbols, to pass information?	What information-related capabilities do criminals possess? How do they spread their narrative and messages among the population?	How are criminal organizations perceived by the population? Are they unwanted, or do people believe their narrative or accept their stated purpose, legitimacy, or capability?	Who has information regarding the people committing crimes? Do people know where criminals operate from and who is responsible for crimes?	

Table 4-4. Analysis of variables influencing crime environments (continued)

Variables	*Areas*	*Structures*	*Capabilities*	*Organizations*	*People*	*Events*
Infrastructure	Do criminals have access or control over critical infrastructure like power, communication, or transportation facilities?	Do criminals profit by extortion or bribery from infrastructure in the AO, such as tolls on roads or subsidies from power companies?	Do criminal organizations subsidize or provide people with critical economic needs like buildings, schools, roads, irrigation, or other economic infrastructure?	What level of infrastructure do criminal organizations directly control? What infrastructure do they have influence over through intimidation or bribery?	Who facilitates illicit activity for criminal organizations? Do local workers or farmers provide infrastructure criminal organizations depend on?	Do major infrastructure repair and maintenance events account for exposure to criminal activities?
Physical environment	Are there areas with degraded environmental conditions that signal to criminals and the population that laws are not enforced there? What and why are some areas targeted for crimes versus other areas?	Who is responsible for the places experiencing crime across the area of operations? Are business owners or other place managers actively controlling crime on their properties?	Will alterations to the physical environment impact or reduce the level of crime in an area such as improving physical security or hardening facilities? Can crime prevention through environmental design principle be implemented?	How do criminal organizations perceive the physical environment? Do they find it conducive to their criminal activities, offering maximum benefits with minimal risks of being caught? Or do they perceive significant risks to overcome?	Do populations feel safe and secure in their environment, or do they fear crime due to environmental cues? Who has control or influence over making improvements to the physical environment?	Do people who coordinate events account for crime prevention considerations? Are criminals able to easily access vulnerable populations gathered for an event?
Time	How are criminal areas impacted by time considerations? Do criminals only operate within certain distances from sanctuaries or safe havens to accommodate rapid escape?	How is time understood and leveraged in local culture and society? Do different understanding or ways of relating to time impact criminal activities?	How do time considerations enhance or limit criminal opportunities? Do short intervals of exposure reduce opportunities and increase risk, or are assets exposed for long durations, lowering risks to criminals?	How do criminal organizations organize their functions and activities in time? Do they operate mostly during daytime or nighttime? Do their activities vary by weekly or seasonal patterns?	Do people follow predictable patterns in time that expose them to criminal activity? Are daily activity patterns well known to criminals who may seize a crime opportunity while property is unguarded?	When are major events that may generate criminal activity occurring? Do these events provide temporal insights into when and where to expect criminal activity?

4-105. Understanding crime environments not only means understanding criminal threats but also understanding friendly or allied forces that can counter the threat. Before seeking to solve crime problems within a jurisdiction or area of operations, it is essential to properly understand the police force that is responsible for conducting police operations. When supporting HN police training, misunderstanding HN police capabilities, cultural paradigms, approaches to policing, taboos and internal bias, and information related to the nature of the police force may result in solutions that make sense from a U.S. perspective but fail because they are incompatible to the force responsible for action.

Police Infrastructure Analysis

4-106. 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 DSCA, to include operations in support of HN police and corrections institutions, 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.

4-107. Military police have developed the POLICE memory aid to guide the assessment of civil considerations that is focused on police activities, available 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 early identification enables commanders to identify criminal threats, potential disruptive events, and police capability and capacity to prevent them. See chapter 5 for further discussion of the POLICE memory aid as part of military police support to the IPB.

Police Operations Analysis

4-108. Assessing the effectiveness of military police operations in solving crime problems is critical to reducing crime, disorder, and fear of crime. Police activity does not automatically result in progress. Similarly, the presence of police alone does not automatically indicate an absence of crime and criminal activity. Military police operations are focused toward producing measurable change in the operational environment through the reduction of crime and its effects. Evaluating whether or not current policing strategies and approaches are producing the desired results is essential to effective police operations. Military police measure the effectiveness of police operations by conducting police operations analysis.

4-109. Operational 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 regularly conduct operations analysis to assess and improve their own operations. Military police also support unified land operations by conducting assessments of HN policing and corrections capabilities to understand a partner force's capability and capacity to establish civil control, enforce laws, apprehend and prosecute criminal subjects, and incarcerate convicted criminal offenders. This support is crucial to successful stabilization, but it must occur early enough in the planning and execution of an operation to determine the critical police infrastructure and effectiveness before transitioning to the consolidation of gains.

POLICE INTELLIGENCE PRODUCTS

4-110. There are several types of police intelligence products that may be produced and disseminated to fulfill information and intelligence requirements and influence military police efforts to prevent, deter, and solve crime problems. The particular type and focus of police intelligence products developed depend on the purpose they are meant to serve and can generally be categorized as criminal intelligence or crime analysis. While these categories assist in organizing and thinking about the different aspects of police intelligence based on their focus, there is significant overlap between categories as the various aspects of crime are examined. Generally, the products that produce knowledge of crime in relation to places, patterns, and problems are crime analysis products, while those products that focus on the people responsible for the crime are criminal intelligence products. Figure 4-13 demonstrates different focuses of criminal intelligence and crime analysis.

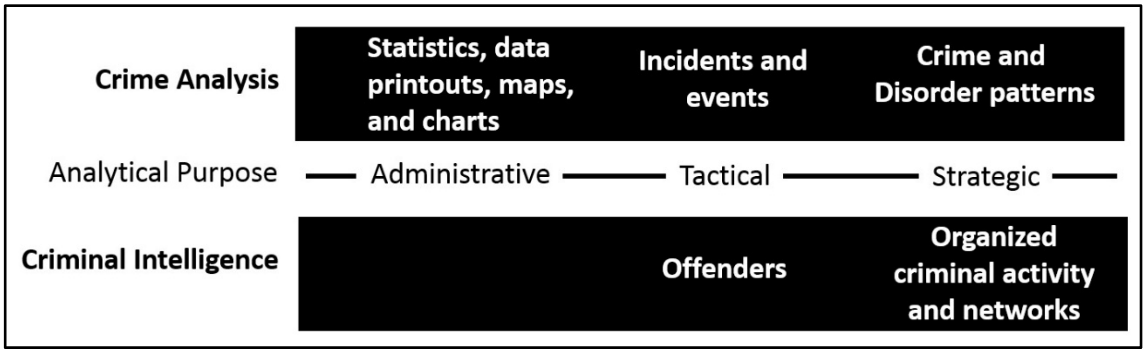


Figure 4-13. Crime analysis and criminal intelligence focus

4-111. During criminal and crime analysis, several analysis techniques generate products in the course of analysis that require minimal adjustment before dissemination. These include such products as crime maps, link analysis diagrams, association matrices, criminal threat assessments, and vulnerability assessments. However, some police intelligence products require applying the knowledge and understanding generated during analysis to produce standardized reports, summaries, alerts, notices, and other types of products. This section provides descriptions of many of these types of products; several other examples are provided in appendix B. The products discussed are not all-inclusive and do not include common types of products that are redundant with other military staff and intelligence processes, such as information papers, staff studies, decision briefs, and intelligence summaries. These products do not limit creative and innovative police intelligence analysts from using additional techniques and methods to solve unique crime problems or generate police intelligence products in other ways within the scope of local demands and standard operating procedures.

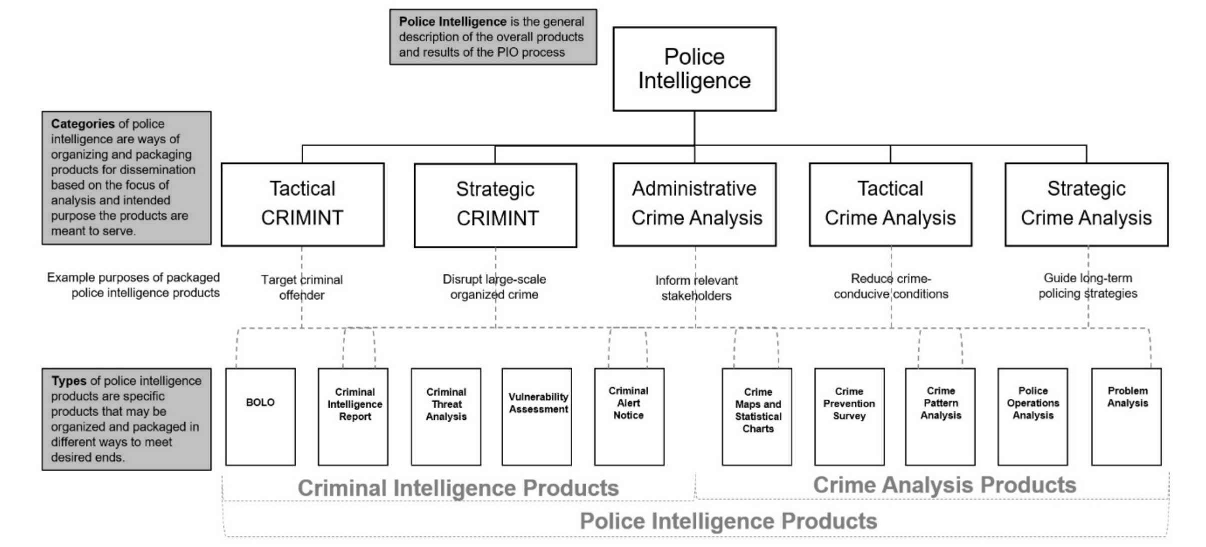
4-112. Police intelligence products generally contain basic police information and analyzed police intelligence. It is important to keep the intended recipient and purpose at the forefront during production. Failure to do so may result in producing multiple documents, each with a specific audience and purpose. Regardless of the format employed, producers of police intelligence must take extreme care to ensure the accuracy of the products and the protection of classified or sensitive information. Police 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.

Note. The term law enforcement-sensitive is used to identify information or intelligence that is obtained for, processed through, or managed by law enforcement organizations. It is essential that the information is restricted to law enforcement channels unless otherwise directed by a competent authority.

4-113. Police intelligence products generated by military police, 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 police intelligence required are very different from the operational or strategic level. The staff and analyst must fully understand the information and intelligence requirements and the specific needs of the target audience to deliver a product that enables decision making appropriate to the level of the recipient.

4-114. The criminal and crime analysis processes result in distinct but related knowledge and understanding about different aspects of crime. The criminal analysis process focuses on criminal offenders and organized criminal activity to produce tactical and strategic criminal intelligence that enable military police to anticipate and predict criminal behavior and activity. This predictive focus enables military police to implement policing strategies to anticipate, prevent, or monitor criminal activity to reduce the capability or impact of criminal threats. From this perspective, criminal intelligence may be used to monitor, investigate, and apprehend criminal offenders or disrupt criminal networks responsible for criminal activity.

4-115. The crime analysis process results in tactical and strategic crime analysis products that focus attention on understanding crime incidents and environments based on the analysis of information and data obtained after crimes have occurred to understand the factors generating crime opportunities and the root causes of crime problems. This understanding enables military police to focus resources to solve criminal incidents and crime problems and addresses the underlying causes of crime, disorder, and fear of crime within an area of operations. Crime analysis also produces the administrative crime analysis products that military police staffs and police intelligence analysts use to inform audiences, communicate to relevant stakeholders, and facilitate police engagement. Figure 4-14 provides an example of various police intelligence products that may be packaged into the categories of police intelligence, depending on their purpose and desired end state.


Police Intelligence is the general description of the overall products and results of the PIO process
Police Intelligence
Categories of police intelligence are ways of organizing and packaging products for dissemination based on the focus of analysis and intended purpose the products are meant to serve.
Tactical CRIMINT
Strategic CRIMINT
Administrative Crime Analysis
Tactical Crime Analysis
Strategic Crime Analysis
Example purposes of packaged police intelligence products
Target criminal offender
Disrupt large-scale organized crime
Inform relevant stakeholders
Reduce crime-conducive conditions
Guide long-term policing strategies
Types of police intelligence products are specific products that may be organized and packaged in different ways to meet desired ends.
BOLO
Criminal Intelligence Report
Criminal Threat Analysis
Vulnerability Assessment
Criminal Alert Notice
Crime Maps and Statistical Charts
Crime Prevention Survey
Crime Pattern Analysis
Police Operations Analysis
Problem Analysis
Criminal Intelligence Products
Crime Analysis Products
Police Intelligence Products

Legend:

BOLO	be-on-the-lookout
CRIMINT	criminal intelligence
PIO	police intelligence operations

Figure 4-14. Example hierarchy of police intelligence products

CATEGORIES OF CRIMINAL INTELLIGENCE

4-116. Criminal intelligence results from the analysis of criminal aspects of compiled police information that, upon dissemination, informs efforts to anticipate, prevent, or monitor criminal activity. Criminal intelligence focuses on identifying specific criminal offenders, co-offending networks, and criminal organizations to understand criminal threats, enable monitoring and police operations aimed at preventing or mitigating criminal activity, or targeting criminals for apprehension. Criminal intelligence can be categorized as tactical criminal intelligence and strategic criminal intelligence based on the purpose it is intended to serve.

Tactical Criminal Intelligence

4-117. Tactical criminal intelligence is focused on the short-term development of patrol and investigative priorities aimed at anticipating, monitoring, and apprehending individual criminal offenders and co-offenders responsible for specific crimes. This type of criminal intelligence is directly linked to and should support, immediate action by military police and USACIDC personnel to interdict criminal threats, observe the activities of local criminal organizations, and target criminal offenders for apprehension based on the commission of specific criminal offenses. Techniques such as criminal threat analysis; criminal target analysis; and link, association, and network analysis are critical to identifying specific criminal offenders responsible for the commission of crimes.

Strategic Criminal Intelligence

4-118. Strategic criminal intelligence focuses on organized criminal activities carried out by large-scale criminal networks and transnational (or transregional) criminal organizations. This focus enables products that support the long-term development of understanding of the organizations, functions, activities, and connections of criminal organization to implement sustained strategies to monitor, infiltrate, disrupt, or defeat large-scale organized criminal activity. This approach significantly differs from tactical criminal intelligence in that tactical criminal intelligence targets individual criminal offenders linked to specific crimes for apprehension, prosecution, and incarceration. Strategic criminal intelligence proceeds from the premise that criminal organizations will survive and continue to thrive despite the loss of individual criminal actors as long as the organization can still offer potential criminals incentives for benefits that outweigh the perceived costs or risks. Based on this premise, strategic criminal intelligence supports a more systems-based approach to countering criminal networks and dismantling criminal organizations.

TYPES OF CRIMINAL INTELLIGENCE PRODUCTS

4-119. Criminal intelligence products share information about known or suspected criminals with relevant and authorized stakeholders to gain credible information that may assist in the investigation or apprehension of criminal offenders or inform the public of active criminal threats. This section discusses those types of police intelligence products that focus on criminals, criminal threats, and organized criminal activity.

Criminal Intelligence Bulletin

4-120. 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. See appendix B for an example criminal intelligence bulletin.

Criminal Intelligence Reports

4-121. Criminal intelligence reports (or 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 criminal intelligence that identifies patterns, methods of operation, organized criminal networks, technology used by criminal threat elements, intelligence requirements, or concerns involving criminal organizations and activities. See appendix B for an example criminal intelligence report.

4-122. 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.

Criminal Alert Notice

4-123. The criminal alert notice is a document prepared by Army law enforcement elements that expedites the reporting of perishable, time-sensitive, and crime-related information. A criminal alert notice is prepared and disseminated to attack an offender's capability to victimize 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 criminal threat. See appendix B for an example criminal alert notice.

4-124. The criminal 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 criminal alert notice is an action document, not an informational report. It is therefore considered a criminal intelligence product rather than simply administrative crime analysis produced to inform the public. Criminal alert notices follow the same basic format that typically includes the—

- Source and reliability of the information.
- Entities involved.
- Known aliases.
- Known personal identification numbers (social security number, driver's license number).
- An up-to-date summary of pertinent information developed 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.

Be-On-The-Lookout Alert

4-125. A BOLO alert is routinely sent out by Army and civilian law enforcement agencies. It 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.

4-126. A BOLO alert may be general or very specific; however, 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, issuing a BOLO alert for a grey sedan automobile to all military police units operating in Germany or for 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 or 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. See appendix B for example BOLO alerts.

Wanted Posters

4-127. 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.

4-128. 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 is a short description and brief history of the criminal listed 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.

4-129. 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 may have a point of contact if additional information is known. 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 also provide points of contact for persons with potential information.

4-130. 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. See appendix B for examples of wanted posters.

Reward Posters

4-131. 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. Similar to 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 appendix B 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) that are 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 referencing the information received.
- Any applicable expirations of the reward offer.

Link Analysis Products

4-132. 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. See appendix B for an example link analysis product.

4-133. 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. The use of automated analytical systems can greatly enhance the ability of police intelligence analysts to use filtering tools to tailor products easily and rapidly for the appropriate audiences.

Forensic Analysis Reports

4-134. Forensic analysis reports are produced at laboratories that conduct forensic examinations of collected materials. These reports are usually produced according to the standards of the laboratory conducting the analysis. When supporting law enforcement investigations, the reports 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 readable format. Law enforcement investigators who review forensic reports should directly contact serving laboratories for clarification or for an explanation of evidence or to correlate the results of other investigative findings.

4-135. In support of decisive action, forensics analysis reports developed in forensic exploitation 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 regarding biometrics information to the intelligence community.

Economic Crime Threat Assessment

4-136. The economic crime threat assessment report is a USACIDC assessment of the overall economic posture of an installation or activity. The economic crime threat assessment process is one of the most important aspects of the USACIDC crime prevention program. Economic crime threat assessments provide valuable information and criminal intelligence to enable the effective employment of limited USACIDC and other law enforcement assets. An economic crime threat assessment is an important element for a proactive effort that relates to economic crimes and logistic security operations.

Logistics Security Threat Assessment

4-137. The logistics security threat assessment report is produced by USACIDC special agents looking specifically at key logistic bases and infrastructure. The logistics security threat assessment 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 communication, the security of U.S. government assets, and the safety of DOD personnel. A logistics security threat assessment report 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, logistics security threat assessments are normally classified.

Personal Security Vulnerability Assessment

4-138. 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 includes a review of the procedures and measures employed for the high-risk personnel at the residence and workplace and for travel between the two locations. The personal security vulnerability assessment scrutinizes all aspects of the physical security of the high-risk individual's (or principal's) residence, workplace, and mode of travel. A review and analysis of the principal's routine habits, 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.

4-139. All supporting documentation (blueprints, schematic drawings, still photographs, videos, written documents) are 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. The conduct of a personal security vulnerability assessment is directed in AR 10-87, AR 190-58, and AR 525-13.

4-140. 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.

CATEGORIES OF CRIME ANALYSIS

4-141. Crime analysis products result from the systematic organizing and analyzing of police information to determine who, what, when, where, and why crime, disorder, fear of crime, and other destabilizing events occur in specific places to apprehend criminal subjects, prevent crime, solve crime problems, and measure police effectiveness. Crime analysis products focus on understanding the environmental and spatial-temporal variables influencing perceptions of crime and disorder, crime opportunities, and victim or target vulnerabilities and on creating conditions conducive to criminal activity. These products can be categorized as administrative crime analysis, tactical crime analysis, or strategic crime analysis based on the focus of the crime analysis process and the outcomes they are intended to serve.

Administrative Crime Analysis

4-142. Administrative crime analysis is directed at the administrative needs of the military police, corrections, government partners, and communities. Examples include providing community town hall participants updates on crime trends in specific neighborhoods; preparing briefings for installation or unit commanders to highlight crime across an installation or area of operations; preparing military police activity reports, sketches, and diagrams; developing press releases in responses to media request; and producing other products used in crime analysis to support the administrative functions of military police or other relevant stakeholders.

Tactical Crime Analysis

4-143. Tactical crime analysis is focused on the short-term development of patrol and investigative priorities and the deployment of resources to achieve immediate organizational or community objectives. The focus includes geographic distribution or concentrations of crime, crime hotspots, high-profile crimes, repeat incidents, and crime patterns. Tactical crime analysis enables military police and USACIDC personnel (or supported organizations) to take immediate actions directed at reducing crime-conducive conditions, enhancing crime prevention strategies, or protecting places susceptible to crime.

Strategic Crime Analysis

4-144. Strategic crime analysis supports the procurement of resources and the evaluation of crime reduction and prevention strategies and influences policy development and implementation to support long-term organizational or community objectives. The focus includes long-term statistical trends, patterns, hotspots, and crime problems. Strategic crime analysis enables decision makers (military police or supported commanders) to develop long-term strategies to address the root causes of crime by engaging relevant stakeholders (unit commanders, community leaders, business owners, and other unified action partners) to implement structural or organizational changes to solve the underlying factors responsible for producing crime versus simply solving the symptoms of crime. This focus enables military police to implement proactive versus strictly reactive approaches to policing.

TYPES OF CRIME ANALYSIS PRODUCTS

4-145. Several products may be created during crime analysis that focus specifically on the crime aspects of the environment. These crime-focused products are used to display or describe aspects of crime to fulfill information or intelligence requirements or influence decisions regarding crime problems and crime environments. Many crime analysis products are generated through the conduct of the crime analysis process versus deliberately prepared reports following analysis. These types of crime analysis products are discussed earlier in this chapter. This section discusses additional crime analysis products that may be produced from the understanding and knowledge generated through crime analysis.

Crime Maps

4-146. Although crime mapping is an analysis technique, the resulting product is a crime map. Crime maps provide visual depictions of crime and criminal incidents in geographic space. These products may include crime incident pin maps, geospatial displays of crime concentrations, crime density or hotspot maps showing the path to and from a crime scene that a criminal offender used to commit a criminal act. See figure 4-8 and figure 4-10 for example crime maps.

Crime Prevention Survey

4-147. 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 is designed to help 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.

4-148. 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 identifies 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—

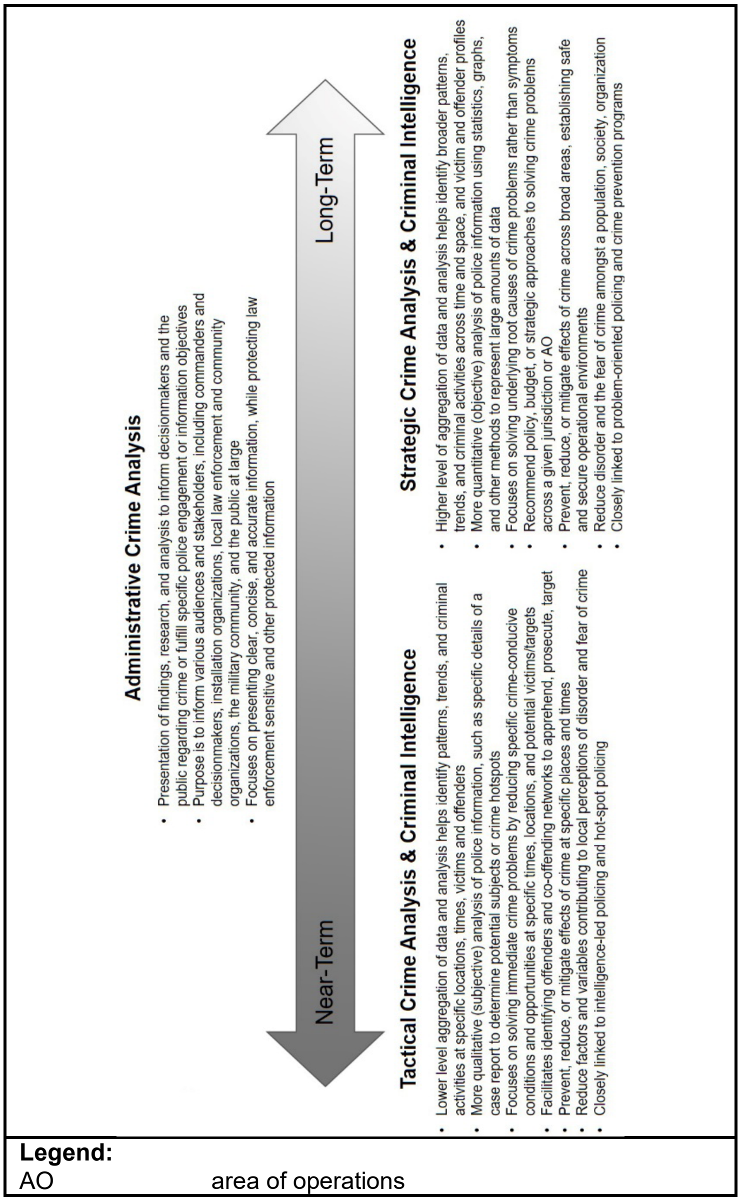
- Criminal activity in a specific location.
- Regulatory deficiencies.
- Economic threats to installations or activities.
- Domestic and international terrorist threats.
- Likely theft, diversion, sabotage, or destruction of U.S. government property or assets.
- Vulnerability of Army automated systems.

Crime Prevention Flyer

4-149. 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 a 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. See appendix B for an example crime prevention flyer.

Crime Forecast

4-150. Crime forecasting relies heavily on trend and pattern analysis. Trend analysis may depict historical trends to predict future events or trajectories in crime rates and criminal activity. For instance, crime data may show that crime trends are increasing or decreasing in a certain area. This information may be used to project continued trends in a particular manner or direction. Similarly, pattern analysis may also be used to anticipate a particular crime condition or outcome based on patterns of activity and crime data from previous similar conditions. For instance, crime data may reflect that previous redeployments have increased crime incidents on an installation and may be able to identify patterns of locations or problems that seem to show patterns during similar conditions. In response to this analysis, military police and USACIDC personnel may present anticipated crime forecasts to unit commanders to enable mitigation efforts to prevent those same crime patterns from occurring (limiting alcohol consumption for a period of days during the initial reintegration and assessment of current crime problem locations that show patterns of alcohol-related offenses). Figure 4-15 shows the different temporal focuses of criminal intelligence and crime analysis.


Administrative Crime Analysis
• Presentation of findings, research, and analysis to inform decisionmakers and the public regarding crime or fulfill specific police engagement or information objectives
• Purpose is to inform various audiences and stakeholders, including commanders and decisionmakers, installation organizations, local law enforcement and community organizations, the military community, and the public at large
• Focuses on presenting clear, concise, and accurate information, while protecting law enforcement sensitive and other protected information
Near-Term
Long-Term
Tactical Crime Analysis & Criminal Intelligence
• Lower level aggregation of data and analysis helps identify patterns, trends, and criminal activities at specific locations, times, victims and offenders
• More qualitative (subjective) analysis of police information, such as specific details of a case report to determine potential subjects or crime hotspots
• Focuses on solving immediate crime problems by reducing specific crime-conducive conditions and opportunities at specific times, locations, and potential victims/targets
• Facilitates identifying offenders and co-offending networks to apprehend, prosecute, target
• Prevent, reduce, or mitigate effects of crime at specific places and times
• Reduce factors and variables contributing to local perceptions of disorder and fear of crime
• Closely linked to intelligence-led policing and hot-spot policing
Strategic Crime Analysis & Criminal Intelligence
• Higher level of aggregation of data and analysis helps identify broader patterns, trends, and criminal activities across time and space, and victim and offender profiles
• More quantitative (objective) analysis of police information using statistics, graphs, and other methods to represent large amounts of data
• Focuses on solving underlying root causes of crime problems rather than symptoms
• Recommend policy, budget, or strategic approaches to solving crime problems across a given jurisdiction or AO
• Prevent, reduce, or mitigate effects of crime across broad areas, establishing safe and secure operational environments
• Reduce disorder and the fear of crime amongst a population, society, organization
• Closely linked to problem-oriented policing and crime prevention programs

Legend:	
AO	area of operations

Figure 4-15. Criminal intelligence and crime analysis focuses

WARNING INTELLIGENCE

4-151. *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 U.S. entities, partners, or interests (JP 2-0). The S-2/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. PIO is planned and executed by the S-3 in functional units and by the provost marshal staff in multifunctional units; police intelligence that may contribute to warning intelligence is immediately coordinated with the S-2/G-2 to ensure timely dissemination.

4-152. 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 and units. Military police provide police information or analyzed police intelligence for timely notification that a possible criminal threat or terrorist attack on U.S. interests has been identified and is imminent.

4-153. The nature of a threat indicator generally dictates 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/G-2, and the commander are normally notified of incoming warning intelligence. As with other police intelligence products, a decision must be made concerning how much information should be released and whether sources of information must be protected in the warning.

AUTOMATION TOOLS FOR ANALYSIS AND PRODUCTION

4-154. Automation increases the capability to correlate large volumes of information from many sources and assists in criminal and crime analysis. Interpretation of the information requires a police intelligence 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 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. Automation enables the effective and efficient flow of information from collection to production through data entry by military police collection assets to data retrieval and analysis by police intelligence analysts.

Automated Databases

4-155. A database is a tool for organizing and storing data and information. A database can store information about people, types of events, or any other information. 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.

4-156. 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 decision making 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, key word searches).

Army Law Enforcement Reporting and Tracking System

4-157. A central feature of ALERTS is the common repository of police information that allows law enforcement personnel across the Army to access common information, reports, and standards to support local analysis processes. Given the common access to this database by law enforcement officers across the

Army, the gaps that previously existed between military police and USACIDC data storage systems have largely been eliminated.

Distributed Common Ground System-Army

4-158. The DCGS-A provides the ability to access data from tactical to national sensors across the national to tactical intelligence effort and facilitates reach with collaboration capabilities for deployed elements. Each intelligence discipline has unique databases established and maintained by a variety of agencies. Database access is accomplished through unit or agency homepages via SIPRNET and the Joint Worldwide Intelligence Communications System.

Automated Analytical Tools

4-159. The automation of analytical tools 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. (See appendix B for several police intelligence products generated using automated analytical tools.) Automated analysis software includes computer-assisted analytical programs that reduce the time required for analysis. These programs help the police intelligence analyst develop predictions and identify information gaps to support collection and targeting. 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.

Army Law Enforcement Reporting and Tracking System

4-160. Besides being a database and repository for police information, ALERTS also provides analytical tools and capabilities that enable police intelligence analysts to perform criminal and crime analysis. Many of the analysis techniques explained in this manual can be performed by using the tools inherent to ALERTS or by using the data stored in ALERTS. ALERTS supports analysis and production with several tools, reports, and product outputs that can be generated by using ALERTS. These include law enforcement reports, crime prevention surveys, BOLOs, criminal intelligence reports, raw data files, and reports that enable analysis and manipulation using common spreadsheet programs to determine patterns or develop charts to depict police information and police intelligence.

Commercial Automated Analytical Tools

4-161. Besides fielded systems like ALERTS and DCGS-A, there are several commercial automation solutions that currently support criminal and crime analysis. The Crime and Criminal Intelligence Analyst Course provided by USAMPS employs the i2 Analyst Notebook to perform criminal and crime analysis. The i2 Analyst Notebook (which is also used within the DCGS-A) is one of many commercial products used to perform these analysis processes. Military police organizations such as USACIDC are equipped with the i2 Analyst Notebook on a limited scale. While this is a current solution that is being employed across the military police force, there are several other tools that are available to perform the same criminal and crime analysis techniques across federal and local police and law enforcement agencies. See appendix B for several examples of police intelligence products generated using the i2 Analyst Notebook.

Geographic Information Systems

4-162. 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 information 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. Data is typically imported from an existing database or is manually input 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.

4-163. 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 analysis of dense urban environments. 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 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 decision making where a law enforcement raid or special reaction team mission is planned.

Preparing Police Intelligence Products for Dissemination

4-164. Police intelligence products are fed into police, detention, and investigative missions through various policing strategies and investigative processes and into the Army operations process through the integrating processes (IPB, targeting, and risk management). This dissemination allows military police personnel, commanders, and staffs to make decisions ranging from policy, budgeting, and resource allocation to direct tactical action to reduce crime, eliminate crime-conducive conditions, target criminal offenders and networks, and establish safe and secure environments for U.S. forces, allies, and HN populations across the range of military operations.

4-165. Police intelligence products must be integrated into the operations process and the common operational picture to affect operations. Integrating police intelligence in tactical plans exploits the police information gathered and promotes the emergence of a common operational picture. As police information continues to be collected, processed, and analyzed, a more holistic picture begins to emerge.

This page intentionally left blank.

Chapter 5

Disseminate

This chapter describes step four of the PIO framework: disseminate. This step focuses on sharing police information and police intelligence with relevant stakeholders to enhance situational awareness and influence decision making. Dissemination serves several purposes. The primary purpose of police intelligence dissemination is to shape military police operations conducted to prevent, mitigate, and respond to crime and criminal activity. Disseminating police intelligence also supports the Army operations process through the integrating processes to support situational awareness, contribute to the common operational picture, and affect decision making.

DISSEMINATION, COLLABORATION, AND FUSION

5-1. 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, influence decision making, and enable action. It is critical that dissemination occurs as early in the process as practical and possible. The need to balance speed with thoroughness should be weighed throughout the process. Commanders and police intelligence analysts should consider interim reports to provide key information 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 those who need it.

5-2. Dissemination delivers relevant information to the right personnel, units, or agencies and 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 police information or police intelligence disseminated.
- Operates in an area of operations that may be directly or indirectly impacted by 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 police information or police intelligence.

5-3. Police intelligence is often maintained in law enforcement functional channels. Functional channels include military police, law enforcement channels, and other groups that operate along functional lines. The law enforcement and intelligence networks are examples of functional channels. Functional channels are established to maintain control over sensitive information (as mandated by law) and to protect police information and police intelligence critical to ongoing law enforcement investigations and operations.

5-4. In support of decisive action, PIO allows command and staff channels to ensure timely and accurate reporting of police information and police intelligence that answers intelligence requirements, CCIRs, or information identified by the staff or commander that is unanticipated but of immediate value to the command. Command and staff channels are also likely used to distribute other products (wanted posters, spot reports, BOLOs). This is typically 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.

5-5. Within a deployed operational environment, military police leaders continuously collect, organize, and analyze police information. Military police units constantly update internal tracking systems and report police information and police intelligence to higher, lower, and other relevant units to facilitate the operations process. This information (and subsequent analysis) is also used by military police during the IPB process to continuously assess criminal threats and other crime-related aspects of the operational environment. Police intelligence analysts—

- Update previous police/criminal estimates provided to the S-2/G-2.
- Identify new or potential irregular threats (criminal, terrorist, and insurgents), networks, and trends in the area of operations.
- Recommend protection-level changes to the supported commander.
- Notify adjacent units of the potential irregular threats (criminal, terrorist, and insurgents), networks, or trends that may affect their forces.
- Reprioritize military police operations and support to the identified threat area.
- Share the information with HN/local police and other agencies as appropriate.

DISSEMINATION CONSIDERATIONS

5-6. 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 users are the personnel or organizations that initiate the requirement and need the products to perform law enforcement 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.

> ***Note.*** 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 about U.S. persons is generally subject to more restrictions than sharing information about non-U.S. persons. Additionally, individuals detained outside the U.S. 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.

5-7. 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 a new classification.

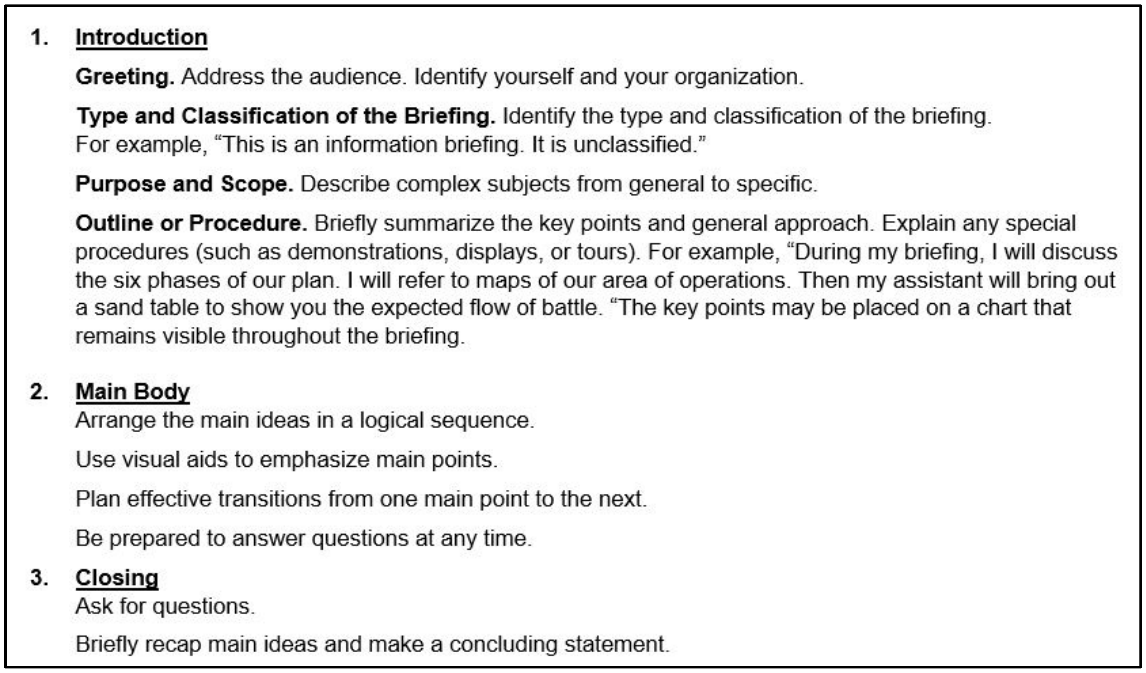
5-8. The classification of a document or data may be required to protect an informant or law enforcement source; a monitoring capability; a tactics, techniques or procedure for gathering police information. It may be possible to prevent the creation of a classified product simply by protecting the manner in which the information is collected or processed. If 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 the compromise of information or intelligence. Coordination with the local offices responsible for computer network defense and security issues should be managed to ensure that security requirements are maintained.

5-9. Military police and USACIDC personnel must also determine which method will be used to disseminate police intelligence products. Dissemination may be conducted through verbal, written, interactive, or graphic formats and systems. 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. Regardless of the method used, military police and USACIDC personnel must ensure that products are delivered to the appropriate users when, where, and in the proper format needed. Frequently, when police intelligence products are delivered, additional information requirements are identified for collection.

> ***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.

Briefings and Reports

5-10. Military police and USACIDC personnel disseminate police information and police intelligence through various forms of briefings and reports. A police intelligence briefing may be conducted to share police information and police intelligence through face-to-face means to communicate important aspects of crime environments and criminal threats or to share critical information directly with decision makers in a clear and concise format. Figure 5-1 provides a general information briefing format as a guide for executing police intelligence briefings.



1. **Introduction**

   Greeting. Address the audience. Identify yourself and your organization.

   Type and Classification of the Briefing. Identify the type and classification of the briefing. For example, "This is an information briefing. It is unclassified."

   Purpose and Scope. Describe complex subjects from general to specific.

   Outline or Procedure. Briefly summarize the key points and general approach. Explain any special procedures (such as demonstrations, displays, or tours). For example, "During my briefing, I will discuss the six phases of our plan. I will refer to maps of our area of operations. Then my assistant will bring out a sand table to show you the expected flow of battle. "The key points may be placed on a chart that remains visible throughout the briefing.

2. **Main Body**

   Arrange the main ideas in a logical sequence.

   Use visual aids to emphasize main points.

   Plan effective transitions from one main point to the next.

   Be prepared to answer questions at any time.

3. **Closing**

   Ask for questions.

   Briefly recap main ideas and make a concluding statement.

Figure 5-1. General information briefing format

5-11. Military police and USACIDC personnel routinely communicate and share police information and police intelligence in various police reports. Police reports generated in support of decisive action typically follow the standard operating procedures for reporting that were established by the higher headquarters to which the military police units are assigned or attached. During police operations, the primary means for law enforcement reporting is ALERTS. ALERTS provides military police and USACIDC personnel the capability of generating and disseminating reports in real-time. This capability enables the efficient and effective sharing of police reports in law enforcement channels to improve situational awareness across Army law enforcement organizations and to support decision making regarding law enforcement and investigations by installation commanders, provost marshals, and USACIDC commanders. See AR 190-45 for requirements in law enforcement reporting.

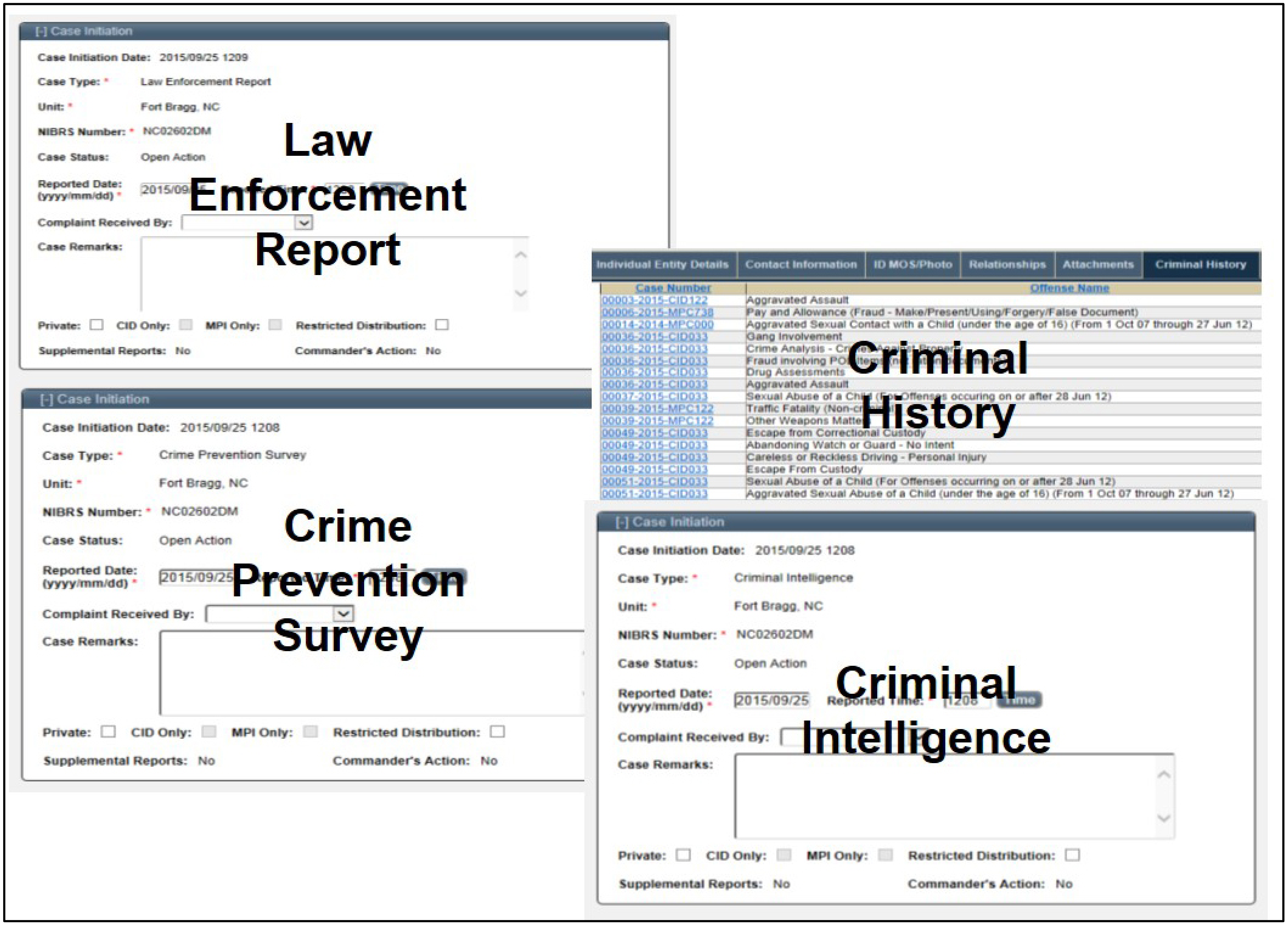
Automated Information Systems

5-12. Automated information systems greatly enhance the efficiency and effectiveness of police information and police intelligence dissemination. Automation enables military police and USACIDC to input data into law enforcement reporting systems (such as ALERTs), allowing for the rapid generation and dissemination of police reports. This digitization of data entry, storage, and retrieval reduces data entry errors, allows the storage of large quantities of data accessible by authorized users connected to the Web, and enables rapid retrieval of relevant information to disseminate police reports in a timely manner. Additionally, automated police information systems enhance police report standardization by providing centralized management of system applications and report formats. This reduces variations in reporting formats and enhances common understanding through common tools and applications across the Army law enforcement community.

Army Law Enforcement Reporting and Tracking System

5-13. The primary automation tool used by military police and USACIDC is ALERTS. ALERTS enables the rapid dissemination of standardized law enforcement and investigative reporting and of police intelligence products generated though criminal and crime analysis processes. ALERTS supports worldwide military police operations with real-time police information and police intelligence sharing across the Army law enforcement community. It is accredited for unclassified law enforcement-sensitive information and uses a virtual private network and Web-based operations. The tools and reports inherent to ALERTS enables police intelligence analysts and investigators to organize, analyze, and disseminate police intelligence products by presenting police information and police intelligence in easily understood and standardized formats.

5-14. ALERTS allows military police staffs and USACIDC personnel the ability to generate standardize police reports for dissemination. There are several varieties of reports generated by ALERTS that facilitate criminal and crime analysis, police management and planning, and other internal analysis or operational functions. Figure 5-2 provides examples of reports generated by ALERTS.



[-] Case Initiation

Case Initiation Date: 2015/09/25 1209

Case Type: * Law Enforcement Report

Unit: * Fort Bragg, NC

NIBRS Number: * NC02602DM

Case Status: Open Action

Reported Date: (yyyy/mm/dd) * 2015/09

Complaint Received By:

Case Remarks:

Private: □ CID Only: □ MPI Only: □ Restricted Distribution: □

Supplemental Reports: No Commander's Action: No

[-] Case Initiation

Case Initiation Date: 2015/09/25 1208

Case Type: * Crime Prevention Survey

Unit: * Fort Bragg, NC

NIBRS Number: * NC02602DM

Case Status: Open Action

Reported Date: (yyyy/mm/dd) * 2015/09/25

Complaint Received By:

Case Remarks:

Private: □ CID Only: □ MPI Only: □ Restricted Distribution: □

Supplemental Reports: No Commander's Action: No

Individual Entity Details | Contact Information | ID MOS/Photo | Relationships | Attachments | Criminal History

Case Number	Offense Name
00003-2015-CID122	Aggravated Assault
00006-2015-MPC738	Pay and Allowance (Fraud - Make/Present/Using/Forgery/False Document)
00014-2014-MPC000	Aggravated Sexual Contact with a Child (under the age of 16) (From 1 Oct 07 through 27 Jun 12)
00036-2015-CID033	Gang Involvement
00036-2015-CID033	Crime Analysis - Crimes Against Property
00036-2015-CID033	Fraud involving POL items [illegible]
00036-2015-CID033	Drug Assessments
00036-2015-CID033	Aggravated Assault
00037-2015-CID033	Sexual Abuse of a Child (For Offenses occuring on or after 28 Jun 12)
00039-2015-MPC122	Traffic Fatality (Non-criminal)
00039-2015-MPC122	Other Weapons Matters
00049-2015-CID033	Escape from Correctional Custody
00049-2015-CID033	Abandoning Watch or Guard - No Intent
00049-2015-CID033	Careless or Reckless Driving - Personal Injury
00049-2015-CID033	Escape From Custody
00051-2015-CID033	Sexual Abuse of a Child (For Offenses occurring on or after 28 Jun 12)
00051-2015-CID033	Aggravated Sexual Abuse of a Child (under the age of 16) (From 1 Oct 07 through 27 Jun 12)

[-] Case Initiation

Case Initiation Date: 2015/09/25 1208

Case Type: * Criminal Intelligence

Unit: * Fort Bragg, NC

NIBRS Number: * NC02602DM

Case Status: Open Action

Reported Date: (yyyy/mm/dd) * 2015/09/25 Reported Time: 1208 Time

Complaint Received By:

Case Remarks:

Private: □ CID Only: □ MPI Only: □ Restricted Distribution: □

Supplemental Reports: No Commander's Action: No

Figure 5-2. Examples of reports generated by ALERTS

Distributed Common Ground System–Army

5-15. The DCGS-A contributes to intelligence sharing across the Army. DCGS-A provides a net-centric and enterprised information collection, weather, geospatial information, and space operations capability to echelons from battalion and higher. DCGS-A is the information collection component of the modular and future force mission command system and the Army's primary system for information collection, tasking, posting, and processing and for understanding the threat, terrain, weather, and civil considerations at all echelons. This system provides a critical tool for generating common understanding across intelligence disciplines.

> ***Note.*** The laws governing the sharing of police information and police intelligence between the law enforcement and intelligence systems are very specific and restrictive. Generally, intelligence agencies cannot collect, gather, or store information from law enforcement agencies. For exceptions to this requirement, see Executive Order (EO) 12333. Appendix A contains information on the legal aspects of intelligence collection and sharing.

Granting Access and Sharing Rights

5-16. Granting access to police databases 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 is made to ensure that law enforcement agencies operating in the area of operations and 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.

5-17. 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, have 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 they can also use databases containing fugitive information from corrections systems and terrorist threat information from DHS and FBI systems.

5-18. Civilian law enforcement partners cannot access DOD proprietary automation systems. 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. Although access restrictions may limit the ability to work with external entities through direct access and sharing via automated information systems and databases, military police and USACIDC personnel leverage police intelligence networks and police engagement to ensure effective and authorized collaboration and fusion of police information and police intelligence with unified action partners.

COLLABORATION AND FUSION

5-19. Military police and USACIDC personnel develop police intelligence networks in support of missions across operational environments. 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 enhances coordination and cooperation between local agencies and provides a springboard for developing vast regional, national, or international police intelligence networks.

5-20. 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 create variations in network memberships. Influencers (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 FBI or Bureau of Alcohol, Tobacco, and Firearms field office in their immediate area of operations, or the United Nations civilian police may be operating in the immediate area of operations while the headquarters and support elements are hundreds or thousands of miles away. Despite local variations, general guidelines for developing, managing, and participating in police intelligence networks can be established.

Network Participants

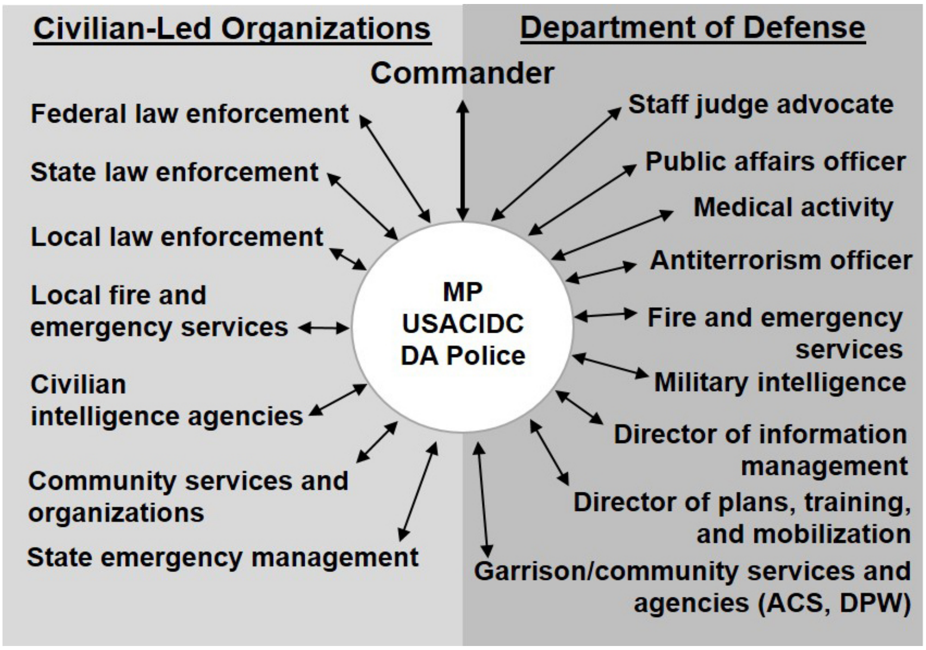
5-21. A police intelligence network should be tailored to meet the requirements of the operational environment and the specific area of operations. Participation is influenced by threat assessments, intelligence requirements, and the specific needs of participating agencies. Police intelligence collaboration and networking can occur in predetermined working groups with a relatively set membership, structure, and function or in ad hoc methods created for a specific mission or event.

5-22. A police intelligence network typically consists 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, region, or the globe. Such arrangements may fill essential capability gaps in the police intelligence network. If particular agencies are not represented in the local environment (FBI, Drug Enforcement Administration field offices, military intelligence, HN law enforcement), military police and USACIDC personnel can add them to their network by leveraging another police intelligence network or making direct contact with the agency using Web-based services.

Networks in Support of Bases and Base Camps

5-23. Police intelligence networks established to support law enforcement and security efforts at bases and base camps can provide significant capability to address criminal threats to military assets and personnel. Cooperation between local, state, federal, and military agencies enhances law enforcement and security 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 typically have a core of constant participants and the flexibility to expand to create focused ad hoc, threat-specific cells to address, prevent, or react to a specific hazard, condition, or event.

5-24. Figure 5-3, page 5-8, provides an example of a police intelligence network supporting a typical base or base camp. Specific networks 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 inside or outside the United States. Relationships between Army law enforcement personnel and other police intelligence network members differ. Some network members require day-to-day working relationships, while others are based on mutually supporting relationships for selected routine activities or occasional collaboration.


Civilian-Led Organizations
Department of Defense
Commander
Federal law enforcement
State law enforcement
Local law enforcement
Local fire and emergency services
Civilian intelligence agencies
Community services and organizations
State emergency management
Staff judge advocate
Public affairs officer
Medical activity
Antiterrorism officer
Fire and emergency services
Military intelligence
Director of information management
Director of plans, training, and mobilization
Garrison/community services and agencies (ACS, DPW)
MP
USACIDC
DA Police

Legend:

ACS	Army community service	MP	military police
DA	Department of the Army	USACIDC	United States
DPW	Directorate of Public Works	Army Criminal	Investigation
		Command	

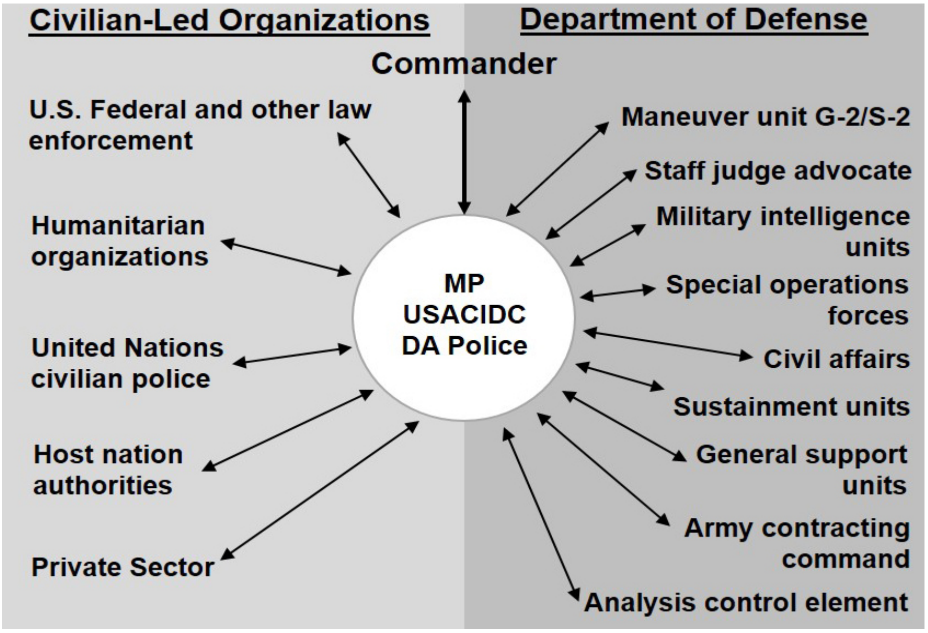
Figure 5-3. Typical police intelligence network in support of a base or base camp

5-25. Police intelligence network relationships between agencies fluctuate based on numerous factors in the operational environment. Relationships 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 greatly affect participation and the level of sharing conducted.

Networks in Support of Decisive Action

5-26. Police intelligence networks are formed to support specific missions or operations during decisive actions. These networks are affected by unit deployments and rotations, governmental and civilian organizations conducting operations throughout the area of operations, mission changes, and threat changes. These factors influence the continuity necessary to build institutional knowledge of crime and criminal threats, improve physical and social conditions, and establish long-term relationships. 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.

5-27. Figure 5-4 shows a typical police intelligence network in a deployed operational environment. As in the previous example, these police intelligence networks vary in composition based on mission and operational variables. In this example of interorganizational cooperation for PIO, civilian-led organizations are located on the left, and military organizations are located on the right.



Legend:

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

Figure 5-4. Typical police intelligence network in a deployed operational environment

5-28. The success of the police intelligence network depends on the mutual exchange of timely, relevant, and accurate police intelligence 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 to compensate for organizational weaknesses, because each organization's capabilities complement each other. The respective staffs should understand each organization's vision, mission, goals, and objectives and identify and develop mutual strategies to overcome cultural, organizational, or operational barriers.

Organizational Alignment and Communication

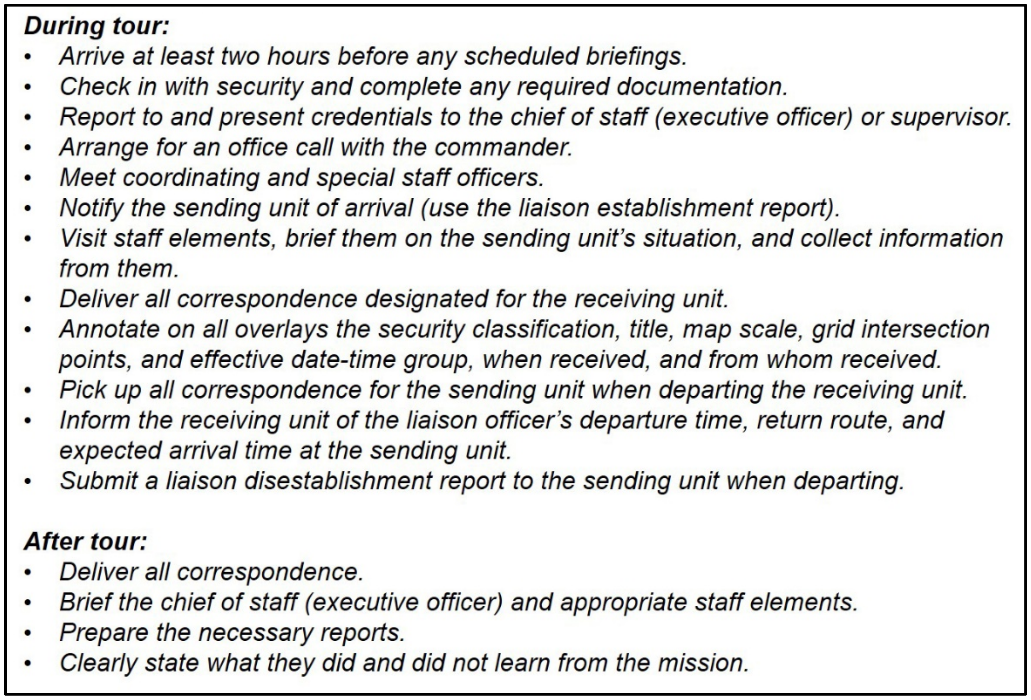
5-29. Military police and USACIDC personnel should identify and properly correlate their personnel with those of other organizations. This is important to ensure that coordination between staffs and commanders from different organizations is conducted with counterparts operating at a similar level and span of control in other organizations. It is important to nest similar commands and staffs, 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. Managers can use a modified organizational chart to identify comparable staff positions and existing gaps between organizations.

5-30. A comprehensive communications system to support the police intelligence network ensures 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 the following:

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

5-31. One way to greatly increase collaboration with external agencies and organizations is through liaison activities. *Liaison* is that contact or intercommunication maintained between elements of military forces or other agencies to ensure mutual understanding and unity of purpose and action (JP 3-08). Most commonly used for establishing and maintaining close communications, liaison continuously enables direct, physical communications between commands and with unified action partners. Military police use liaison when supporting unified land operations and during routine law enforcement, corrections, and investigative missions.

5-32. Liaison helps facilitate shared understanding and purpose among organizations, preserve freedom of action, and maintain flexibility. Liaison provides commanders with relevant information and answers to operational questions, enhancing the commander's situational understanding. Figure 5-5 provides an example of the duties a liaison officer may be expected to perform. See FM 6-0 for additional details on liaison.



During tour:

- *Arrive at least two hours before any scheduled briefings.*
- *Check in with security and complete any required documentation.*
- *Report to and present credentials to the chief of staff (executive officer) or supervisor.*
- *Arrange for an office call with the commander.*
- *Meet coordinating and special staff officers.*
- *Notify the sending unit of arrival (use the liaison establishment report).*
- *Visit staff elements, brief them on the sending unit's situation, and collect information from them.*
- *Deliver all correspondence designated for the receiving unit.*
- *Annotate on all overlays the security classification, title, map scale, grid intersection points, and effective date-time group, when received, and from whom received.*
- *Pick up all correspondence for the sending unit when departing the receiving unit.*
- *Inform the receiving unit of the liaison officer's departure time, return route, and expected arrival time at the sending unit.*
- *Submit a liaison disestablishment report to the sending unit when departing.*

After tour:

- *Deliver all correspondence.*
- *Brief the chief of staff (executive officer) and appropriate staff elements.*
- *Prepare the necessary reports.*
- *Clearly state what they did and did not learn from the mission.*

Figure 5-5. Example of liaison duties

Police Intelligence Fusion Cells

5-33. 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 processing information from multiple systems, assets, and sources and translating that information into refined police information and police intelligence that increase situational understanding and knowledge.

5-34. Fusion enables commanders and military police to gain a significant relative advantage over criminal networks and terrorist groups, cells, and individuals by decreasing the time required to observe, orient, decide, and act in complex environments. 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 decision makers.

5-35. 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, 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 military police, USACIDC personnel, and police intelligence analysts to build a coherent picture of the environment that increases situational understanding and enables informed decision making by commanders, provost marshals, and law enforcement investigators regarding policing and investigative activities.

5-36. 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 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, HN 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 the agencies involved. Table 5-1 shows an example of the composition for a police intelligence fusion cell.

Table 5-1. Example of a 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
n/a	S-2/G-2
n/a	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

5-37. The employment of police intelligence fusion cells is applicable across the range of military operations. Fusion cells 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 cells enable participating elements to eliminate unnecessary duplications of collection and analysis activities. The effective application of fusion cells 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.

SHAPING MILITARY POLICE OPERATIONS

5-38. Due to the employment of military police capabilities across diverse operational environments, it is critical to understand the role that PIO plays as an integrated task. PIO shapes the subsequent employment of military police capabilities. Together, PIO and the responses and assessments generated by military police operations form a continuous process designed to prevent crime and the fear of crime, reduce crime-conducive conditions, target criminal threats and effects, and establish safe and secure environments.

POLICE OPERATIONS

5-39. PIO is most commonly associated with police operations—specifically law enforcement and criminal investigations. The skill sets and capabilities required for PIO are honed during the conduct of police operations. Military police support commanders, Soldiers, family members, and visitors on bases or base camps through comprehensive and preventative policing. Law enforcement is normally the most visible aspect of this support, while military and DA Civilian police forces provide 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. PIO helps shape police operations and provides strategic crime analysis that helps shape the focus of police management, such as—

- Police policy, planning, and management decisions.
- Resource procurement, prioritization, and allocation.
- Crime prevention, reduction, and disruption strategies.
- Broad policing strategies and general deterrence approaches.

5-40. PIO is critical to evaluating the effectiveness of policing strategies that are applied through the conduct of police operations. Police information and police intelligence can lead a commander or provost marshal to increase or decrease military police presence or to modify the techniques used in particular areas. PIO corresponds to the first two steps in the scanning, analysis, response, and assessment model, which enables military police to solve crime problems through intelligence-led, proactive police operations. The policing strategies and tasks that military police perform based on PIO outputs comprise the Response and Assessment steps in the scanning, analysis, response, and assessment model. See ATP 3-39.10 for details on police operations.

Law Enforcement

5-41. Law enforcement includes those activities performed by personnel authorized by legal authority to compel compliance with, and investigate violations of, laws, directives, and punitive regulations. Law enforcement occurs in direct support of governance and the rule of law; however, for law enforcement to occur, a legal system must exist. Typically, law enforcement is performed by personnel trained as police officers. They are held directly accountable to the governmental source of their authority.

5-42. PIO supports the efficient and effective planning, execution, and assessment of law enforcement by providing police intelligence that depicts crime hotspots, crime trends, patterns, and associations. It also evaluates police effectiveness in addressing criminal offenders, networks, organizations, and environmental conditions that create opportunities for crime. This enables 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, USACIDC personnel, and police intelligence analysts in support of Army law enforcement efforts.

Patrol Manpower and Resource Requirements

5-43. Patrol manpower and resources vary across operational environments based on population sizes, crime rates, levels of organized criminal activity, assigned missions, expected activities of the population, and other factors. PIO supports the planning and allocation of specific manpower and resources required in the immediate or near-term by providing the tactical criminal intelligence and crime analysis products necessary to make informed decisions by law enforcement leadership. Examples of support that PIO may provide for near-term patrol manpower and resource planning are—

- Analysis of environmental conditions that may require adjusting routine police manpower and resourcing requirements. As crime rates or organized criminal activity levels increase or decrease, patrol manning and resourcing may require adjustments to meet the demands of the situation. Tactical criminal intelligence and crime analysis provide the critical knowledge, products, and understanding needed to ensure the proper level of police manning and equipping to meet immediate law enforcement requirements.
- Analysis for special missions in the area of operations that require additional manpower and resources. Special missions may include very important person visits, deployment and redeployment escort or security missions, or enhanced force protection posture and special response activities against elevated criminal or terrorist threats.
- Analysis of times, places, and patterns of activity in preparation for special events (sports, holiday, or ceremonial events) that require additional law enforcement manpower, special resources (such as barricades and traffic signs), coordination for specialized capabilities (such as MWDs), and modified planning for patrol distribution, traffic control plans, and other considerations, depending on the special event.

Patrol Distribution

5-44. Military police distribute law enforcement assets across the area of operations or jurisdiction in the most effective and focused manner. There are several ways to direct patrol distribution (see ATP 3-39.10 for various law enforcement patrol strategies). Regardless of the approach adopted, law enforcement patrols seek the most effective means to prevent, deter, and reduce crime and the fear of crime among populations. Preventative and proactive policing requires police intelligence to ensure that military police patrols are distributed and focused in a manner that most effectively prevents crime through the deterrent effects of concentrated patrol activity at places and times where crime concentrates.

5-45. Patrol distribution places military police assets in positions that allow the most impactful employment of resources for the purposes of crime prevention, mitigation, and response. Despite having a proactive policing presence when crimes do occur, patrol distribution at the most likely locations for crime to occur enables rapid responsiveness to investigate reported criminal activity, the ability to quickly engage or apprehend active criminal subjects, and the delivery of critical emergency services and assistance. PIO shapes patrol distribution by providing tactical criminal intelligence and crime analysis regarding known criminal offender locations, crime hotspots, patterns of criminal activity, and places vulnerable or repeatedly targeted by criminals.

Police Engagement

5-46. Police engagement provides an effective means for military police to collect police information and serves as a tool to provide important information to relevant audiences, populations, stakeholders, and decision makers. The relationship between police and the population is critical in the ability to interact with and operate among dense populations. Adequate, timely, and accurate police information sharing with populations is critical to sustaining public trust and confidence. Without revealing the details of sensitive law enforcement activities, military police and USACIDC organizations keep populations informed to gain their understanding, respect, and voluntary compliance to the law. This information sharing may include—

- Sharing BOLOs, criminal alert notices, and other public safety messages so people can take appropriate measures to protect themselves and their property from criminal threats.

- Publicizing administrative changes so that the public is aware of local policy, procedure, and enforcement changes to mitigate unintentional criminal offences due to lack of awareness and allow populations to adjust their behavior to comply with modified policy.
- Offering rewards or compensation for information regarding wanted criminal subjects.

5-47. Just as mistrust and a weak social order can enable criminals and terrorists, a strong relationship between the population, police, and security forces enhances collective efficacy in the population. Key elements to assist investigations are understanding the social order, defeating criminal networks, and ensuring continuous access to sources of police information. By disseminating timely and relevant police information to populations, military police and USACIDC personnel greatly enhance the population's trust, confidence, and support of police organizations.

Crime Prevention

5-48. PIO is critical to effective crime prevention efforts. PIO is one of the primary tools of crime prevention and supports the crime prevention survey. The crime prevention survey formally records the assessment, review, and analysis of existing conditions within 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. It determines the nature, extent, and underlying causes of crime and provides the commander with information for use in the Crime Prevention Program. While there are several different types of crime prevention strategies (see ATP 3-39.10), the following are those approaches to crime prevention that are most reliant on police intelligence:

- Relies heavily on criminal intelligence products.
  - Specific (or focused) deterrence.
  - Situational crime prevention.
- Relies heavily on crime analysis products.
  - Crime prevention through environmental design.
  - Disorder policing.

Criminal Investigations

5-49. PIO directly supports criminal investigations. Law enforcement investigators generate the police intelligence requirements needed for situational understanding and decision making regarding criminal investigations, the disruption of criminal activity, and investigative focus. Criminal analysis generates criminal intelligence that identifies the critical linkages, associations, and patterns necessary to conduct law enforcement investigations, disrupt criminal networks, and solve criminal cases.

Criminal Investigation Task Force

5-50. The DOD Criminal Investigation Task Force is a strategic-level organization with a mission to develop and fuse criminal 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. The Criminal Investigation Task Force combines assets into teams of USACIDC special agents, criminal investigators from other Services, police and intelligence analysts, and attorneys. These teams synchronize and fuse police information and strategic criminal intelligence from available sources to investigate organized criminal activity that enables criminal prosecution in U.S. or HN legal systems.

Traffic Management and Enforcement

5-51. Traffic management and enforcement is a preventive and responsive effort. The deliberate and methodical analysis of police information related to traffic (conditions, offenses, hotspots) is essential to developing effective plans for traffic circulation, control, and enforcement. PIO provides vast amounts of law enforcement data related to traffic to produce crime analysis products that support traffic management. PIO helps identify potential environmental conditions that military police must address to increase effective traffic flow, such as poor sign locations or obstructive landscaping that hinder the ability to see traffic signs. Techniques such as pattern analysis are critical to performing effective traffic studies to determine the causes of traffic problems and to help develop potential solutions. Besides supporting traffic enforcement, PIO also supports risk management by identifying traffic hazards, providing potential risk mitigation control measures based on empirical data, and informing decision making assets to implement and supervise traffic management to provide public safety. See ATP 3-39.10 for additional details on traffic studies.

Support to Civil Security and Civil Control

5-52. Military police and USACIDC personnel support the reestablishment of civil security and civil control following large-scale ground combat operations or during limited contingency operations focused on restoring stability and order in failing or failed states. PIO enables military police support to civil security and civil control by—

- Informing military police efforts to restore and maintain order.
- Providing police information and police intelligence that supports border control and boundary security.
- Providing assessments and information critical to establishing an interim criminal justice system or supporting the improvement of existing criminal justice systems.
- Providing the assessments and information necessary to successfully train and support HN police and corrections organizations.

Host-Nation Police Training and Support

5-53. In support of HN police organizations, police assessments and crime analysis provide insights into the effectiveness and potential systemic problems (training deficiencies, administrative issues, operational challenges) of HN police organizations. PIO integrated within police operations supports decisive action by enhancing the situational understanding of civil considerations as they relate to HN police systems, organizations, capability, and capacity. See ATP 3-39.10 for additional information on building HN police capability and capacity.

5-54. Police information and police intelligence regarding the locations, capability, and dispositions of HN police and security elements can be critical to military police conducting HN police development. This enables the HN to plan for HN response forces and eliminates potential sanctuaries or safe havens. Military police conducting missions to build HN police capability and capacity may be required to engage in the vetting, hiring, training, leading, and safeguarding of new HN police forces, often across a widely dispersed area of operations.

5-55. PIO supports situational awareness to identify, analyze, and act as necessary when HN police elements may be infiltrated by criminal or insurgent elements. Some former or new personnel staffing reconstituted or new police forces may wish to employ illicit modes of operation to increase personal wealth and influence. Criminal or insurgent elements may also infiltrate newly forming police organizations for the same reasons or to carry out direct attacks against U.S. military and HN police. Criminal intelligence generated by PIO that indicates infiltration by criminal elements allows military police to enhance situational awareness, avoid potential ambush locations or situations, and exercise caution during interaction with potential threats.

Host-Nation Police Intelligence Capability

5-56. Building HN police intelligence capability and capacity requires a detailed assessment of the HN police organization, followed by the training and mentoring of HN police personnel identified as potential police intelligence analysts. When building police capability and capacity, key measures of effectiveness and essential elements to operational success are developing a police intelligence capability and an operational capacity.

5-57. HN police effectiveness is greatly enhanced by the ability to exercise foundational criminal and crime analysis techniques that recognize and connect people, places, events, trends, patterns, and associations. In turn, it can greatly enhance U.S. forces effectiveness. The Iraqi Police first received biometrics training in

2006-2007. Within three years of their training, they collected over one million biometric collections that were accessible to U.S. analysts. Military police and USACIDC personnel who conduct HN police training and support train HN police and security forces to conduct PIO and place them in an advantageous position to gain further police information about the HN police force, criminal environment, and the population among whom the HN police operate.

> ***Note.*** As outlined in AR 380-10, when sharing classified military information or controlled unclassified information with foreign partners and HN law enforcement agencies, foreign disclosure considerations and policies must be strictly followed. Early and continuous coordination with the supporting foreign disclosure officer is essential because not all information likely proposed for disclosure falls under the purview of the National Disclosure Policy (information marked law enforcement-sensitive).

5-58. The ability of HN police to conduct PIO may be limited by education, training, available resources, societal norms, 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, when acceptable, these capabilities can be invaluable to the HN police intelligence capability. Deliberate police engagements with prospective leaders of emerging police forces are vital in establishing and prioritizing the development of police intelligence capabilities.

Civil Disturbance Control

5-59. PIO supports civil disturbance control through the production of tactical criminal intelligence and crime analysis that enable the anticipation of civil disorder and the instability to enhance police efforts to prevent, control, or mitigate the impacts of civil disturbances. While the focus to control a single civil disturbance can be enhanced by police intelligence products designed for specific tactical results, strategic crime analysis and criminal intelligence may also contribute to civil disturbance control efforts. Strategic crime analysis can identify patterns, trends, and environmental conditions that may be contributing to multiple civil disturbances throughout an area of operations. This understanding may enhance military police efforts to not only control an immediate civil disturbance, but also to address the underlying causes that fuel disorder throughout a broader area (see ATP 3-39.33).

5-60. Likewise, civil disturbances are often instigated or perpetuated by organized criminal elements hidden within a civilian population. While the civilian population may be demonstrating peacefully to address perceived grievances, criminal (or insurgent) elements may infiltrate the population to achieve their own purposes by instigating violence to threaten civil order, undermine perceptions of police effectiveness in controlling violence, or elicit an overreaction from police to undermine their legitimacy in the eyes of the population. Criminal intelligence products can assist in identifying criminal offenders or individuals affiliated with criminal organizations within a population to assist efforts to apprehend those criminals who seek to transform a peaceful civil protest into a violent confrontation.

Support to Civil Law Enforcement

5-61. *Defense support of civil authorities* is support provided by U.S. Federal military forces, DOD civilians, DOD contract personnel, DOD component assets, and National Guard forces (when the Secretary of Defense, in coordination with the Governors of the affected States, elects and requests to use those forces in Title 32, U.S.C., status) in response to requests for assistance from civil authorities for domestic emergencies, law enforcement support, and other domestic activities, or from qualifying entities for special events (DODD 3025.18). Except for the nonfederalized National Guard, military police support to homeland operations is significantly constrained by various laws—the foremost among them being the Posse Comitatus Act. See ADP 3-28 and FM 3-39 for information regarding DSCA.

5-62. Generally, except for the nonfederalized National Guard, military police support to civil law enforcement is restricted to support related tasks. These support tasks include training, resource management, personnel qualification or certification, equipment certification, communications and information management, technology support, and continuous system improvement. PIO support to civil law enforcement is applied within these legal constraints. PIO enables effective police engagement with civil law enforcement partners to share releasable police information and police intelligence related to police procedures or policy changes affecting local residential populations (such as expected traffic delays), criminal threats affecting domestic populations and resources, or capabilities authorized for use or employment to support civil law enforcement.

5-63. Nonfederalized National Guard support to civil law enforcement is conducted under the authority of the state governor in-state active-duty or Title 32 status and is not restricted by the Posse Comitatus Act. Military Police support for these missions includes support tasks and direct law enforcement for civil disturbances, natural disasters, special security events, and other situations. PIO support for these situations typically includes criminal threat analysis.

DETENTION OPERATIONS

5-64. PIO enables the ability of military police, USACIDC personnel, and police intelligence analysts to connect persons to other individuals, organizations, objects, and events relevant to the criminal threats and conditions. Associations may be relevant to incidents inside a detention facility; however, they may also associate individuals with persons outside the facility or with events that may have occurred before detention. These associations can be especially relevant during counterinsurgency operations. For example, military police in one area may obtain evidence from a crime scene that implicates a detainee at a U.S. or HN detention 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.

> ***Note.*** Police information and police intelligence that indicates the need for the additional interrogation of detainees requires military police to immediately coordinate with supporting military intelligence personnel to conduct interrogations. Military police never participate in interrogations of detainees or in setting conditions for detainee interrogations. See FM 3-63 for roles and responsibilities of military police and military intelligence in detainee operations.

5-65. Police information and police intelligence may identify the need for criminal investigations focused on crimes within a detention facility. Commanders may direct criminal investigations concerning events in a facility when serious criminal infractions occur, such as attacks on other detainees or U.S. personnel, contraband smuggling, and escape attempts. In situations potentially involving a criminal investigation, special care must be taken to recognize, preserve, collect, and process materials with potential evidentiary value. PIO can also link detainees or U.S. military prisoners in a detention facility to crimes, criminals, and activities outside the facility.

5-66. Police information and police intelligence which suggest that criminal activity, associations, or organizations exist within a detention facility may require law enforcement surveillance or criminal investigations into the suspected criminal activity. Identifying and documenting criminal behavior, criminal offenses, and individual criminal perpetrators allow the detention facility commander and military police staff to identify criminal networks and organizations forming within a facility. Armed with this information, commanders may direct action or take steps necessary to interdict these groups before serious breaches of security occur.

5-67. When detainees or U.S. military prisoners perceive that they may benefit from a breakdown of good order and discipline in facilities, they may 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 or prisoners.

5-68. Police intelligence is critical to maintaining good order and discipline in detention facilities. Detention operations are inherently risky due to the potentially high number of U.S. military prisoners or detainees and the relatively low number of guard personnel. Military police commanders and staffs responsible for these facilities must continuously determine intelligence requirements and conduct ongoing criminal and crime analysis to identify and counter criminal and disruptive activities and the associated risks to order and discipline. PIO supports the commander’s risk management efforts in detention environments. See ATP 5-19 for risk management.

United States Military Prisoner Confinement

5-69. The confinement of U.S. military prisoners requires special considerations apart from the general application of PIO to detention operations previously discussed. In particular, military intelligence personnel are prohibited from performing interrogations of detainees in a corrections environment because the detained population consists of U.S. Soldiers. Most often, criminal threats within a U.S. military prisoner population are handled in a manner that is similar to regular law enforcement and criminal investigations in that there must be probable cause to conduct law enforcement interrogations to obtain police information relevant to the prevention and investigation of crimes committed within the detention facility (see AR 190-47).

Detainee Operations

5-70. PIO supports detainee operations by identifying criminal threats and crime-conducive conditions within a detention facility. Military police efforts to maintain good order and discipline in a detention facility require cooperation across functional lines. Police intelligence analysts do not solely analyze police information collected by military police forces; they also leverage police intelligence networks and integrate the information and intelligence obtained from other sources to form a holistic understanding that contributes to the commander’s situational understanding and enables decision making. The following are other sources of information that PIO can integrate and share with the commander and staff:

- Coordination and information sharing with military intelligence HUMINT teams can provide critical information regarding criminal activities and threats within the facility.
- 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 environmental characteristics that may be generating crime-conducive conditions that present crime opportunities to detainees.
- HN and U.S. interpreters are in a position to hear detainee conversations, read graffiti, and screen inbound and outbound mail.

Note. When conducting detainee operations, the general distinction between police intelligence roles and military intelligence roles is that police intelligence focuses on specific crimes and criminal activity occurring or impacting good order and discipline within a facility while military intelligence focuses on the actions of detainees outside the facility that resulted in their detention. Military intelligence also focuses on detainee connections to threat networks outside a facility that pose a threat to U.S. forces or missions and on the knowledge that detainees may have of the locations, organizations, personnel, or tactics of targeted threat networks. See FM 3-63 for details on the roles and responsibilities of military police and military intelligence during the conduct of detainee operations.

Host-Nation Corrections Training and Support

5-71. Similar to building HN police capability and capacity, military police also train and support HN corrections organizations and personnel. PIO supports both the assessment and understanding necessary to initiate penal reforms or prison system improvements, and supports the development of professional and effective HN corrections organizations. As HN corrections organizations develop and mature, the corresponding development of the police intelligence capability is critical to ensure that HN corrections personnel are capable of identifying, collecting, and analyzing relevant information inside and outside detention facilities to—

- Maintain safe and secure environments within facilities.
- Identify and interdict criminal activity and organizations impacting good order and discipline.
- Influence criminal investigations of offenses committed within the facility.

5-72. As with HN police, special care and attention should be paid to the—

- Potential infiltration of HN correction staffs by criminal or terrorist actors.
- Educational, training, resourcing, cultural, legal, and other constraints bearing on the HN corrections organizations, personnel, and facilities.

SECURITY AND MOBILITY SUPPORT

5-73. Security and mobility support is a military police discipline conducted to protect the force and noncombatants and preserve the commander's freedom of action. PIO is integrated into security and mobility support to increase situational awareness and influence decision making. Used in conjunction with other information and intelligence or integrated within an organization's IPB process, police intelligence assist in identifying areas of criminal threat activity or other destabilizing factors. These products enable commanders to make prudent decisions regarding the security of convoys that are transiting lines of communication and provide military police with the information necessary to mitigate risks to forces, routes, bases and base camps, command posts, and other critical assets and personnel operating in support and consolidation areas.

5-74. Police information and police intelligence allow military police conducting security and mobility support to plan and execute measures to reduce crime-conducive conditions and counter the effects of criminal activity on military operations. These countermeasures may include—

- Identifying high-threat areas, focusing military police reconnaissance and surveillance, and recommending bypass routes for movement control teams.
- Conducting offensive operations to destroy criminals, criminal networks, and criminal organizations.
- Hardening likely targets through the implementation of physical security and antiterrorism measures.
- Developing procedures to prevent, detect, and respond to criminal and terrorist actions before they occur.
- Implementing recommendations to reduce vulnerabilities to criminal and other irregular threats.

Reconnaissance and Surveillance

5-75. Whether performed as a deliberate task or performed passively during the conduct of other tasks, reconnaissance and surveillance is a continuous process that is part of military police operations. PIO focus on information collection during reconnaissance and surveillance efforts of military police collection assets. PIO is an adaptive and continuous process that incorporates new requirements requiring future information collection while satisfying current requirements. As collected police information and police intelligence generate understanding of one aspect of the crime or criminal threats, that understanding often reveals additional areas for which information is required to form a more complete picture of the crime environment. As new information or intelligence requirements are generated throughout the PIO process, they may immediately result in planning new or modified information collection tasks that direct additional reconnaissance and surveillance by military police collection assets.

Support to Mobility

5-76. Military police units use traffic control posts, checkpoints, roadblocks, and other traffic control measures to control the movement of vehicles, personnel, and materiel and to prevent illegal actions that may aid the enemy. These control measures serve as deterrents to criminals, terrorists, saboteurs, and other threats. Military police tasked to provide support to mobility operations use the understanding gained by PIO to plan and direct military police mobility support tasks, such as main supply route regulation and enforcement, traffic control, or support to combined arms mobility operations (clearing, breaching, gap crossing).

5-77. PIO shapes military police tasks to support mobility and provides military police commanders and staffs relevant and timely knowledge of criminal actors, activities, or effects that threaten friendly force routes and convoys transiting lines of communication to preserve the freedom of movement and maneuver. Apart from threats, environmental hazards may also negatively impact friendly force mobility. By embracing an integrated threat and environmental-focused approach, PIO enables commanders to understand and appreciate the full array of threats and hazards facing the friendly force to best protect the force and preserve the freedom of movement and maneuver. See ATP 3-39.30 for military police support to mobility and ATP 3-90.4 for combined arms mobility operations.

Area Security

5-78. PIO supports military police conducting area security throughout support and consolidation areas. *Area security* is a security task conducted to protect friendly forces, installations, routes, and actions within a specific area (ADP 3-90). While maneuver forces conduct large-scale ground combat operations in the close area, units assigned to the consolidation area or support area must also contend with a diversity of hybrid threat components, including criminal elements. As the situation evolves from a focus on offensive and defensive tasks to more stability tasks and as U.S. forces seek to consolidate gains, police intelligence complements traditional military intelligence by providing products specifically focused on the crime and criminal aspects of the operational environment. PIO contributes to the commander's understanding of threats and vulnerabilities related to bases and base camps, port area and pier security, critical assets (facilities, infrastructure, personnel), and civilian population centers and transit routes.

5-79. Because human populations are a critical component of the land domain, securing the land domain requires an adequate level of security for populations to restore civil order, maintain stability, and create an enduring peace. PIO influences efforts to secure areas and populations by focusing on building an understanding of those elements most committed to disrupting stability and order. As criminals and other irregular threats seek to take advantage of the chaos, disorder, and instability resulting from armed conflict, efforts to counter them require dedicated focus. PIO enables the commander to gain situational awareness and make informed decisions, focusing on targeting criminal and irregular threats to the population and improving the environmental conditions creating opportunities for crime. The combination of criminal intelligence to target criminal threats and crime analysis to understand the drivers of instability and the root causes of crime greatly enhances the commander's efforts to consolidate gains by providing a secure environment.

5-80. Area security includes securing those assets most critical to the friendly force (command posts or sustainment facilities) and those local civilian facilities and infrastructure most critical to the successful consolidation of gains following large-scale ground combat (government facilities, HN police and corrections infrastructure, economic infrastructure). PIO contributes to critical asset security through the continuous assessment of criminal and irregular threats and of the friendly vulnerabilities to those threats. PIO contributes to the military police assessments of criminal threats against vulnerable friendly assets (personnel, facilities, missions) to ensure adequate protection.

Physical Security

5-81. *Physical security* is that part of security concerned with physical measures designed to safeguard personnel; to prevent unauthorized access to equipment, installations, material, and documents; and to safeguard them against espionage, sabotage, damage, and theft (JP 3-0). The security of property, equipment, facilities, and personnel is the responsibility of each military and civilian leader throughout the Department of Defense. Commanders protect personnel, information, and critical resources in all locations and situations against a wide range of threats through the development and implementation of effective physical security programs, policies, and procedures. PIO supports physical security through the assessment of physical security requirements and criminal and crime analysis that supports physical security designs to reduce vulnerability and deter potential criminals based on known or anticipated criminal threats. See ATP 3-39.32.

Antiterorrism

5-82. *Antiterrorism* is the defensive measures used to reduce the vulnerability of individuals and property to terrorist acts, to include rapid containment by local military and civilian forces (JP 3-07.2). Antiterrorism which is the Army defensive program to protect against terrorism, is a consideration of forces during military operations. Army antiterrorism, at a minimum, focuses on risk management, planning (including the antiterrorism plan), training, exercises, resource generation, and comprehensive program review. Antiterrorism planning coordinates specific antiterrorism security requirements with the efforts of other security enhancement programs (intelligence support to antiterrorism, law enforcement, physical security, operations security, information security). Effective antiterrorism programs synchronize intelligence, risk management, and existing security programs to provide a holistic approach to defend against terrorist threats. PIO provides critical police intelligence related to specific criminal threats and vulnerabilities to crime that supports the prevention, mitigation, and response to terrorist threats and attacks.

Support to Dislocated Civilian Operations

5-83. PIO provides relevant police information and police intelligence regarding crimes occurring or criminals operating within populations. Dislocated civilian operations are conducted to provide safety and security for dislocated civilians uprooted from their routine lives by the disruptive and destructive effects of armed conflict. Unlike detainee operations, dislocated civilians are not typically detained against their will. However, dislocated civilian facilities 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 from individuals under significant amounts of stress. These situations may also be the result of criminal elements in the population seeking to intimidate or exploit dislocated civilians. PIO supports dislocated civilian operations by identifying the causes of potential disorder within a population, providing crime analysis products that address the conditions generating crime opportunities and producing criminal intelligence that supports the targeting of criminal or disruptive agents operating within the population.

Logistics Security

5-84. 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 U.S. Army logistics provided to the military ground force on the ground. USACIDC personnel are assigned the responsibility of conducting logistics security. PIO directly supports this effort by providing criminal threat analysis, vulnerability assessments, economic crime threat assessments, logistics security threat assessments, and other types of criminal intelligence that identify and assess criminal threats that may impact logistics security. Police intelligence analysts produce reports that identify theft or interdiction efforts, suspicious behavior, or other questionable acts that can cause USACIDC personnel to focus efforts on the apprehension of criminal elements and the reduction of vulnerabilities to the logistics enterprise.

SUPPORT TO HOMELAND OPERATIONS

5-85. The law enforcement community in the United States is universally committed to the timely and seamless exchange of information and intelligence related to terrorist and criminal threats. In light of the 11 September 2001 terrorist attack and the continuing threat of terrorism to the homeland, it is critical that law enforcement personnel work together (along with the overall national security intelligence enterprise) to protect the nation. This section details some of the key civilian agencies, initiatives, and venues through which military police and USACIDC personnel synchronize and disseminate police intelligence to enhance the overall effort to secure the homeland. The methods established earlier in this chapter regarding police intelligence networks, collaboration, and fusion are crucial to effective unified actions with interagency partners.

5-86. The civilian law enforcement community typically uses the terms law enforcement or criminal intelligence to refer to police intelligence. The Army uses police intelligence as the overarching term given its contribution to military police operations across operational environments, from installation law enforcement to military police support to decisive action. Within police intelligence as an integrated task, crime analysis products typically serve a greater role in shaping internal policing strategies and approaches and in measuring police effectiveness, while criminal intelligence products are those related to criminal threats and vulnerabilities. Given these different focuses, criminal intelligence products are the most common types of police intelligence that are shared with unified action partners to support situational awareness of criminal threats to the homeland.

DEFINITIONS AND PROCESSES

5-87. When working with interagency partners, it is important to use common language and to strive for common understanding. In the civilian law enforcement community, there are several definitions and processes that describe law enforcement or criminal intelligence. Two prominent definitions for these terms are—

- **Law enforcement intelligence.** Law enforcement intelligence is the end product (output) of an analytic process that collects and assesses information about crimes and criminal enterprises. Its purpose is to make judgments and inferences about community conditions, potential problems, and criminal activity with the intent to pursue criminal prosecution or project crime trends or to support informed decision making by management. (From *Law Enforcement Intelligence: A Guide for State, Local, and Tribal Law Enforcement Agencies*).
- **Criminal intelligence.** Criminal intelligence is information compiled, analyzed, and disseminated in an effort to anticipate, prevent, or monitor criminal activity. (From the *National Criminal Intelligence Sharing Plan*).

5-88. The Army use of the term police intelligence closely resembles the definition of law enforcement intelligence. Both focus on crime and criminal threats to further police or law enforcement efforts. Given the application of PIO as an integrated task across military police operations, the broader designation as police intelligence is more appropriate than the narrow limits of law enforcement intelligence, which implies strict application only in support of law enforcement. The Army's definition of criminal intelligence parallels the definition established in the *National Criminal Intelligence Sharing Plan* to ensure mutual understanding and common terminology.

5-89. The civilian law enforcement community typically defines the law enforcement or criminal intelligence process as consisting of six basic steps:

- **Step 1.** Planning and direction.
- **Step 2.** Collecting.
- **Step 3.** Processing/collation.
- **Step 4.** Analysis.
- **Step 5.** Dissemination.
- **Step 6.** Reevaluation.

5-90. The PIO framework follows the four steps derived from the Army's established intelligence process while still maintaining a close resemblance to common civilian law enforcement or criminal intelligence processes. While the individual steps are divided or labeled differently, the overall process and the tasks performed throughout the process are essentially the same. Keeping in mind the commonalities between processes, it is important for military police and USACIDC personnel to be aware of the different processes or labels unique to individual partner law enforcement agencies. Understanding the commonalities and differences between the processes enhances the overall basis for dialogue, collaboration, and mutual understanding.

> ***Note.*** During DSCA, information collection is limited and categorized as information awareness and assessment. The distinction between information collection, information awareness, and assessment emphasizes that during DSCA, neither Army forces, nor any DOD component may collect information on U.S. persons for intelligence purposes. Information awareness and assessment leverages traditional DOD and other government information capabilities in support of homeland operations while assuring strict adherence to applicable legal frameworks. Information awareness and assessment supports the purposes of DSCA: to save lives, alleviate suffering, and protect property. Information awareness and assessment addresses the limited information collection activities permitted in the homeland in support of these purposes. Information awareness and assessment processes consolidate information and provide analysis of the physical environment; weather impacts; terrorist threats; and chemical, biological, radiological and nuclear hazards; and other operational or mission variables.

5-91. There are several other terms used throughout the law enforcement community that are important to know to enhance common understanding among unified action partners. These terms include intelligence-led policing, community policing, and problem-oriented policing. While these terms all rely (to some degree) on the products of PIO, they are more appropriately viewed as overall policing approaches, models, or strategies and are discussed in ATP 3-39.10.

Initiatives and Programs

5-92. The sharing of police information that is of immediate tactical value and the sharing of criminal intelligence that is related to organized criminal or terrorist activity have 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 common language, understanding, and fusion centers supports the timely exchange of relevant criminal intelligence to protect the homeland from terrorist attacks. The following paragraphs provide information on some of the civilian law enforcement initiatives and programs that enable interagency cooperation and standardization of police/law enforcement/criminal intelligence training. Although these initiatives were developed in the civilian law enforcement community, they are open to Army law enforcement personnel. A thorough understanding of civilian standards, policies, and procedures is critical in the 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

5-93. The 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 to 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 United States Department of Justice Web site.

5-94. 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 Marshals Service) participate in OneDOJ. Criminal information shared includes open- and closed-case documents, investigative reports, witness interviews, criminal event data, criminal history and incarceration information, and individual criminal offender information. Outside agencies connect with OneDOJ through regional sharing systems by using a standard secure platform developed through the Law Enforcement Information Sharing Program. Through the OneDOJ system, the DOJ shares information with the military criminal investigative services (USACIDC, Naval Criminal Investigative Service, and the Air Force Office of Special Investigations).

Law Enforcement Information Sharing Program

5-95. The Law Enforcement Information Sharing Program is an effort by the DOJ to improve 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. The 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 U.S. Immigration and Customs Enforcement Web site.

National Information Exchange Model

5-96. The National Information Exchange Model is a national information framework that eases exchanges across organizations involved in homeland operations. It allows for the transfer of information by 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 Justice Information Sharing Web site.

National Criminal Intelligence Sharing Plan

5-97. The National Criminal Intelligence Sharing Plan resulted from an effort to close identified gaps in the police and law enforcement intelligence capability in the aftermath of the terrorist attacks on 11 September 2001. The original plan published in 2003 outlined 28 recommendations for implementation by law enforcement agencies to improve criminal intelligence sharing. 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 information and intelligence sharing. Additional information on the National Criminal Intelligence Sharing Plan and associated recommendations can be found on the Justice Information Sharing Web site.

5-98. In the decade following the original publishing of the National Criminal Intelligence Sharing Plan, law enforcement agencies across the United States (including USACIDC) have made progress in implementing the recommendations of the National Criminal Intelligence Sharing Plan to enhance the availability, accessibility, and flow of criminal intelligence. The results of this widespread implementation have been improvements in the collection of information, the analysis of this information, and the sharing of criminal intelligence. However, with an evolving crime outlook in the homeland and internationally, the DOJ reviewed and updated the National Criminal Intelligence Sharing Plan in 2013 to identify new opportunities and approaches to promote continued nationwide criminal intelligence sharing. This version 2.0 of the National Criminal Intelligence Sharing Plan is designed to build on the recommendations identified in 2003 to further promote responsible and effective criminal intelligence and information sharing. This update expands the original focus to include recommendations that address the sharing of criminal intelligence and information externally (or outside a law enforcement agency) with other federal and/or homeland security partners and with state, local, and tribal law enforcement agencies.

Global Intelligence Working Group and Criminal Intelligence Coordinating Council

5-99. The Global Intelligence Working Group is composed of federal, state, local, and tribal justice representatives; homeland security representatives; and public safety representatives. As needed, the Global Intelligence Working Group has the capability of drawing on subject matter experts external to the working group. 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 criminal 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

5-100. The Global Justice Information Sharing Initiative is a federal advisory committee that advises the U.S. Attorney General on 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

5-101. The *National Strategy for Information Sharing* focuses on sharing information related to terrorism from multiple sources (including homeland security, law enforcement, and the national security establishment). 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.

5-102. 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.

5-103. The *National Strategy for Information Sharing* identifies baseline requirements for fusion cells. Defining these operational standards enables federal, state, and local officials to identify and plan for the resources needed (including financial, technical assistance, and human support) to attain the capacity required for successful information fusion cells. This baseline capability ensures that fusion cells have the necessary structures, processes, and tools in place to support the gathering, processing, analysis, and dissemination of information in support of specific operational capabilities; suspicious activity reporting; alert, warning, and notification reporting; risk assessments; and situational understanding reporting.

Regional Information Sharing Systems®

5-104. Regional Information Sharing Systems are conduits for the exchange of criminal information and criminal intelligence among participating law enforcement agencies. Regional Information Sharing Systems are composed of six regional centers that share criminal intelligence and coordinate efforts against criminal networks operating in many locations across jurisdictional lines. Typical targets of Regional Information Sharing Systems activities are terrorism, drug trafficking, violent crime, cyberspace crime, gang activity, identity theft, human trafficking, organized crime and criminal activities. Each center selects its own target crimes and the range of services provided to member agencies. Additional information can be accessed on the Regional Information Sharing Systems Web site.

SUPPORT THE ARMY OPERATIONS PROCESS

5-105. PIO supports the Army through the dissemination of police information and police intelligence into the operations process through the integrating processes. Police information and police intelligence complement other sources of information and intelligence to fulfill the commander’s information and intelligence requirements, develop a common operational picture, and develop situational understanding of the crime and criminal aspects of the operational environment.

The Operations Process

5-106. The *operations process* is the major mission command activities performed during operations: planning, preparing, executing, and continuously assessing the operation (ADP 5-0). 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; to make and articulate decisions; and to direct, lead, and assess operations. The activities of the operations process—plan, prepare, execute, and assess—are not discrete, but they overlap and recur as circumstances demand (see figure 5-6, page 5-26). See ADRP 5-0 for details on the operations process. 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.

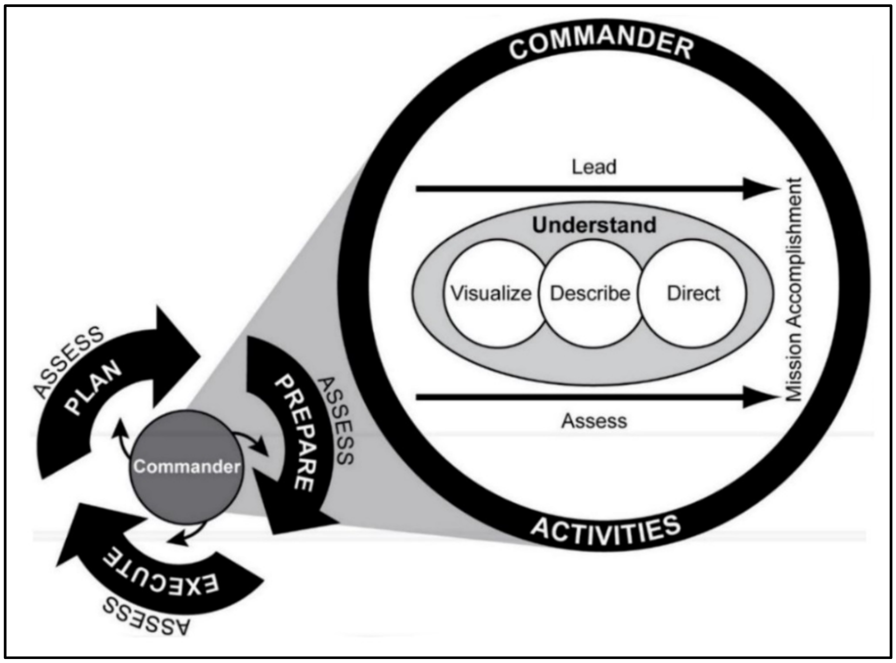


Figure 5-6. The operations process

5-107. PIO continuously feeds police information and police intelligence into the operations process through the integrating processes and ongoing military 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. The continuous flow of police information and police intelligence into the operations process enables commanders to achieve greater understanding and awareness of crime environments and criminal threats to assist in visualizing, describing, and directing current and future operations that account for and address relevant crime aspects of the operational environment.

5-108. PIO is continuously conducted by military police and USACIDC personnel to collect, produce, and disseminate police information and police intelligence on crime environments, criminal activity, and police and corrections infrastructure and systems. Police information is collected and analyzed from a unique policing viewpoint gained through experience in policing populations, conducting criminal investigations, and detaining criminal offenders. Information and intelligence from other operational elements are fused with police information and police intelligence delivered by military police and USACIDC to develop a common operational picture. See FM 3-39 for a further discussion of the military police perspective and core competencies.

CONTRIBUTIONS TO THE COMMON OPERATIONAL PICTURE

5-109. 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.

5-110. 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/G-2 and S-3/G-3 personnel to disseminate the appropriate and authorized police information and police intelligence for inclusion in the common operational picture.

CONTINUOUS ASSESSMENT

5-111. Assessment is a continuous process that precedes and concludes the operations process, scanning, analysis, response, and assessment policing model and is integral to modifying and adjusting the focus and direction of PIO. Figure 5-7 shows the activities of assessment, which includes—

- Monitoring the current situation to collect relevant information.
- Evaluating progress toward attaining end state conditions, achieving objectives, and performing tasks.
- Recommending or directing action for improvement.

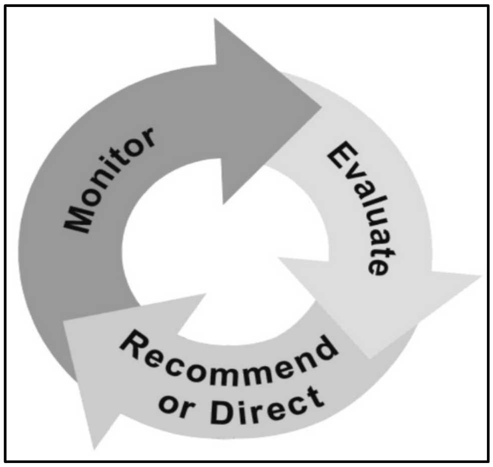


Figure 5-7. Activities of assessment

5-112. Continuous assessment plays a critical role in evaluating the information collected during the PIO process and in the effectiveness of the operations and the outputs that PIO produces. Continuous assessment throughout the conduct of PIO and the operations process enables commanders and staffs to make use of new information and change indicators related to the mission and operational variables to ensure that the staff—

- Answers the information and intelligence requirements.
- Provides clarification to ensure that military police collection assets understand the intent, objectives, and tasks necessary to fulfill intelligence requirements.
- Provides appropriate input to redirect military police collection assets.

5-113. During military police operations, the effectiveness of policing strategies is continuously assessed by monitoring crime trends, patterns, and other insights gained from crime analysis. Effective policing strategies should lead to lower crime rates and reduced criminal activity in the area of operations. *Monitoring* is continuous observation of those conditions relevant to the current operation (ADRP 5-0). Monitoring allows military police commanders and staffs to collect information about the current crime situation to determine if current policing strategies and approaches are successfully achieving the commander's intent and concept of operations or if they require modification. Progress cannot be judged—and effective decisions cannot be made—without an accurate understanding of the current situation.

5-114. Staffs analyze relevant information collected through monitoring to evaluate the operation's progress. *Evaluating* is using criteria to judge progress toward desired conditions and determining why the current degree of progress exists (ADRP 5-0). Evaluation is at the center of the assessment process where most of the analysis occurs. Evaluation helps commanders determine what is and what is not working, and it helps them gain insights into how to better accomplish the mission.

5-115. Criteria in the forms of measures of effectiveness (MOEs) and measures of performance (MOPs) aid in determining the progress toward attaining end state conditions, achieving objectives, and performing tasks. MOEs help determine if a task is achieving its intended results. MOPs help determine if a task is completed properly. MOEs and MOPs are simply criteria—they do not represent the assessment itself. MOEs and MOPs require relevant information in the form of indicators for evaluation (see table 5-2, page 5-28).

- **MOE.** A *measure of effectiveness* is a criterion used to assess changes in system behavior, capability, or operational environment that is tied to measuring the attainment of an end state, achievement of an objective, or creation of an effect (JP 3-0). MOEs help measure changes in conditions, both positive and negative. MOEs help to answer the question, "Are we doing the right things?" MOEs are commonly found and tracked in formal assessment plans. Examples of MOEs for the objective to provide a safe and secure environment may include—
  - A decrease in crime and criminal activity.
  - An increase in the population's trust of HN police forces.
- **MOP.** A *measure of performance* is a criterion used to assess friendly actions that is tied to measuring task accomplishment (JP 3-0). MOPs help answer questions such as, "Was the action taken?" or "Were the tasks completed to standard?" or "Are we doing things right?" A MOP confirms or denies that a task has been properly performed. MOPs are commonly found and tracked at all levels in execution matrices. MOPs are also commonly used to evaluate training. Using a MOP to evaluate a task accomplishment using MOPs is relatively straightforward and often results in a yes or no answer.
- **Indicator.** In the context of assessment, an indicator is an item of information that provides insight into a MOE or MOP. Indicators result from reports from subordinates, surveys and polls, and information requirements. Indicators help to answer the question, "What is the current status of this MOE or MOP?" A single indicator can influence multiple MOEs and MOPs. Examples of indicators for the MOE are the decrease in crime and criminal activity by the—
  - Number of crime incidents per area each week.
  - Number of drug seizures per area each week.
  - Number of reports of criminal activity by the population per area per week.

Table 5-2. Assessment measures and indicators

MOE	*MOP*	*Indicator*
Answers the question*: Are we doing the right things?*	Answers the question: *Are we doing things right?*	Answers the question: *What is the status of this MOE or MOP?*
Measures the purpose accomplishment.	Measures the task completion.	Measures raw data inputs to influence MOEs and MOPs.
Measures *why* in the mission statement.	Measures *what* in the mission statement.	The information used to make measuring *what* or *why* possible.
Often formally tracked in formal assessment plans.	Often formally tracked in execution matrixes.	Often formally tracked in formal assessment plans.
Typically challenging to choose the correct ones.	Typically simple to choose the correct ones.	Typically as challenging to select correctly as the supported MOE or MOP.
Legend: MOE measures of effectiveness MOP measures of performance		

5-116. Based on the evaluation of progress and effectiveness, the staff brainstorms possible improvements to the plan and makes preliminary judgments about the relative merit of those changes. Staff members identify those changes possessing sufficient merit and provide them as recommendations to the commander or make adjustments within their delegated authority. Commanders integrate recommendations from the staff, subordinate commanders, and other mission partners with their personal assessments. Using those recommendations, they decide if and how the operation should be modified to better accomplish the mission.

5-117. In decisive action, recommendations to the commander range from continuing the operation as planned, executing a branch, or making unanticipated adjustments. Making adjustments includes assigning new tasks to subordinates, reprioritizing support, adjusting information collection assets, and significantly modifying the course of action. During law enforcement and investigations on bases and base camps, recommendations may suggest adjustments to police management, patrol distribution, or investigative focuses.

5-118. Measuring the performance and effectiveness of policing and crime prevention efforts to shape future policing strategies and methods is an integral aspect of policing models such as CompStat. CompStat uses statistics, crime analysis, and other police intelligence products to evaluate police effectiveness through regular meetings and by holding subordinates accountable for criminal activity in an assigned jurisdiction or area of operations. CompStat allows military police commanders and staffs to evaluate police operations against empirical data to ensure the effective and efficient allocation of limited military police resources. Police operations that are ineffective or fail to achieve desired objectives may be modified or redirected to produce desired outcomes or effects. See ATP 3-39.10 for a discussion of the policing models.

5-119. PIO is a continuous and iterative process. As such, an assessment may conclude a cycle of PIO, provide direction for another cycle that modifies focus areas, introduce new aspects of crime problems that were not previously observed, or adjust information and intelligence requirements to drive police information collection. Police information collection may fully satisfy information or intelligence requirements; however, criminal and crime analysis often reveals other knowledge gaps related to crime environments and organized criminal activity that must be filled. When this happens, the assessment process provides critical feedback to guide future PIO planning and direction.

INTELLIGENCE PREPARATION OF THE BATTLEFIELD

5-120. *Intelligence preparation of the battlefield* is the systematic process of analyzing the mission variables of enemy, terrain, weather, and civil considerations in an area of interest to determine their effect on operations (ATP 2-01.3). Although staff integration of IPB is generally led by the S-2/G-2, all staff elements must fully participate and provide their individual areas of expertise to the effort. See ATP 2-01.3 for information on IPB. Figure 5-8 depicts the four IPB steps.

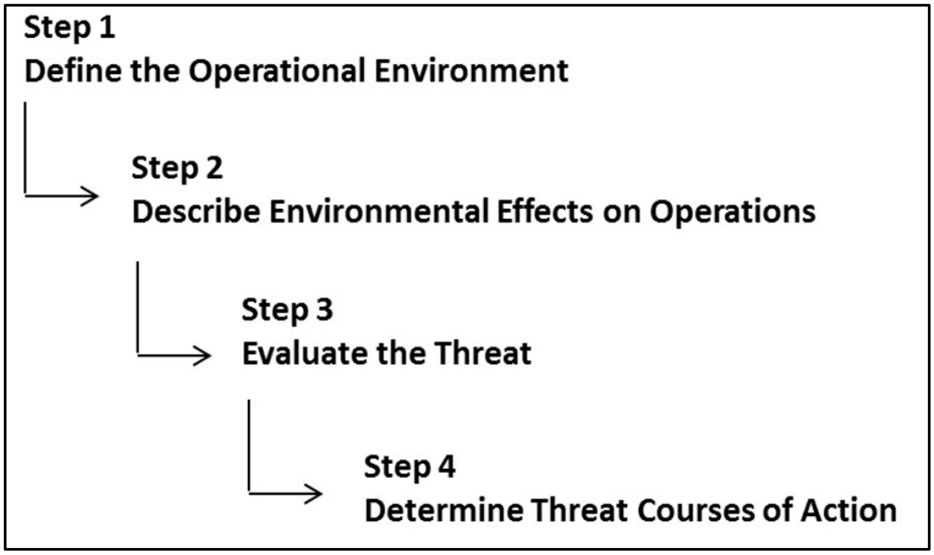

Step 1
Define the Operational Environment
Step 2
Describe Environmental Effects on Operations
Step 3
Evaluate the Threat
Step 4
Determine Threat Courses of Action

Figure 5-8. Intelligence preparation of the battlefield steps

5-121. Commanders and staffs develop the IPB 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 IPB products. All staff members must understand and participate in the IPB process. PIO is a reciprocating effort that feeds and draws from IPB to help commanders understand the crime aspects of the environment, mitigate vulnerabilities, and exploit opportunities to counter crime and criminal threats. In addition to tactical information obtained during the conduct of military police operations, PIO provides information on possible criminal threats and threats to stability and civil order that support current operations and may change friendly threat posture.

5-122. 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 by using the operational variables of political, military, economic, social, information, infrastructure, physical environment, and time analyzed and viewed from a policing perspective. See FM 3-39 for additional information on the operational variables analysis with a policing focus and on the military police commander and staff roles and responsibilities in supporting IPB.

5-123. Military police use the POLICE assessment tool for assessing crime environments, criminal activity, and police effectiveness in reducing crime and disorder in the operational environment. This assessment tool helps shape military police planning and the execution of military police operations. Military police and USACIDC personnel identify existing HN police and corrections organizations and assess police structures and current police capability and capacity, to include the existence or lack of a functioning legal system. Military police conduct criminal and crime analysis to assess the crime environment for crime-conducive conditions. They also assess the existence and activities of criminal networks and organizations. The POLICE assessment tool is 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 the U.S. and joint forces?
  - Is the equipment, communications systems, and other capabilities the indigenous police force have reliable? What equipment and capabilities are needed?
  - Does the police force have adequate systems (administrative, training, logistic, and investigative systems) in place to operate effectively?
  - 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?
  - Motivations for 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, including 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, guards, or police forces?
  - 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

5-124. *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 to nonlethal weapons to 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 (see figure 5-9). This targeting methodology facilitates the 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.

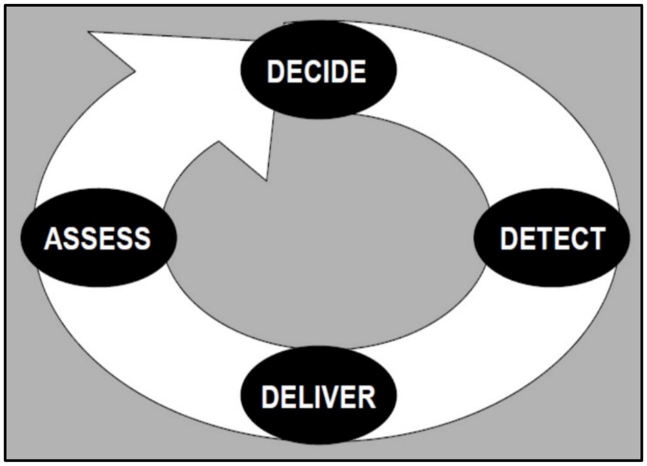


Figure 5-9. Decide, detect, deliver, and assess methodology cycle

5-125. In many operational areas, the threat is more criminal than conventional in nature. In these environments, belligerents use or mimic established criminal enterprises and methods 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 distinguishing that activity from other threat or environmental factors can be essential to effective targeting and mission success.

5-126. PIO contributes to the targeting process by providing timely, relevant, and accurate police information and police intelligence regarding 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 PIO supports the targeting process. PIO supports the targeting process by providing several unique policing skills and perspectives focused on the crime and criminal aspects of the operational environment. Military police leverage policing skills and knowledge using the PIO process to support the targeting process through—

- **Target identification.**
  - Uses the information gathered and stored in raw data files to identify threats (crimes, criminals, and other threat elements and activities) and locations of threat activity.
  - Identifies the organizations involved in the threat activity. This may be criminal enterprises affecting U.S. interests, or it may be irregular threat groups (terrorists, insurgents, or groups engaging in criminal activity that disrupts or endangers U.S. operations, including threats from corrupt officials or infiltrators internal to HN organizations).
- **Analysis of threat information.** Criminal and crime analysis is central to PIO. Analysis converts police information into police intelligence and contributes to other intelligence products (within mission, regulatory, and policy constraints).
  - 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 HN organizations. Police intelligence is also used to assess and clarify targets during the targeting process.
- **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, law enforcement surveillance, or other law enforcement source contacts.
  - 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 it can be acted on by the appropriate geographic combatant commander for military action.
- **Information sharing and support to active investigations.**
  - Regardless of the agency, ongoing investigations can be solved by using information that is collected and documented by military police and USACIDC personnel. One law enforcement officer may have an informant who knows the perpetrator of a burglary that another officer is investigating. Aggressive and proactive analysis and information sharing can contribute to the resolution of specific investigations or criminal activity across organizational lines.
  - In operational environments outside the U.S., this support can assist commanders and staffs by identifying key threat actors, 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.

5-127. Military police, USACIDC personnel, and police intelligence analysts integrate police 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 decide, detect, deliver, and assess methodology provides the structure for staffs to integrate analysis, monitor operations, and make recommendations enabling commanders to make informed targeting decisions. Table 5-3 illustrates decide, detect, deliver, and assess key activities and shows how military police and USACIDC personnel who conduct PIO integrate with the overall targeting process. See ATP 3-60 for additional information on the targeting process.

Table 5-3. Military police support to targeting

D3A Activities		***PIO 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 military police operations. • Develop the information collection plan. • Ensure that police-related intelligence requirements and the collection plan are integrated and synchronized with the overall information collection plan. • Identify change indicators relevant to the criminal environment. • Identify military police, USACIDC, or other collection assets capable of collecting against specific 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 assets (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 military police information collection efforts are synchronized with maneuver and other collection elements. • Monitor collection efforts. • Gather reports, evidence, and other pertinent police information. • Conduct debriefings of collection elements to ensure that all available police information is gathered and collated. • Analyze collected data to determine trends, patterns, and associations regarding crime, criminals, and associated data. • Identify potential targets (criminals, crime conditions, populations). • Develop criminal intelligence collection folders for specific criminal cases or targets. • Recommend adjustments to the information collection plan and policing strategies.

Table 5-3. Military police support to targeting (continued)

D3A Activities		***PIO Support to Targeting***
Deliver the appropriate effects (conduct the 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.	• Identify specific targets (criminals, crime conditions, populations) and timelines for recommended engagement. • Monitor change indicators for causal relationships (cause and effect). • 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 the 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(s) .	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 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 an analysis of postengagement 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	
PIO	police intelligence operations	
USACIDC	United States Army Criminal Investigation Command	

5-128. In brigade combat teams and echelons above brigade, the provost marshal is responsible for providing understanding of the crime environment, developing linkages between criminal actors, establishing correlations in time and space, and identifying trends and patterns in criminal activity that contributes to the targeting process by enabling selection and prioritizing crime and criminal targets. Provost marshals duties related to targeting include the following:

- Develop police intelligence products that enable targeting.
- Fuse police intelligence with the S-2/G-2 (within mission, regulatory, and policy constraints).
- Participate in targeting boards and provide recommendations for criminal targets or crime conditions or locations to concentrate effects.
- Identify high-payoff criminal targets and timelines for recommended engagement.
- Identify military police and USACIDC personnel for participation in targeting actions (lethal or nonlethal).

5-129. Developments in biometrics technology, evidence collection and examination at incident sites, site exploitation in operational areas, and corresponding forensic analysis capabilities have proven the effectiveness and relevance of PIO and its ability to provide timely and accurate police intelligence products to maneuver commanders and support 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 criminal and other irregular threats within an operational area and across combatant command areas of responsibility.

5-130. 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 the policing and protection of U.S. personnel and infrastructure follow the same basic methodology. Police intelligence, integrated into police operations on bases and base camps, is critical to enable effective, proactive, and responsive policing to target criminal offenders and crime-conducive conditions. Leveraging the targeting methodology is 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. Targeting the people who commit crimes and the places and problems that present opportunities for crime are essential components to achieving comprehensive and effective policing outcomes that reduce crime and the fear of crime among a population and provide a safe and secure environment.

RISK MANAGEMENT

5-131. Risk—the exposure of someone or something valued to danger, harm, or loss—is inherent in all operations. *Risk management* is the process to identify, assess, and control risks and make decisions that balance risk cost with mission benefits (JP 3-0). The Army uses risk management to help maintain combat power while ensuring mission accomplishment in current and future operations. Throughout the operations process, commanders and staffs use risk management to identify and mitigate risks associated with hazards that have the potential to injure or kill friendly and civilian personnel, damage or destroy equipment, or otherwise impact mission effectiveness. (See figure 5-10, page 5-36). As with targeting, risk management begins in planning and continues through preparation and execution. Risk management consists of the following steps:

- **Step 1**. Identify the hazards.
- **Step 2**. Assess the hazards.
- **Step 3**. Develop controls and make risk decisions.
- **Step 4**. Implement controls.
- **Step 5**. Supervise and evaluate.

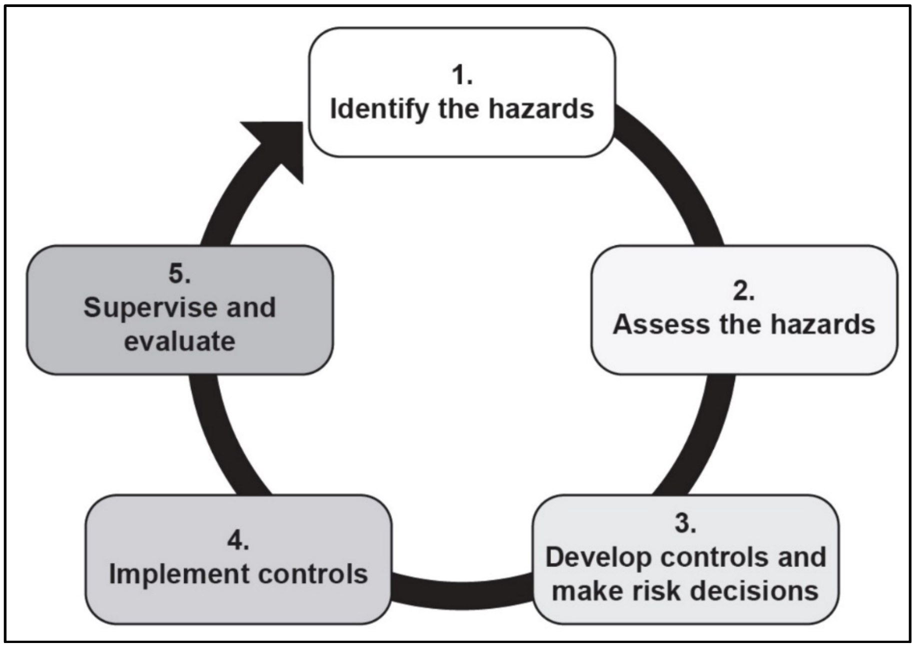


Figure 5-10. Risk management process

5-132. All staff elements incorporate risk management into their running estimates and provide recommendations for control measures to mitigate risk within their area of expertise. Risk management integration occurs during all operations process activities and is coordinated by the unit operations officer and protection officer. The provost marshal often directly participates in risk management processes by participating in protection cells or working groups that focus on risk management integration. Military police staff elements leverage police information and police intelligence related to crime environments, criminal threats, drivers of disorder and instability, and other crime factors threatening the safety and security of U.S. forces as part of the overall protection effort. See ATP 5-19 for discussion of the risk management process.

5-133. Information obtained through PIO directly contributes to the risk management process by identifying potential threats and hazards or conditions or problems that allow threats or hazards to pose a risk to U.S. forces and civilians. These risks may be 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 are corrupt. Lawlessness and disorder may present conditions with persistent threats and hazards due to—

- Widespread street crime across an area of operations.
- Unsafe conditions resulting from poor place management, regulatory oversight, and property maintenance.
- Corruption or lack of capacity by government or police to enforce laws pertaining to environmental hazards, safety standards, and public health and safety.

5-134. PIO supports the ability of commanders and staffs to prevent and mitigate risks by providing predictive analysis that may identify threats and hazards within the environment before they manifest themselves. These threats and hazards may be conventional, criminal, or environmental. The continuous flow of police information and police intelligence from military police and USACIDC elements into 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 determine the risk to personnel and equipment, assess the effects of those risks, and develop and implement control measures to mitigate threats or hazards.

Appendix A
Legal Requirements and Authorities

The number of agencies involved in PIO and the array of applicable laws, regulations, and directives can make navigating 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, DSCA, 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 PIO) and its restrictions and provisions to Army law enforcement conducting PIO are discussed in this appendix.

AUTHORITY TO CONDUCT POLICE INTELLIGENCE OPERATIONS

A-1. The following authoritative documents do not specifically refer to PIO; however, they do provide the authority and the premises on which to conduct PIO on installations. The police information and police intelligence that results from the activities described in the documents comprise the PIO activities. As implemented by AR 525-13, DODI 2000.12 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 2000.12 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 to support antiterrorism efforts.

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 conducted according to applicable regulations and directives. It also requires commanders to ensure that the threat information prepared by the intelligence community, USACIDC, provost marshals, and other organizations or sources is used when conducting threat assessments.

EXECUTIVE ORDER 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 EO is to apply to 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 described in EO 12333. Only foreign intelligence and counterintelligence elements (S-2/G-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 for 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 FBI. 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.

DEPARTMENT OF DEFENSE DIRECTIVE 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 while using their own forces and equipment. It also does not apply to authorized inspector general or military criminal investigative organization investigations by elements in the DOD.

DEPARTMENT OF DEFENSE DIRECTIVE 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 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 is 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. DOD policy prohibits the collecting, reporting, processing, or storing of information on individuals or organizations not affiliated with DOD, except in limited circumstances where such information is essential to the accomplishment of DOD missions. Information-gathering activities are under overall civilian control, while a high level of general supervision and frequent inspections exists at the field level. When collection activities are authorized to meet an essential requirement for information, maximum reliance is 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 is given to protect DOD functions and property in the different circumstances that exist in the geographic areas outside the continental United States. Relevant factors include the—

- Level of disruptive activity against U.S. forces.
- Competence of HN investigative agencies.
- Degree to which U.S. military and HN 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. The 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 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 persons being considered for participation in other authorized DOD programs.
- **Civil disturbance control.** 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 DOD to assist civil authorities in dealing with civil disturbances. Such authorization is granted only 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 in the United States and its territories or on U.S. citizens abroad, but it does not restrict the collection of information against non-U.S. belligerents outside the United States. The prohibitions state that—

- The acquisition of information on individuals or organizations not affiliated with 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.

DEPARTMENT OF DEFENSE DIRECTIVE 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 that have a law enforcement mission.

ARMY REGULATION 190-5

A-14. AR 190-5 establishes policy and procedures for motor vehicle traffic supervision. This regulation describes responsibilities and prescribes procedures for collecting, analyzing, and sharing data and information regarding traffic enforcement, accidents, and information sharing. Portions of this regulation relevant to PIO include—

- Selective enforcement by increased presence at places where violations, congestion, or accidents frequently occur based on traffic data, studies, and analysis.
  - Selective enforcement applies proper enforcement measures to traffic congestion and focuses on selected time periods, conditions, and violations that cause accidents.
  - Law enforcement personnel rely on police intelligence products to influence and focus selective enforcement to ensure the most effective use of resources.
- Law enforcement personnel record traffic accident investigations and release information according to policy, the Privacy Act, and the Freedom of Information Act.
  - These law enforcement officers provide local safety offices copies of traffic accident investigation reports.
  - The reports pertain to accidents investigated by military police personnel that resulted in a fatality, personal injury, or estimated damage to government vehicles or property in excess of $1,000.
- Data derived from traffic accident investigation reports and from vehicle owner accident reports is analyzed to determine probable causes of accidents. When frequent accidents occur at a location, the conditions at the location and the types of accidents (collision diagram) are examined.
- Data shared with the installation legal, engineer, safety, and transportation officers. The data is used to inform and educate drivers and to conduct traffic engineering studies.

ARMY REGULATION 190-24

A-15. 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.
- 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.

Note. On an armed forces disciplinary control board where an Army installation is the senior service, the provost marshal typically serves as the senior representative.

A-16. 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-17. 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 constraints of Section 1385, Title 18, United States Code (18 USC 1385) and with applicable agreements between the United States and HNs. 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-18. The constraints on the authority of Soldiers and DA Civilian police to act on off-installation operations (and the specific scope of off-installation operations) are clearly delineated in all authorizations for off-installation support. Off-installation operations are coordinated with the local installation commander through the staff judge advocate or higher authority and appropriate civilian law enforcement agencies. 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.

ARMY REGULATION 190-30

A-19. AR 190-30 describes the purpose of gathering police intelligence to identify individuals or groups of individuals to anticipate, prevent, or monitor possible criminal activity. It states that an investigation by the military police, USAICDC, or other investigative agency will be initiated if police intelligence is developed to the point at which it factually establishes a criminal offense. Furthermore, it specifies that police intelligence will be actively exchanged between DOD law enforcement agencies; military police; USACIDC; and local, state, federal, and international law enforcement agencies.

A-20. This regulation discusses the development of a tool (called the Joint Protection Enterprise Network) created for DOD for sharing police intelligence. The Joint Protection Enterprise Network provides users with the ability to post, retrieve, filter, and analyze real-world events based on seven reporting criteria:

- Nonspecific threats.
- Surveillance.
- Elicitation.
- Tests of security.
- Repetitive activities.
- Bomb threats/incidents.
- Suspicious activities/incidents.

ARMY REGULATION 190-45

A-21. 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 and the 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 ALERTS 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 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, the 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-22. In referring specifically to PIO, AR 190-45 states that when pertaining to garrison law enforcement operations, the purpose of gathering police intelligence is to identify individuals or groups of individuals 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-23. 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-24. This regulation establishes policy regarding the—

- Information exchanges 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 only 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.

ARMY REGULATION 195-2

A-25. 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 to 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 is 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, similar to 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 decision-making ability.

ARMY REGULATION 380-13

A-26. 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 USACIDC. 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 the prompt reporting to Army law enforcement personnel of any information that indicates the existence of a threat to life or property and the violation of a law.

ARMY REGULATION 381-10

A-27. 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 are relinquished to USACIDC or the appropriate military police investigating agency according to AR 190-45 and AR 195-2.

A-28. 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 is 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-29. 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-30. The term collection, as defined in AR 381-10, is different from the everyday, common definition of assemble or gather. The AR 381-10 definition includes the intent to use or retain information received from cooperating sources.

ARMY REGULATION 525-13

A-31. AR 525-13 establishes and provides implementation guidance and requirements for the antiterrorism program. The antiterrorism program protects—

- Soldiers.
- Members of other Services.
- DA Civilian employees.
- DOD contractors.
- Family members of DOD personnel.
- Information.
- Property.
- Facilities.

A-32. 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 Headquarters, DA; Assistant chief of staff for operations (G-3) for the management and execution of the Army antiterrorism mission, are 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 Headquarters, DA, Office of the Deputy Chief of Staff and the 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-33. 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, HN, 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 HN 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 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-34. 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 HN intelligence, criminal investigations, police information, and police intelligence.
- Coordinate law enforcement support with higher headquarters if 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 is integrated into the antiterrorism training program.

A-35. In reference to terrorist threat assessments, AR 535-13 specifically addresses the law enforcement and intelligence community as follows:

- Threat information prepared by the intelligence community, USACIDC, and the provost marshal's office is used when conducting threat assessments and collecting technical information from information management.
- Threat assessments serve as the basis and justification for antiterrorism plans, enhancements, program and budget requests, and the establishment of force protection conditions.
- Threat assessments are 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-36. Ordinarily a SOFA is established when a long-term U.S. presence is required or anticipated. While this is common, some areas of operations in which U.S. forces operate do not have established SOFA agreements between the United States and the HN. This is common in an area of operations experiencing major combat operations or significant instability. As the theater matures and a stable HN government establishes control, a SOFA is typically developed if an enduring U.S. presence is required.

A-37. A SOFA plays a vital role in preserving command authority and the protecting military personnel. The purpose of a SOFA is to set forth rights and responsibilities between the U.S. government and an HN government on matters such 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-38. All SOFAs are unique and reflect specific considerations based on the countries entering into the agreement. 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 recognizes the right of an HN government to primary jurisdiction, allowing jurisdiction for cases in which U.S. military personnel violate HN laws. Most SOFAs provide two exceptions for which 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-39. In some areas of operations, agreements between the United States and HN countries may establish legal parameters regarding U.S. authority over HN personnel. The HN typically retains jurisdiction over its citizens; however, in some cases, the HN 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 HN 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 HN 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 an HN population.

A-40. As the operational environment becomes stable and the HN begins to reestablish the rule of law, U.S. military forces may still be necessary to assist the HN in policing activities. This is only done pending the full assumption of control by the HN. During the interim, legal agreements between the HN 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 HN and that the rights of the local population are maintained.

This page intentionally left blank.

Appendix B

Police Intelligence Products

This appendix provides examples of various police intelligence products. These examples are baseline products; they change with command and HN requirements, technological advances, and legal restrictions. Formats may vary; however, the accuracy, timeliness, and relevancy of the product is critical to the targeted audience. Several analytical techniques generate products during the process of analysis that can be prepared for respective audiences and disseminated throughout. This appendix provides examples of the types of police intelligence products discussed in chapter 4.

CRIMINAL INTELLIGENCE PRODUCTS

B-1. Criminal intelligence products share information pertinent to known or suspected criminals to inform the public or gain credible information that may assist in the prevention, investigation, or apprehension of criminal offenders. This section provides examples of criminal intelligence products that may be produced during criminal analysis.

CRIMINAL INTELLIGENCE REPORT, BULLETIN, OR ADVISORY

B-2. Figure B-1 displays an example criminal intelligence report (also called bulletin or advisory depending on the receiving audience, such as internal to an Army law enforcement organizations, across the broader law enforcement community, or to a specific unit or commander requiring the information).

[CLASSIFICATION]
CRIMINAL INTELLIGENCE REPORT

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.

Figure B-1. Example of a criminal intelligence report

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	MPR	military police report
MP	military police	PIA	police intelligence advisory

Figure B-1. Example criminal intelligence report (continued)

Criminal Alert Notice

B-3. Figure B-2 shows an example criminal alert notice.

CRIMINAL 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.

Figure B-2. Example of a criminal alert notice

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.

Criminal 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. Criminal 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 are 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 Doe, 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.

Legend:

U.S.	United States

Figure B-2. Example of a criminal alert notice (continued)

Be-On-the-Lookout Alert

B-4. Figure B-3 and figure B-4, page B-4, provide two examples of BOLO alerts in FBI and Army formats.

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

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.

Figure B-3. Example of a Federal Bureau of Investigations be-on-the-lookout alert

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 https://www.fbi.gov/.

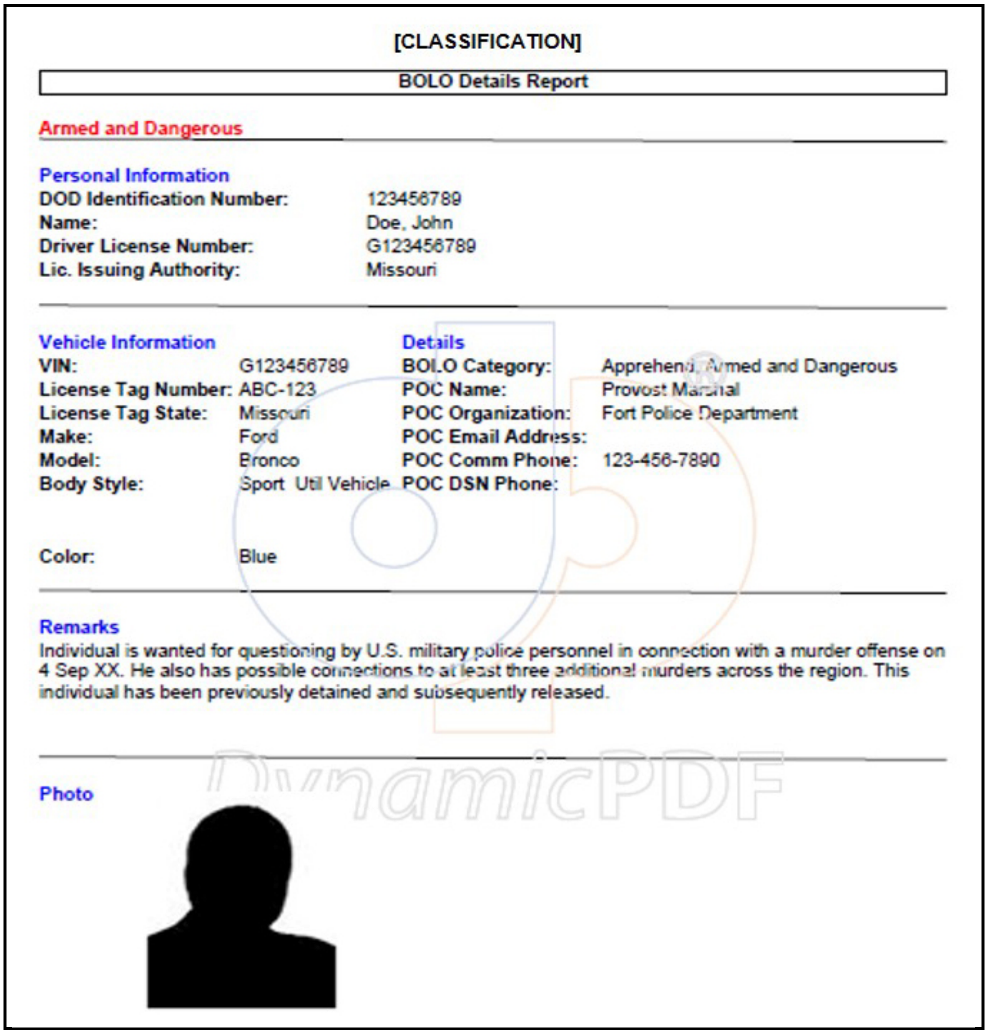
The subject carries a Guyana passport; however, he may attempt to enter the United States with a Saudi Arabia, Trinidad, or Canadian passport. The subject is also known by the following aliases:

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

Legend:

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

Figure B-3. Example of a Federal Bureau of Investigations be-on-the-lookout alert (continued)



[CLASSIFICATION]

BOLO Details Report

Armed and Dangerous

Personal Information

DOD Identification Number: 123456789
Name: Doe, John
Driver License Number: G123456789
Lic. Issuing Authority: Missouri

Vehicle Information

VIN: G123456789
License Tag Number: ABC-123
License Tag State: Missouri
Make: Ford
Model: Bronco
Body Style: Sport Util Vehicle

Color: Blue

Details

BOLO Category: Apprehend, Armed and Dangerous
POC Name: Provost Marshal
POC Organization: Fort Police Department
POC Email Address:
POC Comm Phone: 123-456-7890
POC DSN Phone:

Remarks

Individual is wanted for questioning by U.S. military police personnel in connection with a murder offense on 4 Sep XX. He also has possible connections to at least three additional murders across the region. This individual has been previously detained and subsequently released.

DynamicPDF

Photo

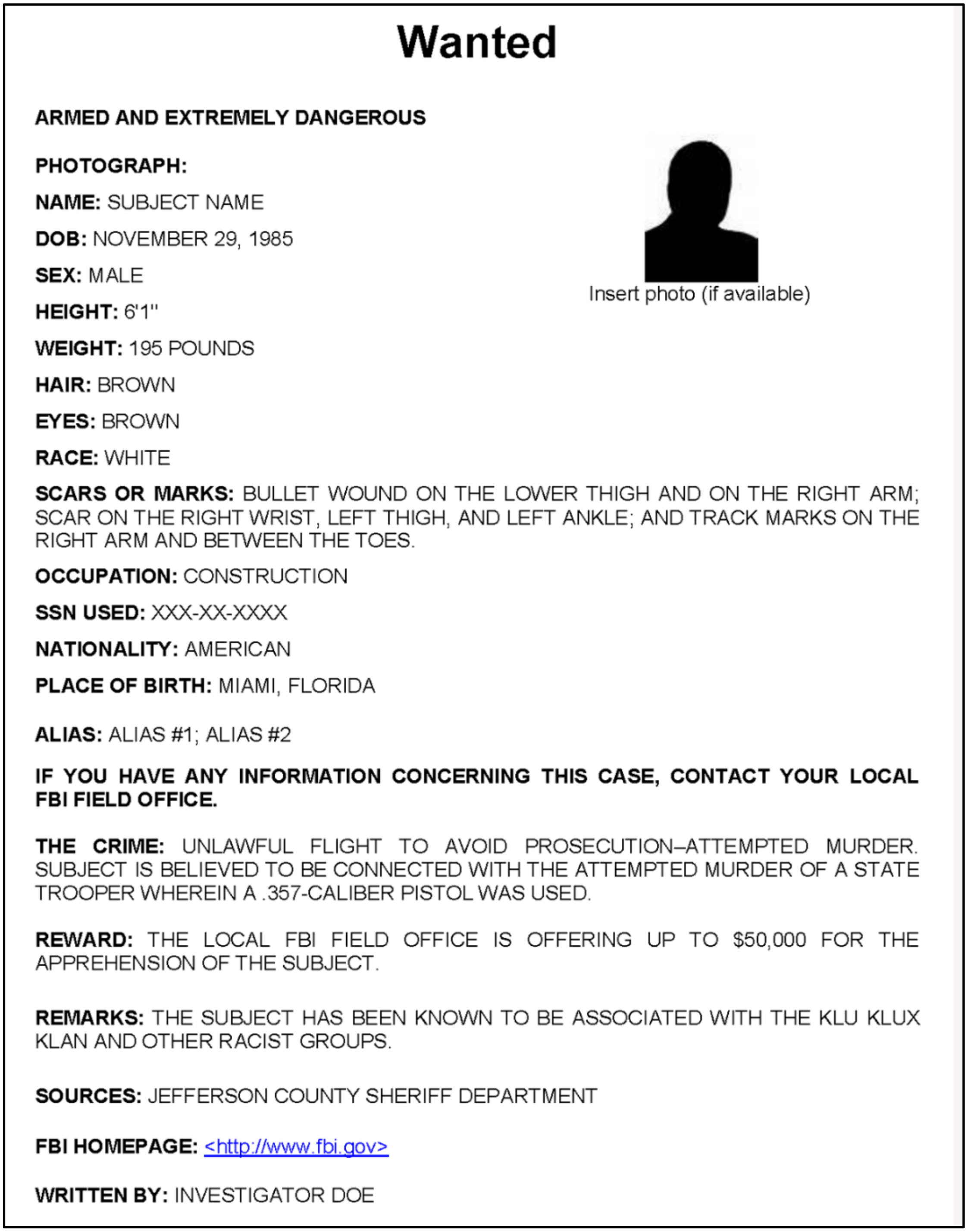
Legend:

BOLO	be-on-the-lookout	POC	point of contact
DSN	Defense Switched Network	U.S.	United States
DOD	Department of Defense	VIN	vehicle identification number

Figure B-4. Example of an Army BOLO alert

WANTED POSTERS

B-5. Figure B-5 and figure B-6, page B6, provides examples of a wanted posters.



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

Figure B-5. Example of a Federal Bureau of Investigations 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.

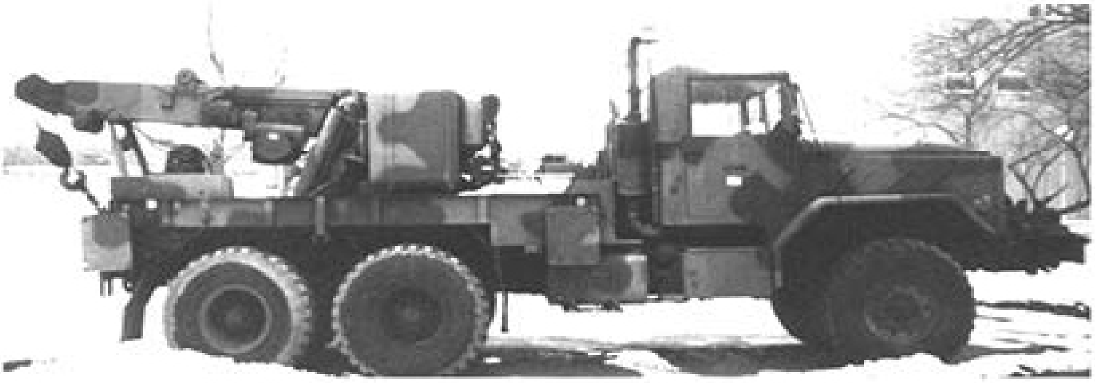
Legend:			
APO	Army post office	HMMWV	high-mobility, multipurpose, wheeled vehicle
CID	criminal investigation division	USACIDC	United States Army Criminal Investigation Command
DSN	Defense Switched Network		

Figure B-6. Example of a United States Criminal Investigation Command wanted poster

Reward Posters

B-6. Figure B-7 provides an example of a reward 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 is 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 B-7. Example of a reward poster

Communication (Toll) Analysis Chart

B-7. Figure B-8 provides an example communication (or toll) analysis chart.

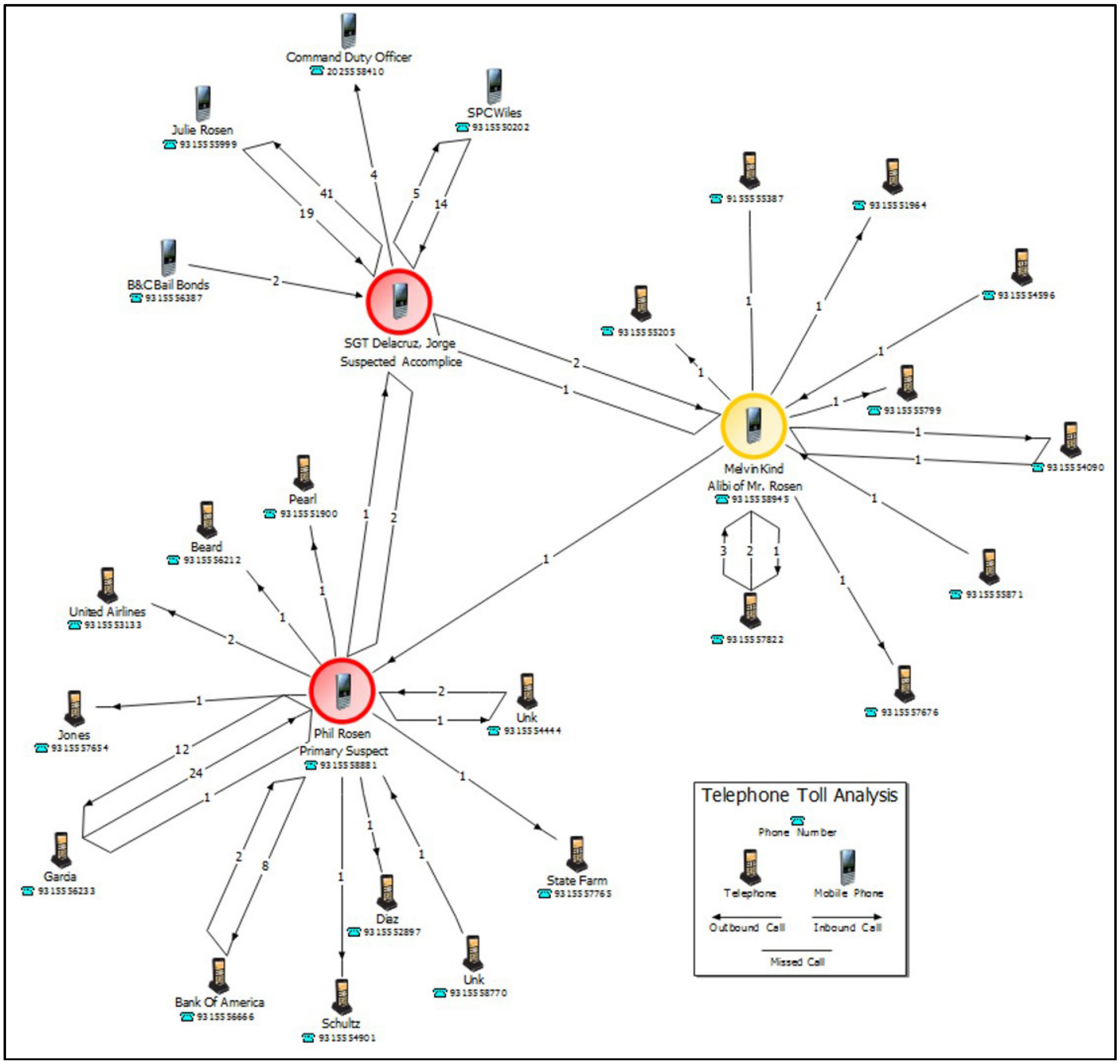


Figure B-8. Example of a communication (toll) analysis chart

Link Analysis Diagram

B-8. Figure B-9, page B-8, demonstrates a link analysis diagram generated by using analytical software with which police intelligence analysts may be equipped with to perform criminal and crime analysis.

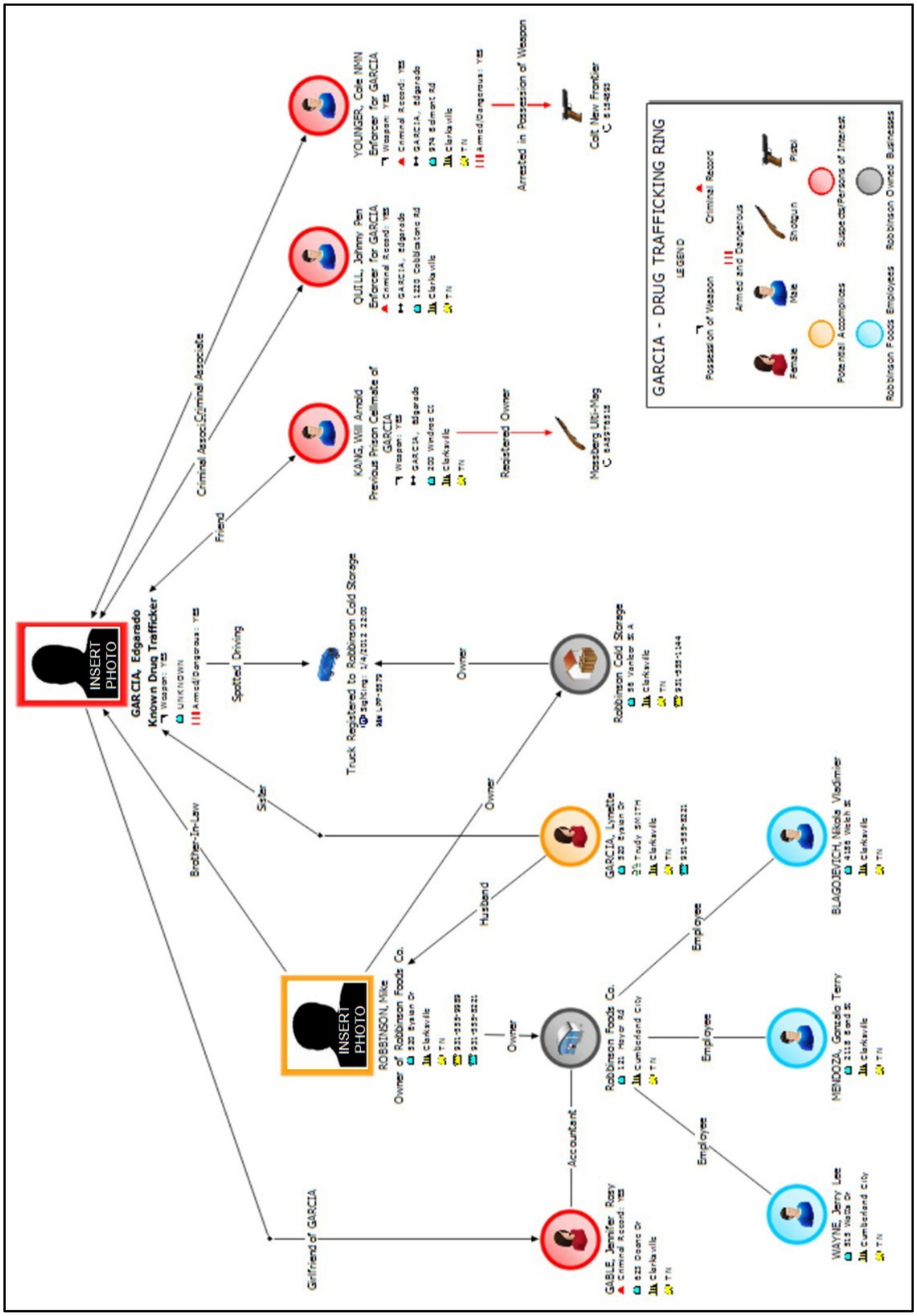


Figure B-9. Example of a link analysis product

Timeline and Theme Line Flow Chart

B-9. Figure B-10 provides an example timeline and theme line flow chart.

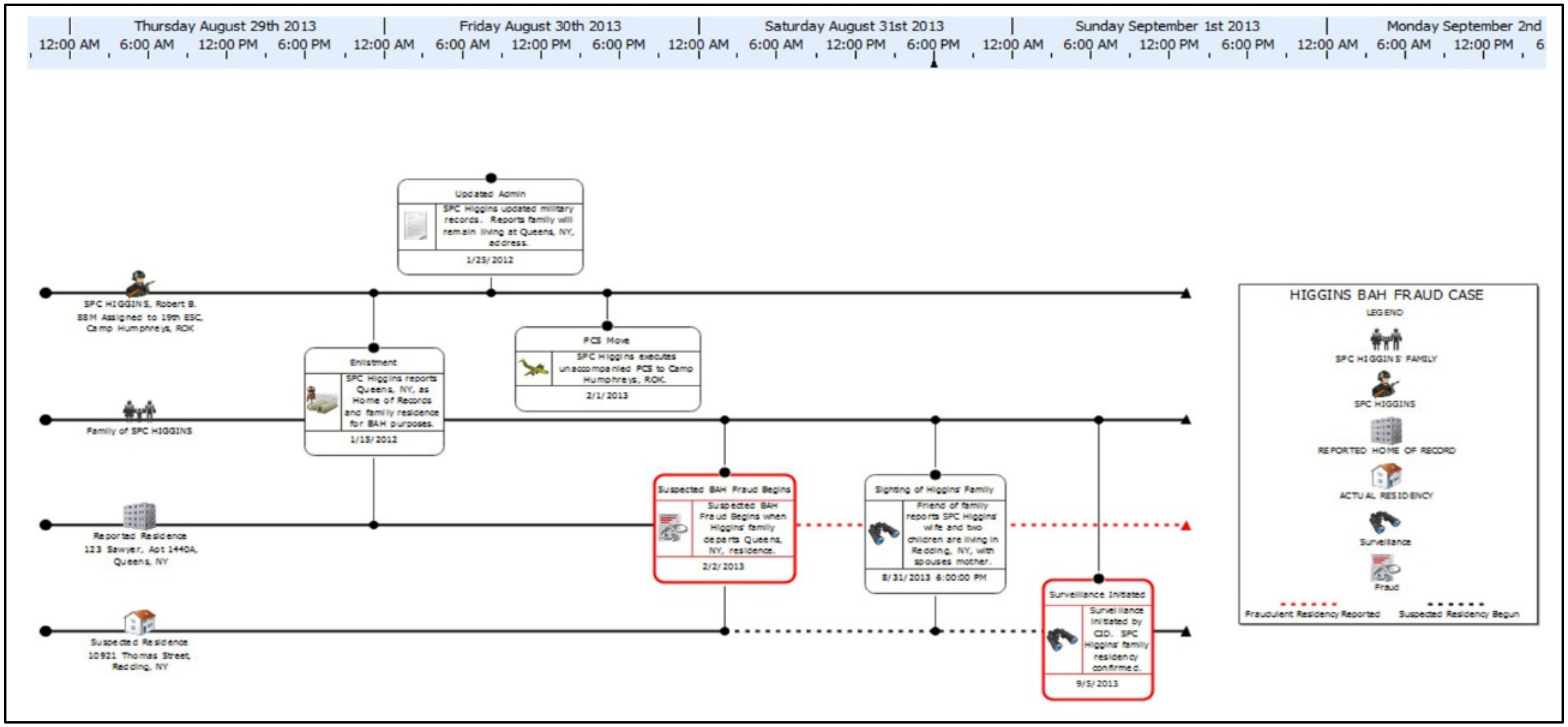
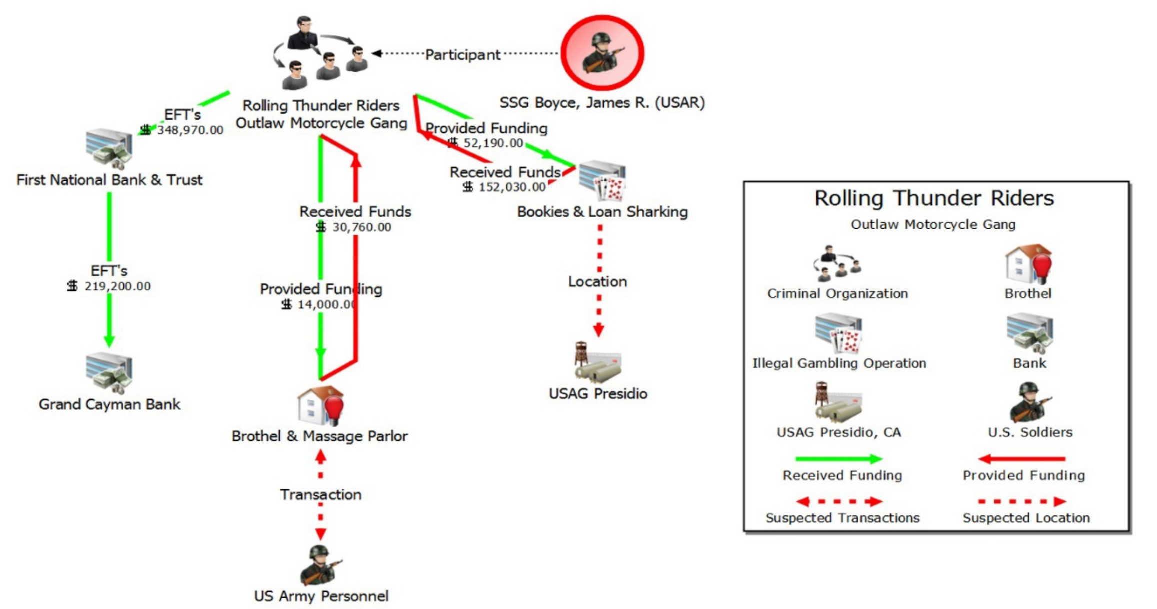

Thursday August 29th 2013
Friday August 30th 2013
Saturday August 31st 2013
Sunday September 1st 2013
Monday September 2nd
12:00 AM
6:00 AM
12:00 PM
6:00 PM
6
SPC HIGGINS, Robert B.
88M Assigned to 19th ESC,
Camp Humphreys, ROK
Family of SPC HIGGINS
Reported Residence
123 Sawyer, Apt 1440A,
Queens, NY
Suspected Residence
10921 Thomas Street,
Redding, NY
Updated Admin
SPC Higgins updated military records. Reports family will remain living at Queens, NY, address.
1/25/2012
Enlistment
SPC Higgins reports Queens, NY, as Home of Records and family residence for BAH purposes.
1/15/2012
PCS Move
SPC Higgins executes unaccompanied PCS to Camp Humphreys, ROK.
2/1/2013
Suspected BAH Fraud Begins
Suspected BAH Fraud Begins when Higgins' family departs Queens, NY, residence.
2/2/2013
Sighting of Higgins' Family
Friend of family reports SPC Higgins' wife and two children are living in Redding, NY, with spouses mother.
8/31/2013 6:00:00 PM
Surveillance Initiated
Surveillance initiated by CID. SPC Higgins' family residency confirmed.
9/5/2013
HIGGINS BAH FRAUD CASE
LEGEND
SPC HIGGINS' FAMILY
SPC HIGGINS
REPORTED HOME OF RECORD
ACTUAL RESIDENCY
Surveillance
Fraud
Fraudulent Residency Reported
Suspected Residency Begun

Figure B-10. Example of a timeline and theme line flow chart

Commodity Flow Chart

B-10. Figure B-11 provides an example commodity flow chart.



Legend:

CA	California	USAG	United States Army Garrison
EFT	electronic funds transfer	U.S.	United States
SSG	staff sergeant		

Figure B-11. Example of a commodity flow chart

Combined Charts

B-11. Figure B-12 depicts a chart that combines several different analysis techniques and types of information to depict connections across time, space, people, places, and things that can greatly enhance the understanding of criminal networks and activities in dynamic, multifaceted, and complex relationships.

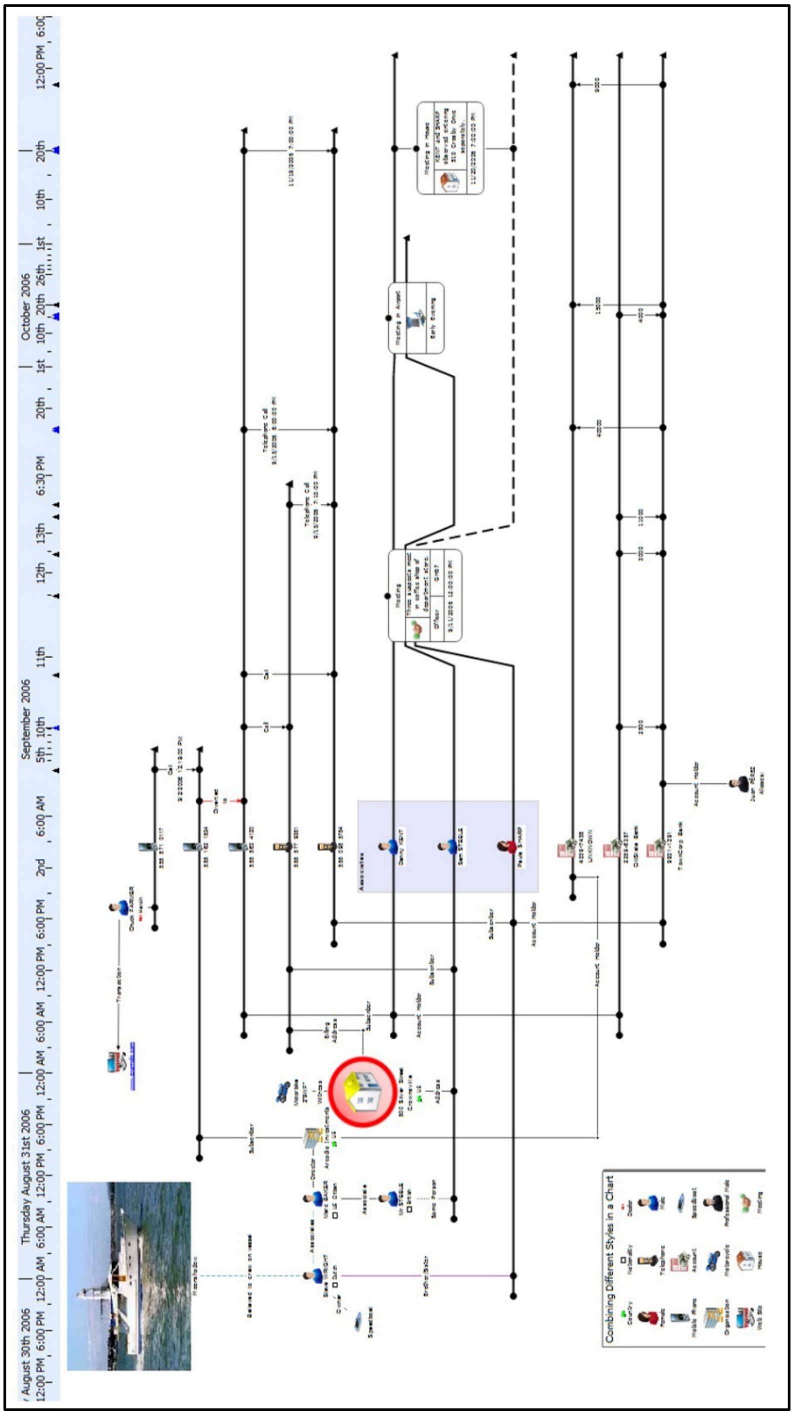


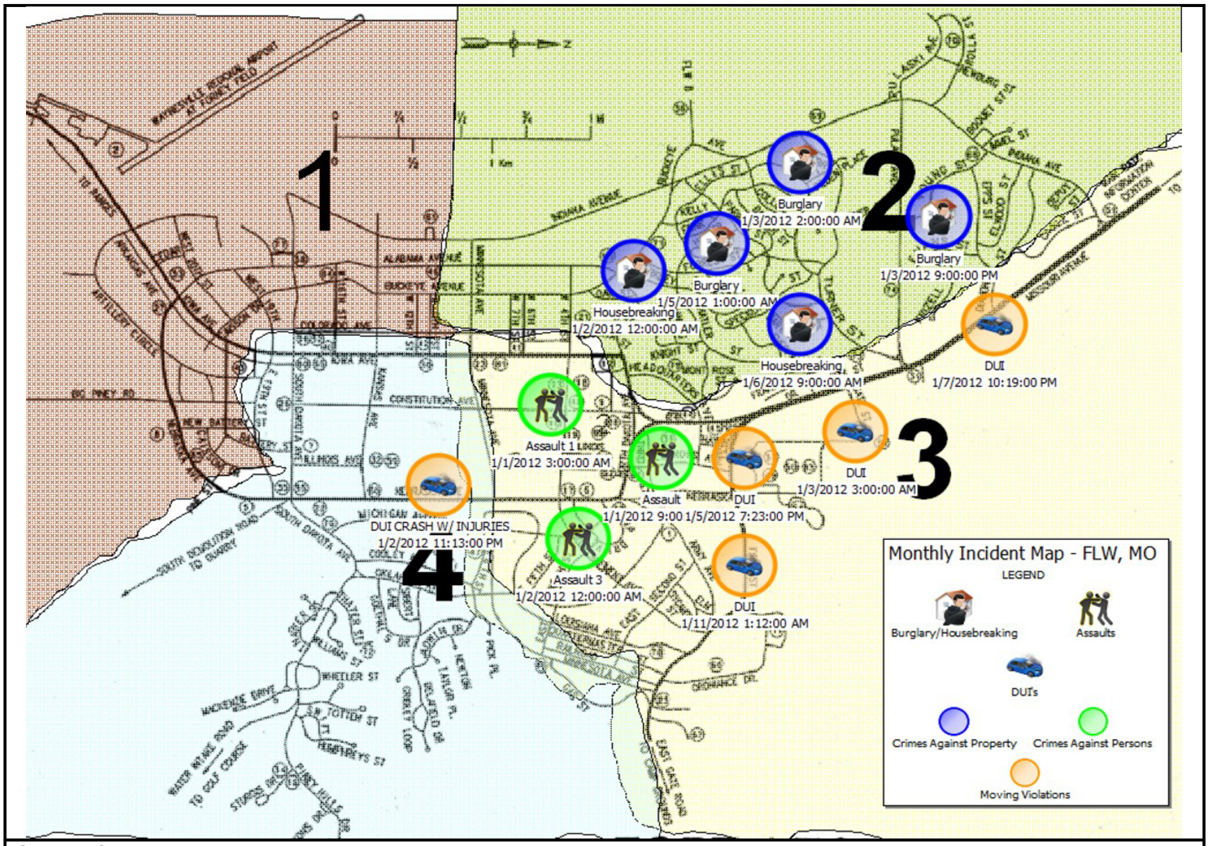
Figure B-12. Example of a combined chart

CRIME ANALYSIS PRODUCTS

B-12. Crime analysis products focus on the places, patterns, and problems that are producing crime opportunities and contributing to crime-conducive conditions. This section provides some examples of crime analysis products that may be produced during the crime analysis process.

Crime (or Incident) Maps

B-13. Figure B-13 provides an example crime (or incident) map.



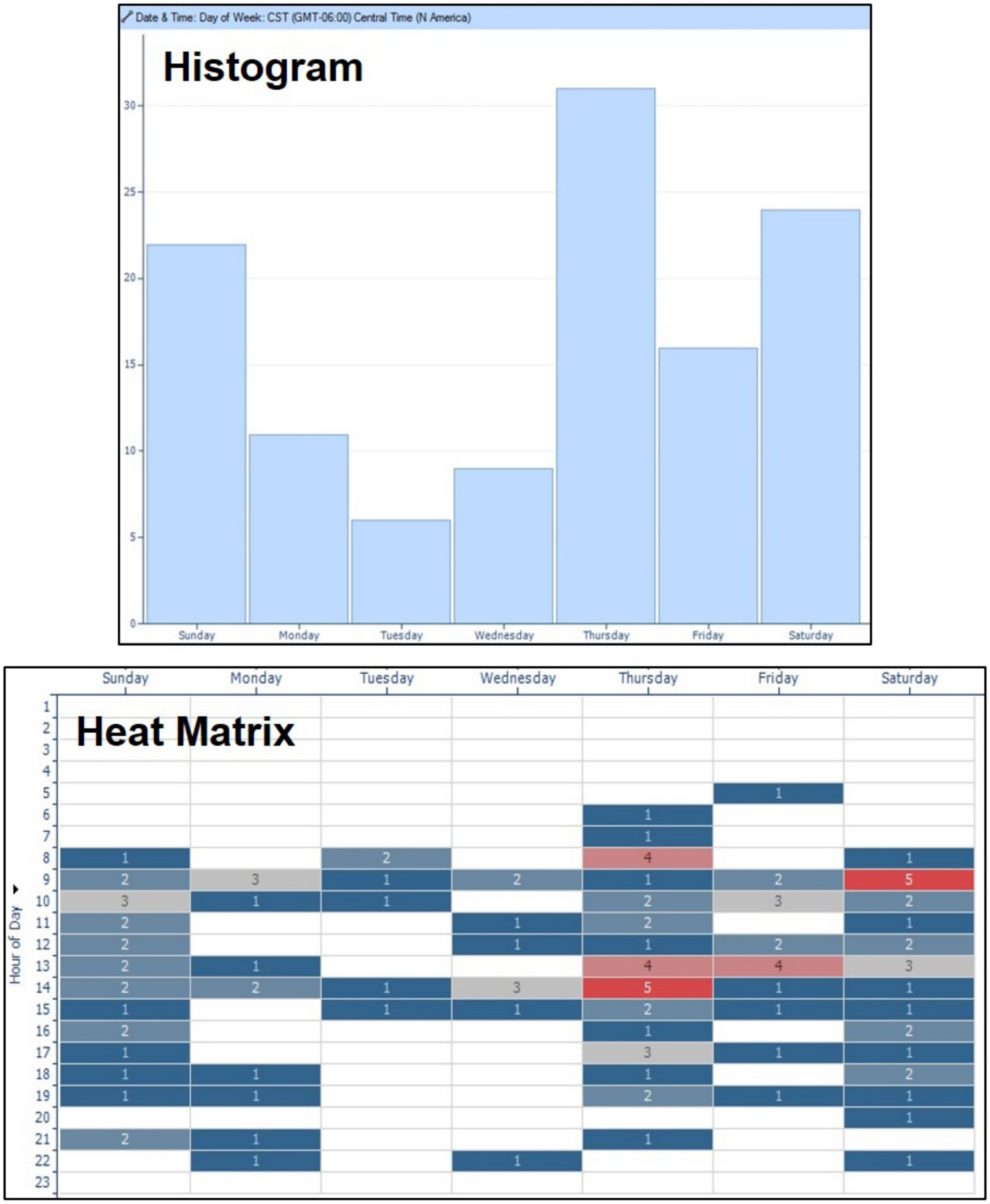
Legend:

DUI	driving under the influence	MO	Missouri
FLW	Fort Leonard Wood		

Figure B-13. Example of a crime (or incident) map

Histograms and Heat Matrices

B-14. Figure B-14 provides an example of a histogram and heat matrix.

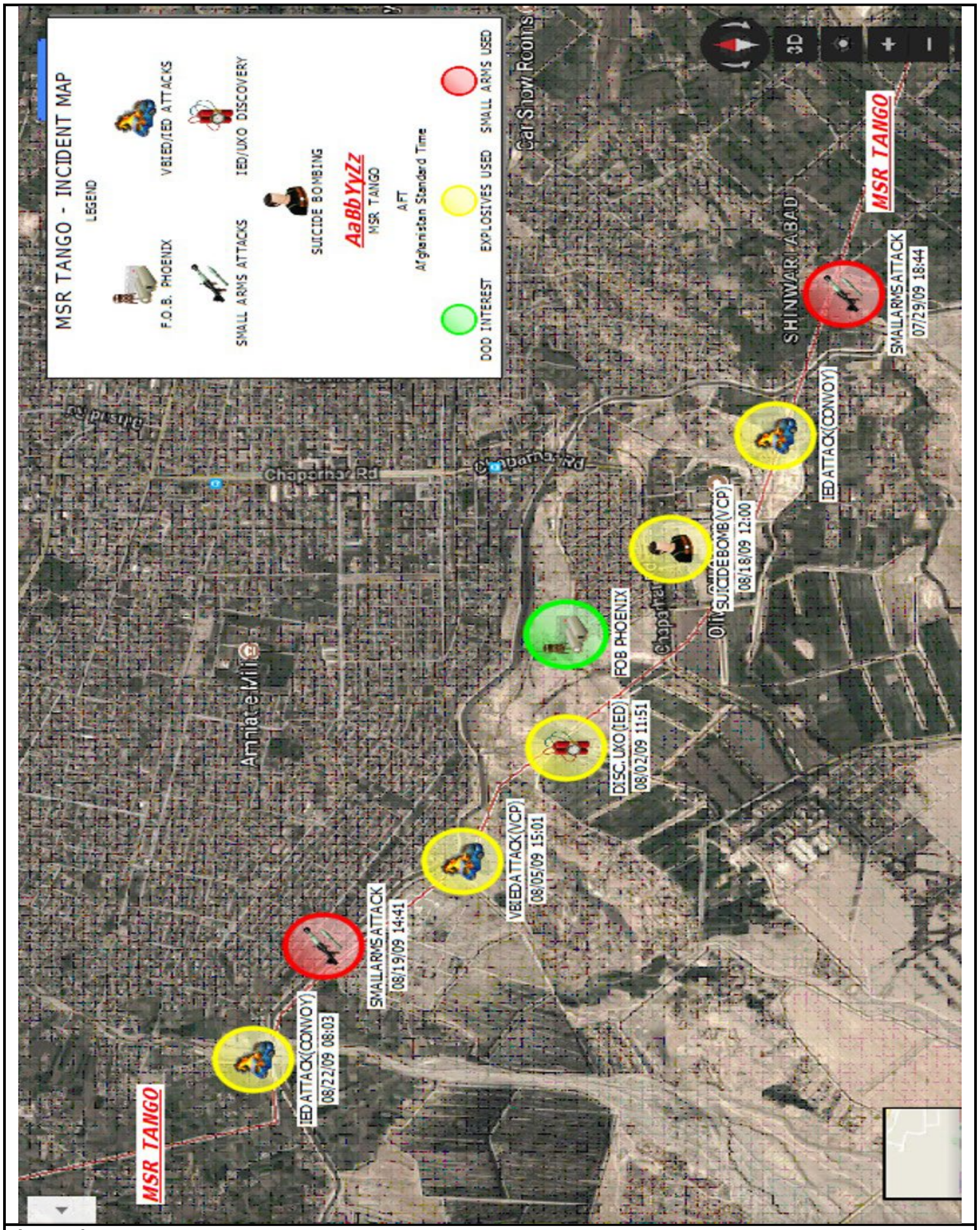


Hour of Day	Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
1							
2							
3							
4							
5						1	
6					1		
7					1		
8	1		2		4		1
9	2	3	1	2	1	2	5
10	3	1	1		2	3	2
11	2			1	2		1
12	2			1	1	2	2
13	2	1			4	4	3
14	2	2	1	3	5	1	1
15	1		1	1	2	1	1
16	2				1		2
17	1				3	1	1
18	1	1			1		2
19	1	1			2	1	1
20							1
21	2	1			1		
22		1		1			1
23							

Figure B-14. Example of a histogram and heat matrix

Geospatial Mapping

B-15. Figure B-15, page B-14, displays an example incident map that uses geospatial mapping technology.



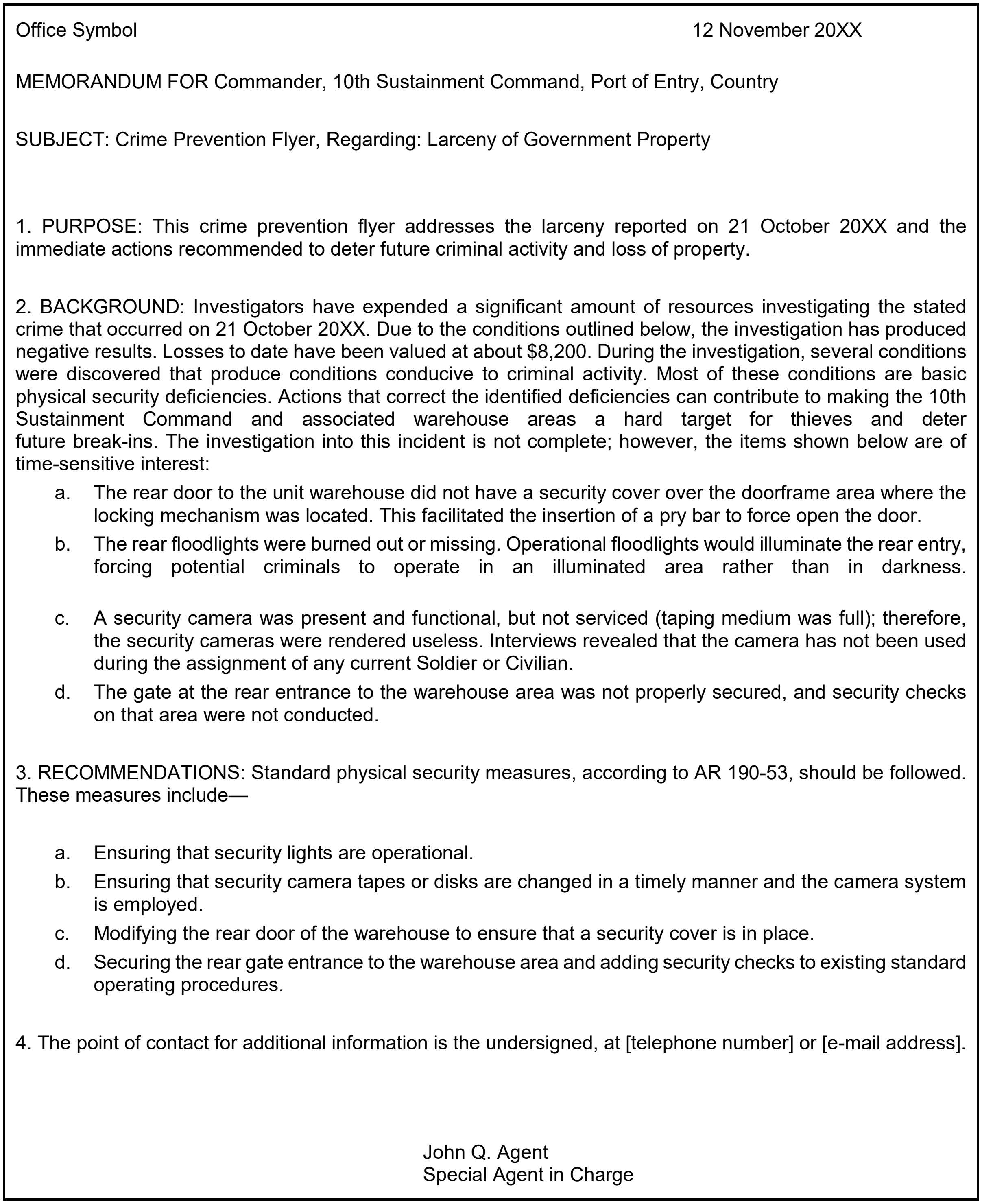
Legend:

DOD	department of defense	UXO	unexploded ordinance
FOB	forward operating base	VBIED	vehicle-borne improvised explosive device
IED	improvised explosive device	VPC	vehicle collection point
MSR	main supply route		

Figure B-15. Example of an incident map that uses geospatial technology

Crime Prevention Flyer

B-16. Figure B-16 displays an example crime prevention flyer.



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 B-16. Example of a crime prevention flyer

This page intentionally left blank.

Appendix C

Police Intelligence Employment Considerations

This appendix provides several employment considerations to support the implementation of the doctrine contained in this manual. First, considerations for military police forces are discussed for implementing PIO within military police companies, battalions, and brigades/groups. Second, considerations for supported Army forces are provided to generate understanding of what PIO capabilities can provide to commanders at the brigade combat team, division, and corps levels. Lastly, this appendix provides several resources for military police, USACIDC personnel, and police intelligence analysts to help inform their efforts to conduct PIO.

CONSIDERATIONS FOR MILITARY POLICE FORCES

C-1. PIO is insufficient unless it is capable of being employed to influence situational awareness, support commander's decision making, and enhance efforts to protect the force and preserve readiness. This section provides several employment considerations across various echelons and force structures that support the ability of military police, USACIDC personnel, and police intelligence analysts to achieve relevant and sustainable outcomes through the implementation and integration of PIO into military police operations and support.

MILITARY POLICE COMPANY

C-2. Recent operational experience has demonstrated that a lack of sufficient police intelligence capabilities within the military police company significantly limits the ability of military police commanders to provide police intelligence support to maneuver commanders to understand relevant crime, criminal, and policing aspects of the operational environment. Due to the lack of organic police intelligence personnel and organizations at the company level, military police companies often develop ad hoc solutions (such as the development of the PIO team) to enable the conduct of PIO at the company level.

C-3. Military police company commanders may organize and train PIO teams from within their assigned and experienced military police Soldiers to perform criminal and crime analysis and produce police intelligence products to inform company leadership and supported maneuver formations. The PIO team does this by combining police information gained from military police operations with other information and intelligence received from adjacent and higher units. The PIO team analyzes and reports police information collected by the company while receiving, reviewing, and integrating information and intelligence collected from other organizations into the company common operational picture. The ability of military police commanders to organize and train a PIO team significantly increases the military police company's ability to perform PIO and produce timely, accurate, and relevant police intelligence products. This section provides broad descriptions of PIO teams.

Mission

C-4. The mission of the PIO team is to describe the effects of crime environments, criminal threats, and police and detention organizations to assist efforts to prevent, monitor, and reduce crime, criminal activity, disorder, and fear of crime amongst relevant populations. The PIO team provides criminal and crime analysis, production, and dissemination capability to the military police company commander to support situational awareness, support protection efforts, and shape crime and criminal environments through effective and efficient police prevention and response efforts. This support also enables military police commanders to—

- Assist commanders and provost marshals in preventing, investigating, and reducing crime within formations, on bases and base camps, and across an area of operation.
- Enhance commander crime prevention and protection programs and efforts.
- Feed the Army operations process and its integrating activities with timely, relevant, and accurate police information and intelligence related to crime, criminal activity, disorder, and fear of crime amongst relevant populations.

Organization and Tasks

C-5. The manning and organization of a PIO team is dependent on the situation and varies according to the operational environment and assigned mission. When performing in a relatively static environment (law enforcement on bases and base camps), a PIO team may be smaller and have a more normalized battle rhythm when performing crime and criminal analysis in support of ongoing and routine police operations. When performing in dynamic and expeditionary environments (in combat training centers or when deployed), a PIO team should increase in size to accommodate for continuous and sustained operations. The ideal approach may be to first organize and train a core PIO team as a foundation to develop the capability of producing crime analysis and criminal intelligence as part of PIO and then train additional resources as time permit.

C-6. An initial PIO team likely consists of an officer or noncommissioned officer in charge; two police intelligence analysts capable of conducting crime and criminal analysis techniques; and an experienced military police Soldier capable of performing administrative tasks, preparing reports, and demonstrating familiarity with police operations and processes. As resources permit, that foundational PIO team may be expanded with additional analysts to provide greater analytical capacity or to enable the PIO team to perform continuous and sustained operations. Chapter 4 discusses the variety of analysis techniques that police intelligence analysts may be tasked to perform. Figure C-1 provides an example organization and tasks for establishing a PIO team.

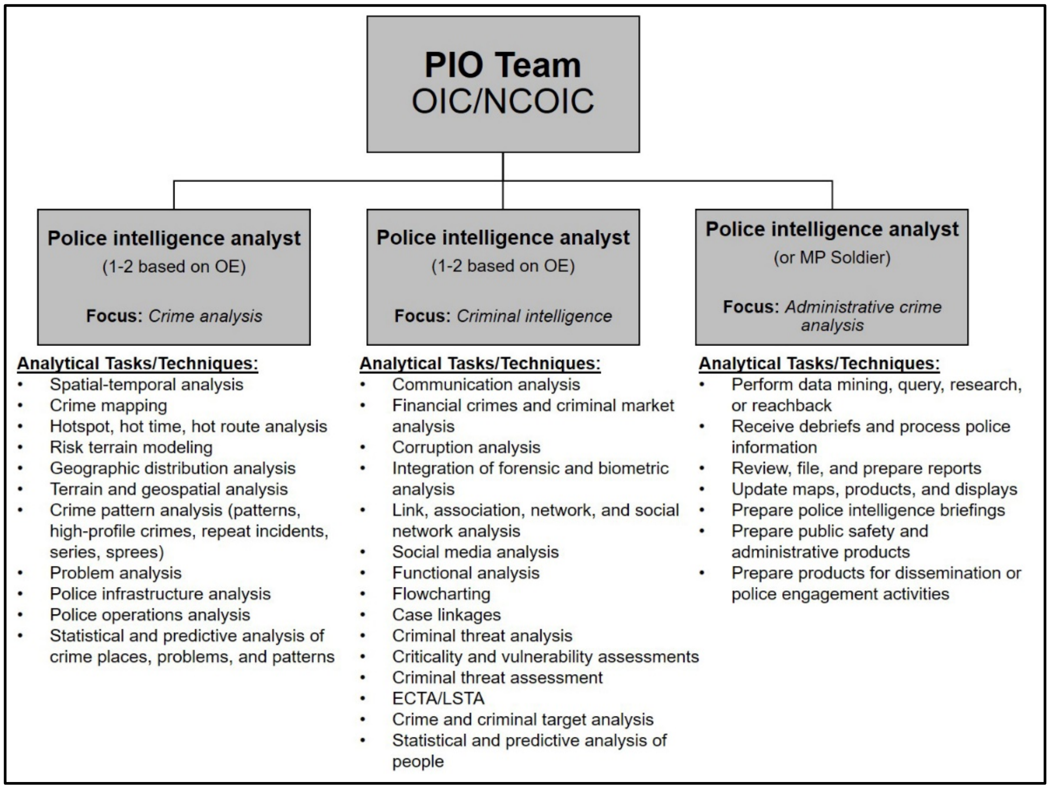

PIO Team
OIC/NCOIC
Police intelligence analyst
(1-2 based on OE)
Focus: Crime analysis
Police intelligence analyst
(1-2 based on OE)
Focus: Criminal intelligence
Police intelligence analyst
(or MP Soldier)
Focus: Administrative crime analysis
Analytical Tasks/Techniques:
• Spatial-temporal analysis
• Crime mapping
• Hotspot, hot time, hot route analysis
• Risk terrain modeling
• Geographic distribution analysis
• Terrain and geospatial analysis
• Crime pattern analysis (patterns, high-profile crimes, repeat incidents, series, sprees)
• Problem analysis
• Police infrastructure analysis
• Police operations analysis
• Statistical and predictive analysis of crime places, problems, and patterns
Analytical Tasks/Techniques:
• Communication analysis
• Financial crimes and criminal market analysis
• Corruption analysis
• Integration of forensic and biometric analysis
• Link, association, network, and social network analysis
• Social media analysis
• Functional analysis
• Flowcharting
• Case linkages
• Criminal threat analysis
• Criticality and vulnerability assessments
• Criminal threat assessment
• ECTA/LSTA
• Crime and criminal target analysis
• Statistical and predictive analysis of people
Analytical Tasks/Techniques:
• Perform data mining, query, research, or reachback
• Receive debriefs and process police information
• Review, file, and prepare reports
• Update maps, products, and displays
• Prepare police intelligence briefings
• Prepare public safety and administrative products
• Prepare products for dissemination or police engagement activities

Figure C-1. Example of a police intelligence operations team organization and tasks

Legend:

ECTA	economic crime threat assessment	OE	operational environment
LSTA	logistics security threat assessment	OIC	officer in charge
MP	military police	PIO	police intelligence operations
NCOIC	noncommissioned officer in charge		

Figure C-1. Example of police intelligence operations team organization and tasks (continued)

Training

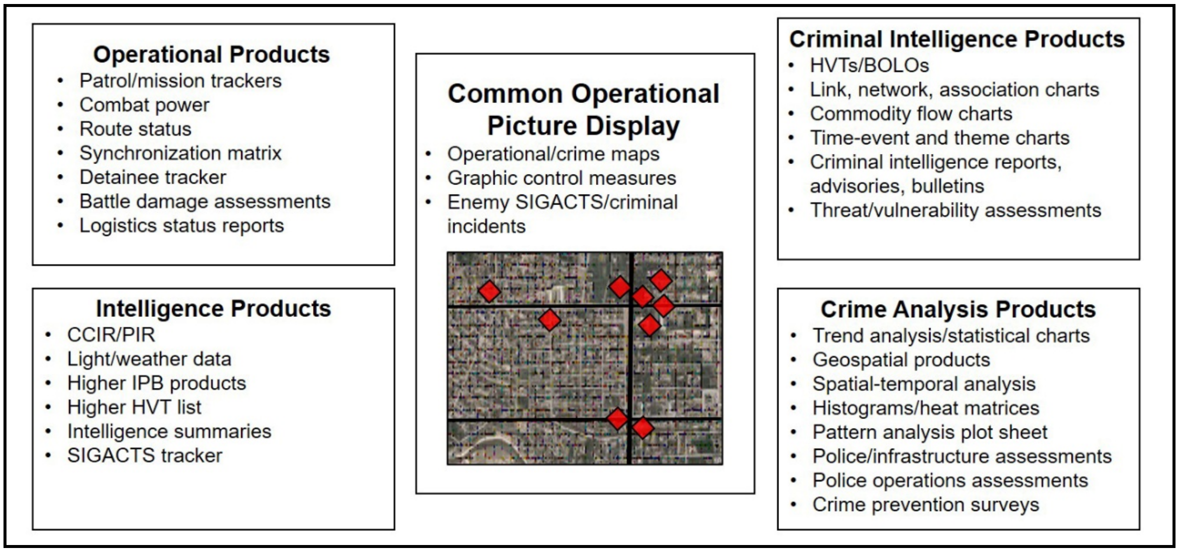
C-7. Training a PIO team begins with the certification of basic criminal and crime analysis skills by attending the Crime and Criminal Intelligence Analyst course administered by USAMPS. This initial training provides police intelligence analysts with the foundational skills upon which to build analytical capability and knowledge of crime and criminality. (See chapter 1 for greater details on selecting and training police intelligence analysts.)

Products

C-8. At the company level, there are several immediate and relevant products for which the PIO team may be responsible for producing or disseminating. These products may include—

- Mission trackers, AO maps, graphical overlays, significant activity trackers, and other relevant operational trackers.
- Criminal intelligence product displays (high value target lists, BOLOs, link diagrams, time-event charts, commodity flow charts).
- Crime analysis product displays (crime or incident maps, POLICE assessments, geospatial analysis products, spatial-temporal analysis, histograms and heat matrices).

C-9. In addition to generating these products, the PIO team must visually display and update these products to support situational awareness and contribute to the commander's common operational picture. Figure C-2 provides an example PIO team product display that depicts some techniques that units have adopted to facilitate common understanding. See chapter 4 and appendix B for additional police intelligence products and examples of what the PIO team can generate and display as part of the common operational picture.



Operational Products
- Patrol/mission trackers
- Combat power
- Route status
- Synchronization matrix
- Detainee tracker
- Battle damage assessments
- Logistics status reports

Intelligence Products
- CCIR/PIR
- Light/weather data
- Higher IPB products
- Higher HVT list
- Intelligence summaries
- SIGACTS tracker

Common Operational Picture Display
- Operational/crime maps
- Graphic control measures
- Enemy SIGACTS/criminal incidents

Criminal Intelligence Products
- HVTs/BOLOs
- Link, network, association charts
- Commodity flow charts
- Time-event and theme charts
- Criminal intelligence reports, advisories, bulletins
- Threat/vulnerability assessments

Crime Analysis Products
- Trend analysis/statistical charts
- Geospatial products
- Spatial-temporal analysis
- Histograms/heat matrices
- Pattern analysis plot sheet
- Police/infrastructure assessments
- Police operations assessments
- Crime prevention surveys

Figure C-2. Potential products for police intelligence operations team displays

Legend:

BOLO	be-on-the-lookout	IPB	intelligence preparation of the battlefield
CCIR	commander's critical information requirement	PIR	priority intelligence requirement
HVT	high value target	SIGACTS	significant activities

Figure C-2. Potential products for police intelligence operations team displays (continued)

Integration

C-10. The military police company does not have formal staffs with functional and integrating cells. Integration of intelligence and operations processes at the company level is the responsibility of the commander. While battalion and higher echelons follow deliberate planning processes, military police at the company level and below follow the troop leading procedures. In time-constrained and highly dynamic tactical situations, the commander must seek to rapidly and seamlessly integrate the efforts of company operations personnel and the PIO team. Figure C-3 demonstrates the integration of military police operations and police intelligence at the company level with PIO team support.

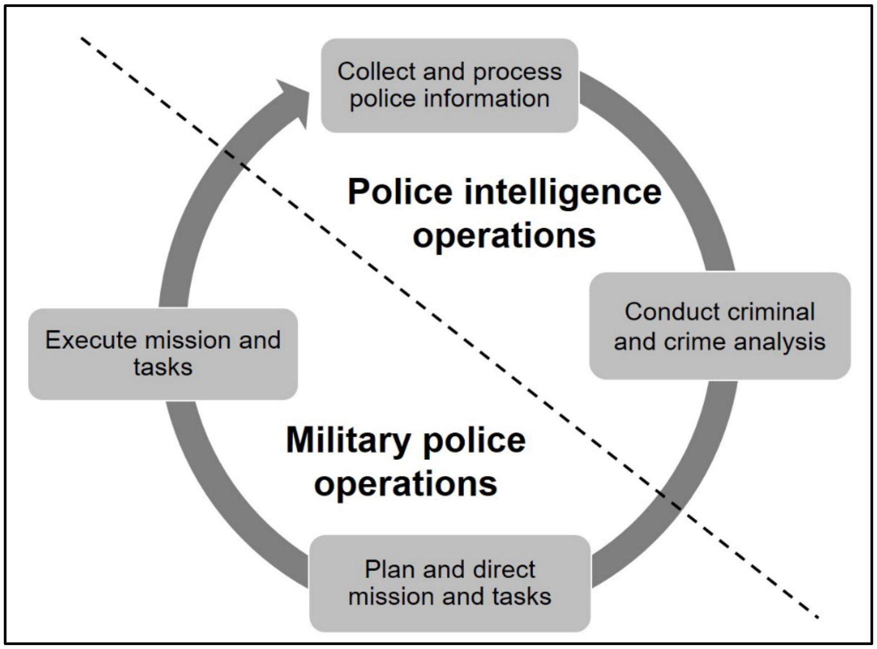

Collect and process police information
Police intelligence operations
Conduct criminal and crime analysis
Execute mission and tasks
Military police operations
Plan and direct mission and tasks

Figure C-3. Integration of police intelligence operations and military police operations

MILITARY POLICE BATTALIONS, BRIGADES, AND GROUPS

C-11. While the military police company focuses PIO teams on directly understanding immediate crime environments and criminal threats, higher level military police organizations are capable of adopting a broader and more strategic approach to understanding and solving crime problems across an area of operations. The military police battalions and brigades, assigned to the S-2 and S-3 sections possess the organic capabilities to create integrated PIO teams or sections. Each battalion or brigade differs in execution based on local circumstances and the crime situation; however, some factors that military police commanders and staffs may consider include—

- Training, certifying, and developing police intelligence analysts (Military Occupational Specialty 31 series) by their attendance at the USAMPS Crime and Criminal Intelligence Analysis Course and by unit-based professional development.
- Creating PIO fusion cells by integrating military intelligence personnel, police intelligence analysts, and military police operational personnel.
- Establishing police intelligence networks with supported maneuver units and intelligence staffs to maintain situational awareness of threats and share police information and police intelligence, as authorized.
- Establishing police intelligence networks with local, state, and federal law enforcement and community agencies to share police information and police intelligence, as authorized.
- Leveraging battalion PIO capabilities to support situational understanding and influence military police operations performed on installations (law enforcement, criminal investigations, antiterrorism and physical security measure implementation).
- Leveraging battalion PIO capabilities to support situational understanding and influence military police operations performed in support of decisive action (physical security, base defense, critical site security, logistics security, area security).

C-12. Military police Criminal Investigation Division battalions and groups focus more exclusively than other military police units on investigating serious crimes and organized criminal activity. Because of this investigative focus, USACIDC organizations often possess more robust PIO capabilities and focus the majority of those PIO capabilities on developing criminal intelligence. In addition to providing organic criminal investigative analysts, USACIDC also bears responsibility for providing advanced technical capabilities to produce unique investigative or police intelligence products. These specialty areas include the Defense Forensic Science Center (and its deployable forensic expeditionary teams) and the 701st Criminal Investigation Division Group, which provides unique investigative capabilities focused on investigating and generating reports on technical areas such as computer crimes, financial crimes, and major procurement fraud. The contributions of military police Criminal Investigation Division battalions and groups and their unique technical reachback capabilities allow USACIDC organizations to provide police information and police intelligence to supported organizations (when authorized) from the tactical through the strategic levels of warfare.

EMPLOYMENT CONSIDERATIONS FOR SUPPORTED ARMY FORCES

C-13. The complexity of operational environments results in a multiplicity of threat actors, threat networks that cross international and regional boundaries and jurisdictions, and connections among different types of legitimate and illicit networks. These networks blur the distinctions of criminal threats, terrorist threats, and nation-state proxies, and of neutral, and friendly actors and networks. This complexity requires police intelligence networks and information sharing that reaches across the levels of warfare to connect criminal networks and actors producing negative effects across the tactical, operational, and strategic levels of warfare. This section considers the support that PIO provides to the Army and its primary organizations across the different levels of warfare.

BRIGADE COMBAT TEAM

C-14. The role that PIO plays is relative to the type of operations and the type of threats occurring at a particular time within the area of operations. While brigade combat teams are engaged in large-scale ground combat in the close area, the commander focuses maneuver forces to regularly defeat enemy forces along the forward edge of the battle area while supporting military police efforts in countering criminal and irregular threats in the support area. Military police combine traditional military intelligence and PIO to defeat irregular threats capable of destroying, disrupting, or otherwise negatively impacting critical mission command, sustainment, and fire support assets operating from support areas. As the bulk of the commander's information collection and analysis capabilities remain focused on the most capable threat (such as enemy maneuver formations and long-range fires capability), PIO provides additional capabilities that focus on criminal and irregular threats. Inattention to irregular threats operating in the support area may cause early culmination due to disrupted lines of communication or it may limit the reach and endurance of maneuver forces due to the requirement of additional forces to secure the support area. As large-scale ground combat concludes and the security situation stabilizes, brigade combat teams begin to conduct stability tasks to consolidate gains. Unaddressed criminal and irregular threats can threaten long-term success by generating disorder, instability, and a sense of distrust and fear in the population that makes consolidation of gains more difficult.

C-15. PIO provides commanders with capabilities that complement military intelligence while maintaining a deliberate focus and attention on criminal and irregular threats throughout all phases of a joint operation. As commanders require the attention of military intelligence to focus on the most capable threats, military police can fulfill an economy of force role by continuing to collect information on crimes, criminal networks, and police and corrections organizations that will eventually be responsible for stability and order in the consolidation area. This complementary capability allows the commander to maintain primary focus on near-term, highly capable threats while also shaping the environment for long-term success by maintaining situational awareness of potential threats to civil security and civil order following large-scale ground combat.

C-16. The most immediate venue for PIO support that complements military intelligence is the provost marshal staff organic to the brigade combat team, who focuses on crime, criminal activity, and HN police and corrections organizations capable of countering criminal and irregular threats. The provost marshal provides technical oversight and advises the commander regarding military police operations and capabilities. (See FM 3-96 for details of provost marshal responsibilities and capabilities within brigade combat teams.) Provost marshal sections are limited by not having dedicated police intelligence analysts assigned; however, they possess the capability to organize and train the ad hoc police intelligence analytical capability by attending the Crime and Criminal Intelligence Analyst course and by training organic personnel to perform PIO tasks. Due to the manning constraints with the provost marshal section, this analytical capability will remain significantly limited and will remain limited in the ability to employ or task military police collection assets. To augment this constraint, brigade combat teams may be supported by a military police company that can perform information collection tasks focused on crime, criminal activities, and police or correction organizations.

C-17. Brigade combat teams are typically supported by a military police company based on the mission and required military police capabilities. (See FM 3-39 for additional information on military police organization; capabilities; and recommended force tailoring, task organization, and employment considerations.) When military police companies are task-organized to support a brigade combat team, they bring with them the ability to collect information during the conduct of military police operations among populations and often provide PIO capabilities in the form of a PIO team that may complement military intelligence sources of information. Military police companies provide police information and police intelligence focused on crime, criminal threats, and HN police and corrections organizations that may be fused with other information and intelligence to drive the operations process and influence the common operational picture.

DIVISION AND CORPS

C-18. Division and corps provost marshals are the primary staff elements responsible for integrating police intelligence into the broader division or corps intelligence process. Provost marshals synchronize their efforts with the G-2 to provide policing, investigative, and detention expertise to help the G-2—

- Interpret criminal intelligence reports and crime analysis products.
- Use fused intelligence and police intelligence to inform division and corps staffs who create protection annexes and antiterrorism and physical security plans.
- Integrate police intelligence products into division or corps working groups, boards, and cells to enhance common understanding and awareness across the staff.
- Provide timely and accurate briefings and updates to the commander and other senior leaders to increase situational awareness and influence decision making.

C-19. Given that the provost marshal section does not have organic police intelligence analysts, the provost marshal often works with supporting military police and the USACIDC organization to provide police intelligence products regarding crime trends and patterns, crime prevention support, detention statistics, and high-profile criminal investigations. Based on the operational environment, some of the organizations and support that the provost marshal may leverage to support the commander's overall situational understanding include the following, based on the operational environment:

- **Supporting installation provost marshal/police station.** At home station, corps and divisions are supported by the installation's Directorate of Emergency Services infrastructure that typically includes an installation provost marshal and/or police station. While the division occupies its home station and/or operates from its home station command post, the supporting police station may support the division or corps provost marshal's efforts to generate police intelligence to improve the commander's situational awareness of criminal threats and influence the decision-making processes aimed at protecting forces, assets, and readiness from the negative impacts of crime (crime within formations disrupting good order and discipline and undermining unit readiness).
- **Supporting military police organizations.** While the division and corps do not have organic military police organizations, they are often supported by military police battalions and brigades at home station and in overseas operational areas. Military police battalions (including detention battalions) and brigades designated in a command or support relationship with the division or corps leverage their PIO capabilities in coordination with the provost marshal to support the commander's situational awareness of crime within friendly formations and integrate police intelligence (as authorized) with the supported unit's operations process through the integrating processes.
- **Supporting criminal investigation division organizations.** USACIDC organizations maintain a more direct and insulated command structure reporting through internal USACIDC channels directly to USACIDC to ensure independent investigative authority. USACIDC elements that are co-located with divisions and corps can provide police intelligence products that support the commander's internal judicial processes and leverage formal criminal intelligence programs to provide understanding of organized criminal elements that threaten the commander's personnel, facilities, and operational readiness.

THEATER ARMY AND ARMY SERVICE COMPONENT COMMAND

C-20. Unified land operations contend with complex operational environments that extend from theater to home station and encompass the physical and virtual lines of communication between. This space is confronted by complex transregional, multidomain, and multifunctional threats that include criminals, criminal networks, criminal organizations, and other irregular threat networks operating across multiple theaters. Criminal and irregular threats not only threaten readiness to deploy promptly from home station into theater to engage in decisive action, but they also threaten the ability to conduct sustained unified land operations for the duration of a joint campaign. (See chapter 1 for different ways in which criminal threats undermine force readiness, discipline and morale, and sustainment capabilities.)

C-21. Because criminal and other irregular threat networks do not confine their operations to narrowly defined areas of operations but instead conduct criminal activities across the levels of warfare, it is crucial that the PIO capability is organized, trained, and leveraged at each echelon. Criminals and other irregular threat networks seek positions of relative advantage over U.S. forces by leveraging neutral or facilitator networks and legitimate business enterprises to conceal their illicit activities. PIO offers commanders at every level of warfare the complementary capabilities necessary to target criminal and other irregular threat networks that operate across the levels of warfare. By unveiling the actors, organizations, links, associations, relationships, communications, commodity flows, and financial flows of threat networks operating with, among, between, or through criminals, PIO offers the commander unique capabilities. These capabilities provide planning, collection, and analysis skills with unique authorities, jurisdictions, and expertise in policing, investigations, and corrections focused on countering crime, criminal activities, criminal networks, and large-scale organized crime. Figure C-4, page C-8, shows how criminal and other networks (terrorist, neutral, facilitators) operate across the levels of warfare.

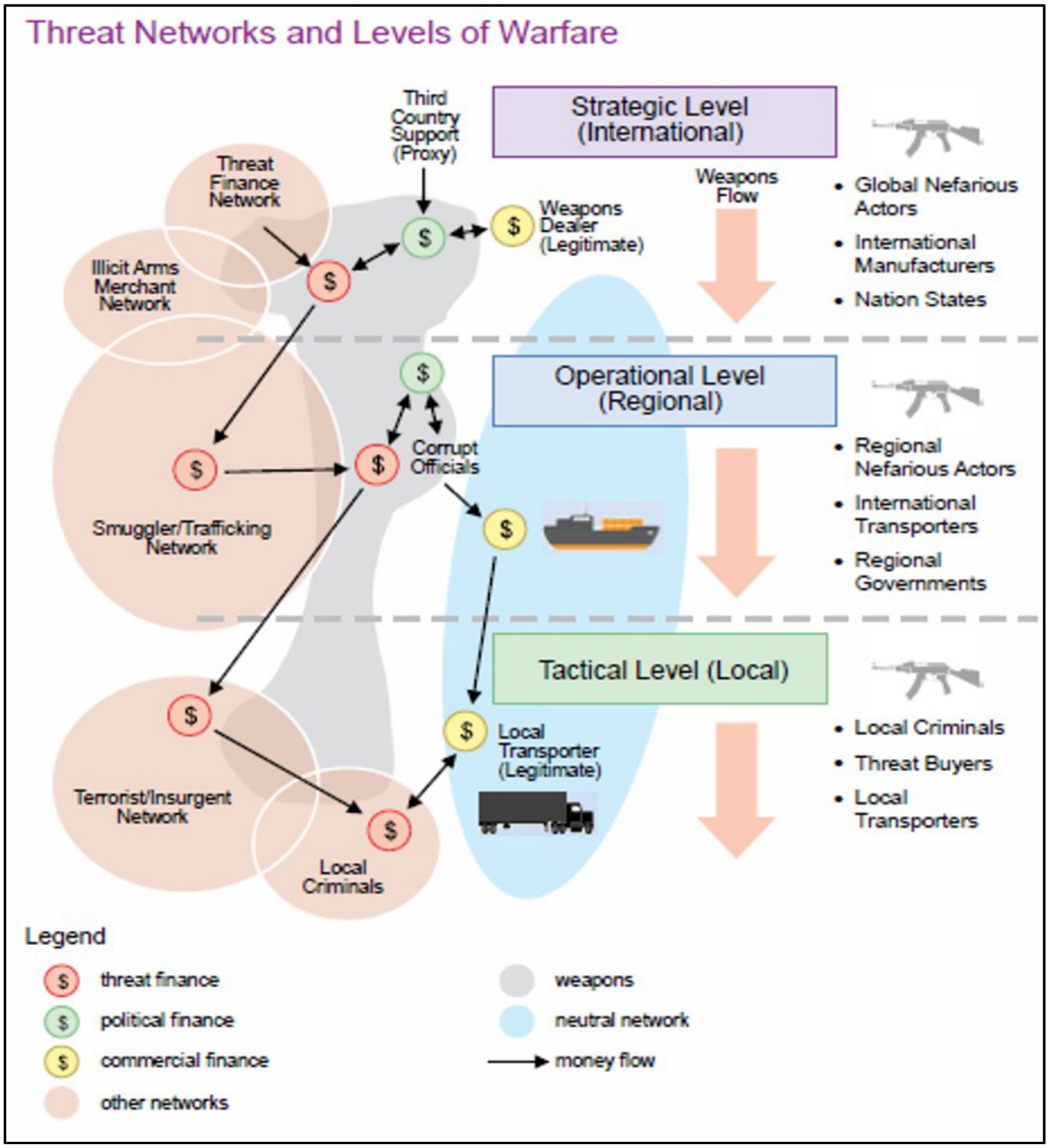

Threat Networks and Levels of Warfare
Third Country Support (Proxy)
Strategic Level (International)
Threat Finance Network
Weapons Flow
Weapons Dealer (Legitimate)
Illicit Arms Merchant Network
Global Nefarious Actors
International Manufacturers
Nation States
Operational Level (Regional)
Corrupt Officials
Regional Nefarious Actors
International Transporters
Regional Governments
Smuggler/Trafficking Network
Tactical Level (Local)
Local Criminals
Threat Buyers
Local Transporters
Local Transporter (Legitimate)
Terrorist/Insurgent Network
Local Criminals
Legend
threat finance
political finance
commercial finance
other networks
weapons
neutral network
money flow

Figure C-4. Threat networks across the levels of warfare

C-22. At the theater level, theater army and Army service component command provost marshals are the central point for coordinating, synchronizing, and integrating police intelligence into the common operational picture and joint planning process. They focus information collection and analysis by military police elements on criminal and irregular threat networks that cross national and regional boundaries. Transnational threat networks defy simple tactical solutions and demand solutions integrated across all levels of warfare. Theater army and Army service component command provost marshals contribute to countering complex threats operating in transregional, multidomain, and multifunctional environments by—

- Contributing to requirements planning by providing or recommending information and intelligence requirements focused on crime, criminal threats, or HN police or corrections organizations.
- Providing police information and police intelligence regarding crime, criminal threats, and police or corrections organizations to support theater security cooperation and theater engagement plans.
- Sharing critical police information and police intelligence with sustainment planners to support efforts (such as criminal threat assessments of prospective sites, recommended physical security measures, and protection prioritization planning for critical sustainment nodes) to set the theater.

- Fusing police intelligence with information and intelligence to influence theater-level force protection planning and decision making.
- Contributing to geographic combatant commander force tailoring decision making to ensure that military police capabilities to counter crime and criminal threats are incorporated into operational planning and requests for forces.
- Coordinating and synchronizing the employment and contributions of PIO across assigned, attached, or supporting military police forces (including military police, detention, and USACIDC organizations).
- Leveraging capabilities from strategic resources (such as the Defense Forensic Science Center) to provide expeditionary forensic analysis capabilities in theater or to coordinate for reachback forensics support.
- Participating in boards, working groups, and cells to integrate and share relevant police intelligence (as authorized) to enhance common understanding and awareness across the staff.
- Providing briefings, updates, and police intelligence products to the commander and other relevant stakeholders to increase situational awareness and influence decision making.

This page intentionally left blank.

Glossary

The glossary lists acronyms and terms with Army or joint definitions. Where Army and joint definitions differ, (Army) precedes the definition. Terms for which ATP 3-39.20 is the proponent are marked with an asterisk (*).

SECTION I – ACRONYMS AND ABBREVIATIONS

ADP	Army doctrine publication
ADRP	Army doctrine reference publication
AFI	Air Force Instruction
AFMAN	Air Force manual
AFTTP	Air Force tactics, techniques, and procedures
ALERTS	Army law enforcement reporting and tracking system
AR	Army regulation
AT	antiterrorism
ATP	Army techniques publication
attn	attention
BOLO	be-on-the-lookout
CCIR	commander's critical information requirement
CFR	Code of Federal Regulations
CGTTP	Coast Guard tactics, techniques, and procedures
CoIST	Company Intelligence Support Team
COMDTINST	Commandant instruction (USCG)
CRIMINT	criminal intelligence
DA	Department of the Army
DC	District of Columbia
DCGS-A	Distributed common ground system-Army
DD	Department of Defense (forms)
DFBA	Defense Forensics and Biometrics Agency
DHS	Department of Homeland Security
DIBRS	Defense Incident-Based Reporting System
DLAR	Defense Logistics Agency Regulation
DNA	deoxyribonucleic acid
DOD	Department of Defense
DODD	Department of Defense directive
DODI	Department of Defense instruction
DODM	Department of Defense manual
DOJ	Department of Justice

DSCA	defense support of civil authorities
EO	executive order
FBI	Federal Bureau of Investigation
FFIR	friendly force information requirement
FM	field manual
G-2	assistant chief of staff, intelligence
G-3	assistant chief of staff, operations
G-9	assistant chief of staff, civil affairs operations
HN	host nation
HUMINT	human intelligence
IPB	intelligence preparation of the battlefield
JP	joint publication
MCO	Marine Corps order
MCRP	Marine Corps reference publication
MCWP	Marine Corps warfighting publication
MO	Missouri
MOE	measure of effectiveness
MOP	measure of performance
MSCoE	Maneuver Support Center of Excellence
MWD	military working dog
NATO	North Atlantic Treaty Organization
No.	number
NTTP	Navy tactics, techniques, and procedures
OPNAV	Office of the Chief of Naval Operations
OPNAVINST	Chief of Naval Operations instruction
PIN	publication identification number
PIO	police intelligence operations
PIR	priority intelligence requirement
POLICE	police and prision structures, organized criminal elements, legal systems, investigations and interviews, crime-conducive conditions, enforcement gaps and mechanisms
RISS	Regional Information Sharing System
S-2	battalion or brigade intelligence staff officer
S-3	battalion or brigade operations staff officer
S-9	battalion or brigade civil affairs operations staff officer
SAR	suspicious activity report
SIPRNET	SECRET Internet Protocol Router Network
SOFA	status-of-forces agreement
STANAG	standardization agreement (NATO)
TC	training circular
U.S.	United States
USACIDC	United States Army-Criminal Investigation Command

USAMPS	United States Army Military Police School
USC	United States Code

SECTION II – TERMS

None.

This page intentionally left blank.

References

All URLs were accessed on 12 February 2019.

REQUIRED PUBLICATIONS

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

DOD Dictionary of Military and Associated Terms. February 2019.

ADP 1-02. *Terms and Military Symbols.* 14 August 2018.

RELATED PUBLICATIONS

These documents contain relevant supplemental information.

28 Code of Federal Regulations part 23. *Criminal Intelligence Systems Operating Policies.* 1998. <https://it.ojp.gov/documents/28CFR_Part_23.PDF>.

10 USC. *Armed Forces.* 7 January 2011. <https://www.govinfo.gov/content/pkg/USCODE-2017-title10/pdf/USCODE-2017-title10.pdf>.

18 USC. *Crimes and Criminal Procedure.* 25 June 1948. <http://uscode.house.gov/view.xhtml?req=USC+18&f=treesort&fq=true&num=4109&hl=true&edition=prelim&granuleId=USC-prelim-title18-front>.

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>.

22 USC. *Foreign Relations and Intercourse.* 2010 Edition. <https://www.gpo.gov/fdsys/pkg/USCODE-2010-title22/html/USCODE-2010-title22.htm>.

32 USC. *National Guard.* 10 August 1956. <https://www.govinfo.gov/content/pkg/USCODE-2017-title32/pdf/USCODE-2017-title32.pdf>.

50 USC. *Servicemembers Civil Relief.* 1 February 2010. <https://www.gpo.gov/fdsys/granule/USCODE-2009-title50/USCODE-2009-title50-app-serviceme>.

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>.

Geneva Conventions of 12 August 1949. <http://www.icrc.org/eng/resources/documents/publication/p0173.htm>.

Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field. Geneva, 12 August 1949.

Convention (II) for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea. Geneva, 12 August 1949.

Convention (III) relative to the Treatment of Prisoners of War. Geneva, 12 August 1949.

Convention (IV) relative to the Protection of Civilian Persons in Time of War. Geneva, 12 August 1949.

Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflict (Protocol I), 8 June 1977.

Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of Non-International Armed Conflicts (Protocol II), 8 June 1977.

JOINT PUBLICATIONS

Most joint publications are available online at <https://www.jcs.mil/Doctrine/>.

JP 1-04. *Legal Support to Military Operations*. 2 August 2016.

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

JP 2-01. *Joint and National Intelligence Support to Military Operations*. 5 July 2017.

JP 2-01.3. *Joint Intelligence Preparation of the Operational Environment*. 21 May 2014.

JP 2-03. *Geospatial Intelligence in Joint Operations*. 5 July 2017.

JP 3-0. *Joint Operations.* 17 January 2017.

JP 3-07. *Stability*. 3 August 2016.

JP 3-07.2. *Antiterrorism*. 14 March 2014.

JP 3-08. *Interorganizational Cooperation*. 12 October 2016.

JP 3-13.3. *Operations Security*. 6 January 2016.

JP 3-24. *Counterinsurgency.* 25 April 2018.

JP 3-25. *Countering Threat Networks*. 21 December 2016.

JP 3-28. *Defense Support of Civil Authorities*. 29 October 2018.

JP 3-30. *Command and Control of Joint Air Operations*. 10 February 2014.

ARMY PUBLICATIONS

Most Army publications are available online at <https://armypubs.army.mil>.

ADP 2-0. *Intelligence.* 4 September 2018.

ADP 3-28. *Defense Support of Civil Authorities*. 11 February 2019.

ADP 3-37. *Protection*. 11 December 2018.

ADP 3-90. *Offense and Defense*. 13 August 2018.

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

ADRP 3-0. *Operations*. 6 October 2017.

ADRP 3-07. *Stability*. 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.* 11 December 2017.

AR 25-22. *The Army Privacy Program*. 22 December 2016.

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

AR 27-10. *Military Justice.* 11 May 2016.

AR 190-13. *The Army Physical Security Program*. 25 February 2011.

AR 190-14. *Carrying of Firearms and Use of Force for Law Enforcement and Security Duties*. 12 March 1993.

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

AR 190-45. *Law Enforcement Reporting.* 27 September 2016.

AR 190-47. *The Army Corrections System*. 15 June 2006.

AR 190-53. *Interception of Wire and Oral Communications for Law Enforcement Purposes.* 16 July 2018.

AR 190-58. *Designation and Protection of High Risk Personnel.* 25 February 2018.

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

AR 195-6. *Department of the Army Polygraph Activities*. 21 April 2016.

AR 380-5. *Department of the Army Information Security Program*. 29 September 2000.

AR 380-10. *Foreign Disclosure and Contacts With Foreign Representatives.* 14 July 2015.

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.* 1 June 2016.

AR 525-2. *The Army Protection Program*. 8 December 2014.

AR 525-13. *Antiterrorism.* 17 February 2017.

ATP 2-01. *Plan Requirements and Assess Collection*. 19 August 2014.

ATP 2-01.3. *Intelligence Preparation of the Battlefield.* 1 March 2019.

ATP 2-22.82. *Biometrics-Enabled Intelligence.* 2 November 2015.

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

ATP 2-91.8. *Techniques for Document and Media Exploitation.* 5 May 2015.

ATP 3-07.5. *Stability Techniques*. 31 August 2012.

ATP 3-34.80. *Geospatial Engineering.* 22 February 2017.

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

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

ATP 3-39.11. *Military Police Special Reaction Teams*. 26 November 2013.

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

ATP 3-39.30. *Security and Mobility Support*. 30 October 2014.

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

ATP 3-39.33. *Civil Disturbance*. 21 April 2014.

ATP 3-39.34. *Military Working Dogs*. 30 January 2015.

ATP 3-39.35. *Protective Services*. 31 May 2013.

ATP 3-55.4. *Techniques for Information Collection During Operations Among Populations*. 5 April 2016.

ATP 3-60. *Targeting.* 7 May 2015.

ATP 3-90.15. *Site Exploitation*. 28 July 2015.

ATP 5-0.1. *Army Design Methodology.* 1 July 2015.

ATP 5-0.6. *Network Engagement*. 19 June 2017.

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

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

FM 3-39. *Military Police Operations.* 9 April 2019.

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

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

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

FM 3-90-1. *Offense and Defense Volume 1.* 22 March 2013.

FM 3-90-2. *Reconnaissance, Security, and Tactical Enabling Tasks Volume 2*. 22 March 2013.

FM 3-96. *Brigade Combat Team*. 8 October 2015.

FM 4-30. *Ordnance Operations*. 1 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 2-91.4. *Intelligence Support to Urban Operations*. 23 December 2015.

TC 7-100. *Hybrid Threat*. 26 November 2010.

TC 19-210. *Access Control Handbook*. 4 October 2004.

Department of Defense Publications

Most DOD publications are available online at <https://www.esd.whs.mil/dd/>.

DODD 2310.01E. *DOD Detainee Program*. 19 August 2014.

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

DODI 5505.17. *Collection, Maintenance, Use, and Dissemination of Personally Identifiable Information and Law Enforcement Information by DOD Law Enforcement Activities*. 19 December 2012.

DODI 5525.18. *Law Enforcement Criminal Intelligence (CRIMINT) in DOD*. 18 October 2013.

DODI 7730.47. *Defense Incident-Based Reporting System (DIBRS).* 23 January 2014.

Multi-service Publication

AR 190-5/OPNAV 11200.5D/AFI 31-218(I)/MCO 5110.1D/ DLAR 5720.1. *Military Police Motor Vehicle Traffic Supervision.* 22 May 2006.

AR 190-24/OPNAVINST 1620.2A/AFI 31-213/MCO 1620.2D/COMDTINST 1620.1E. *Armed Forces Disciplinary Control Boards and Off-Installation Liaison and Operations*. 27 July 2006.

ATP 2-22.85/MCRP 3-33.1J/NTTP 3-07.16/AFTTP 3-2.85/CGTTP 3-93.6. *Multi-Service Tactics, Techniques, and Procedures for Tactical Employment of Biometrics in Support of Operations*. 6 May 2016.

ATP 3-90.4/MCWP 3-17.8. *Combined Arms Mobility.* 8 March 2016.

ATP 4-10/MCRP 4-11H/NTTP 4-09.1/AFMAN 10-409-O. *Multi-Service Tactics, Techniques, and Procedures for Operational Contract Support*. 18 February 2016.

Other Publications

Carter, David L., *Law Enforcement Intelligence: A Guide for State, Local, and Tribal Law Enforcement Agencies (2d Edition).* Michigan State University. May 2009. <https://it.ojp.gov/documents/d/e050919201-IntelGuide_web.pdf>.

Department of Justice. *National Criminal Intelligence Sharing Plan.* Version 2.0. October 2013. <https://it.ojp.gov/1180>.

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

Manual for Courts-Martial United States, 2019 Edition. Web site <https://jsc.defense.gov/Portals/99/Documents/2019%20MCM%20(Final)%20(20190108).pdf?ver=2019-01-11-115724-610>.

National Disclosure Policy. <http://www.discs.dsca.mil/documents/ips/Chapter3_04052010.pdf>.

National Strategy for Information Sharing: Successes and Challenges in Improving Terrorism-Related Information Sharing. October 2007. <https://nsi.ncirc.gov/documents/National_Strategy_for_Information_Sharing.pdf>.

United Nations. *World Urbanization Prospects* 2018. <https://esa.un.org/unpd/wup/cd-rom/>.

United States Code of Military Justice Web site <http://www.ucmj.us/>.

United States Agency for International Development. *Anticorruption Assessment Handbook.* <http://pdf.usaid.gov/pdf_docs/pa00jp37.pdf >.

WEB SITES

Army Publishing Directorate Web site. <https://armypubs.army.mil/>.

Department of Justice OneDOJ Web site. <http://www.justice.gov/jmd/pia/onedoj-pia.pdf>.

Federal Bureau of Investigations Web site. <https://www.fbi.gov/>.

Justice Information Sharing Web site. <http://it.ojp.gov/>.

Law Enforcement Information Sharing Initiative Web site. <https://www.ice.gov/le-information-sharing>.

National Crime Information Center database Web site. <https://www.fbi.gov/services/cjis/ncic>.

National Information Exchange Model Web site. <https://www.niem.gov/Pages/default.aspx>.

Regional Information Sharing Systems (RISS) Web site. <https://www.riss.net/>.

U.S. Army Criminal Investigation Command Web site. <http://www.cid.army.mil/>.

PRESCRIBED FORMS

This section contains no entries.

REFERENCED FORMS

Unless otherwise indicated, DA forms are available on the Army Publishing Directorate Web site at <https://armypubs.army.mil/>. DD forms are available on the Office of the Secretary of Defense Web site at <https://www.esd.whs.mil/dd/ >. Printed forms are available through normal forms supply channels.

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

DA Form 3881. *Rights Warning Procedure/Waiver Certificate.*

DD Form 1408. *Armed Forces Traffic Ticket.*

RECOMMENDED READINGS

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>.

ADRP 1. *The Army Profession.* 14 June 2015.

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

Center for Army Lessons Learned. Handbook Number 13-09. *CoIST Company Intelligence Support Team.*18 July 2013. <https://call2.army.mil/toc.aspx?document=7101>.

Clarke, Ronald and Eck, John. *Crime Analysis for Problem Solvers in 60 Small Steps.* Department of Justice. 8 August 2005. <http://www.popcenter.org/learning/60steps/>.

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/ric.php?page=detail&id=COPS-W0418>.

DHS/DOJ. Global Justice Information Sharing Initiative. *DHS/DOJ Fusion Process: Technical Assistance Program and Services.* 7th Edition. May 2013. <https://www.hsdl.org/?view&did=776455>.

DOD 5240.1-R. *Procedures Governing the Activities of DOD Intelligence Components that affect United States Persons [Procedures 11-13 remain].* 7 December 1982 <*http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodm/524001r.pdf*>.

DODD 2311.01E. *DOD Law of War Program.* 9 May 2006.

DODM 5240.01. *Procedures Governing the Conduct of DOD Intelligence Activities.* 8 August 2016. <https://dodsioo.defense.gov/Portals/46/DoDM%20%205240.01.pdf?ver=2016-08-11-184834-887>.

DOJ. Global Justice Information Sharing Initiative. *Findings and Recommendations of the Suspicious Activity Report (SAR) Support and Implementation Project.* October 2008. <https://nsi.ncirc.gov/documents/SAR_Report_January_2009.pdf >.

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>.

DOJ. Global Justice Information Sharing Initiative. *Law Enforcement Analytic Standards*. 1 May 2012. <https://it.ojp.gov/gist/91/Law-Enforcement-Analytic-Standards>.

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>.

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

Felson, Marcus and Eckert, Mary. *Crime and Everyday Life (5th Edition)*. 2016.

FM 3-0. *Operations.* 6 October 2017.

FM 7-0. *Train to Win in a Complex World.* 5 October 2016.

Gottlieb, Steven. *Crime Analysis: From First Report to Final Arrest.* 1994.

Lersch, Kim M. *Space, Time, and Crime (2d Edition).* 2007.

The National Security Act of 1947. <https://history.state.gov/milestones/1945-1952/national-security-act>.

STANAG 2226 (ATP – 3.7.2). *NATO Military Police Guidance and Procedures.*

STANAG 2296 (AJP 3.2.3.3). *Allied Joint Doctrine for Military Police.*

Weisburd, David. *Place Matters-Criminology for the Twenty-First Century.* April 2016.

Index

Entries are by paragraph number.

This page intentionally left blank.

ATP 3-39.20

13 May 2019

By Order of the Secretary of the Army:

MARK A. MILLEY
General, United States Army
Chief of Staff

Official:

Kathleen S. Miller

KATHLEEN S. MILLER
Administrative Assistant
to the Secretary of the Army
1912680

DISTRIBUTION:
Distributed in electronic media only(EMO).

PIN: 105125-000