From AFIO's **The Intelligencer**
Journal of U.S. Intelligence Studies
Volume 21 • Number 1 • $15 single copy price **Winter 2014-15**

© 2015 AFIO - Association of Former Intelligence Officers, All Rights Reserved

Association of Former Intelligence Officers
7700 Leesburg Pike Ste 324
Falls Church, Virginia 22043
Web: **www.afio.com**, E-mail: **afio@afio.com**

Guide to the Study of Intelligence

Law Enforcement Intelligence

by Arthur E. Gerringer and Josh Bart

American society with its strong sense of civil liberties has long held in disdain the conduct of intelligence operations within the United States against its own citizens. Yet the intelligence gathered by law enforcement agencies has played an important role in preventing criminal activity and acts of terrorism. Intelligence gathered by law enforcement is often overlooked by those who narrowly view the Intelligence Community as just the military and those three letter agencies, such as the CIA or NSA. While the FBI and Drug Enforcement Administration (DEA) are listed as Intelligence Community (IC) members, a comprehensive list of contributing agencies of intelligence must also include the Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF) within the Justice Department; Immigration and Customs Enforcement (ICE), Secret Service (USSS), Customs and Border Protection (CPB), all within the Department of Homeland Security; and all state and local law enforcement agencies. In actuality, the state and local agencies often are greater producers of tactical or operational intelligence than federal agencies, due to their familiarity with their areas of jurisdiction and life on the street.

The goals of law enforcement intelligence are to save lives, protect property, and preempt crime. The concept of "intelligence-led policing" stresses the use of intelligence to effectively and efficiently allocate policing resources. Additionally, law enforcement agencies regularly use their intelligence to support investigations and contribute to prosecutions. The critical difference between investigations and intelligence is that investigations are retrospective and focus on an event that has occurred, while intelligence is prospective and attempts to predict likely future events. Investigations produce evidence that can be used for prosecutions. Intelligence produces judgments based on an incomplete picture of the future. Evidence from investigations must be made public under our system of jurisprudence. To do so with intelligence would negate its value.

The intelligence cycle for law enforcement is a fluid one, but not dissimilar to the traditional cycle of the national intelligence community. The first step is to determine the requirements and direction for the collection process. As collected information is gathered from a wide array of open, human, and technical sources, it must be collated and processed before exploitation takes place. Certain information must be translated from foreign languages, and all information must be evaluated for reliability and relevancy. Once this raw intelligence is deemed appropriate, the analyst evaluates and interprets its significance and disseminates it to authorized consumers. Feedback occurs throughout the entire process and involves revising requirements or guidelines based on policy-makers' decisions as to how to proceed using the processed intelligence.

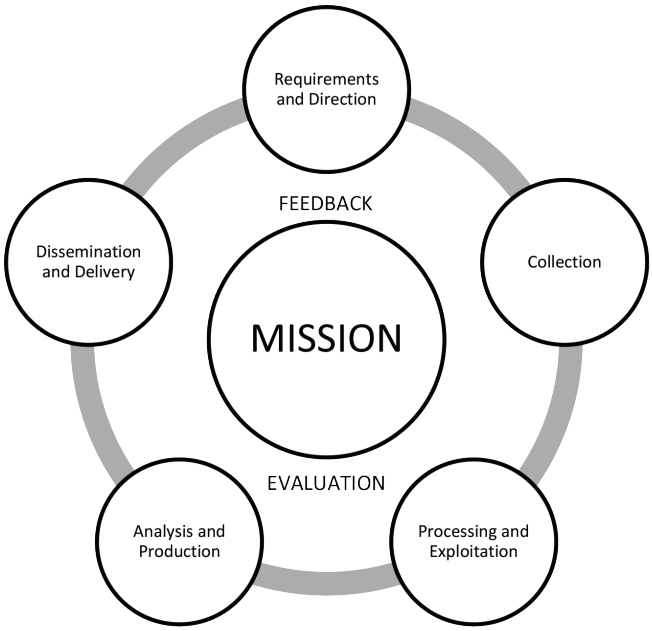
Law enforcement agencies employ similar collection methods to the national intelligence community, but they vary in scale and scope and terminology. For example, one term used by civilian and US Army law enforcement officials is "criminal intelligence" (CRIMINT). CRIMINT describes longer-term crime data and behaviors of organizations and groups. Open sources for law enforcement intelligence include publicly available information as well as data, such as travel records and financial statements, that may require a warrant to obtain. The use of witnesses, undercover agents, confidential informants, surveillance, and dumpster diving (picking through discarded trash) is akin to HUMINT. Wiretaps, call traces, forensics, surveillance photos and closed circuit TV video are means of technical law enforcement intelligence collection.

Regardless of their differing nomenclatures, each of these types of intelligence provides valuable insights and indicators of potential future criminal activities. The sharing of law enforcement intelligence historically has been limited. Assessments of intelligence failures have revealed that important indicators were often available but overlooked or not used.[1]

To be effective, law enforcement intelligence analysts must be accurate, timely, and predictive. Analysts must be aware of what is known, what is unknown or

1. One indicator of potential terrorist activity that was not appreciated until after the attacks of 9/11 was the enrollment of certain individuals in flight training schools. This was cited in the 9/11 *Commission Report*.

unclear, and what is presumed. Understanding this assists in both the feedback and the planning stages of the intelligence process. During the analytical phase of the cycle, analysts employ a number of different methods and models in order to predict both possible and probable results. These techniques range from comparing current situations with relevant historical events, to designing probability matrices and timelines, and development of social network models. There are a number of computer modeling and analytical software that are used such as Analyst's Notebook, Orion, and Black Oak. Additionally, in many cases, the use of "red-teaming" and "devil's advocacy analysis" is highly beneficial when attempting to analyze the target organization. Of importance in an often "politically correct" environment is that intelligence analysts must (1) be willing to make judgments and not rely solely on computer produced data and (2) be willing to stick their professional necks out and take a chance on a position that may not be popular. In recent years emphasis has been placed on the professional training of law enforcement intelligence analysts. According to the International Association of Law Enforcement Intelligence Analysts (IALEIA) and the Department of Justice it is preferred that law enforcement intelligence analysts have a four-year college degree or a minimum of five years' experience.[2] Further, it is important for analysts to continue their educations through additional training throughout their careers.



Prior to September 11, 2001, law enforcement agencies typically consisted of units designed to deal with major narcotics trafficking, gangs, organized crime, and, occasionally, dignitary protection. In a post-9/11 America, however, many law enforcement agencies now have terrorism divisions, especially those operating within large metropolitan areas, particularly Houston, Los Angeles and New York. Many have their own specialized Counter-Terrorism and Criminal Intelligence Bureaus.

Over the past decade cooperation and coordination between law enforcement and the intelligence community has been emphasized and resulted in the expansion of task-oriented units such as the Joint Terrorism Task Forces (JTTF) led by the Department of Justice and the FBI. JTTF units "are small cells of highly trained, locally based, passionately committed investigators, analysts, linguists, SWAT experts, and other specialists from dozens of US law enforcement and intelligence agencies."[3] The first JTTF was an FBI and NYPD cooperative initiative created in 1980. In 2002, the National JTTF was established to coordinate communication with localized JTTFs. There are currently over 100 JTTFs across the country. Another example of a multi-agency intelligence task force is the High Intensity Drug Trafficking Area (HIDTA) fusion centers. HIDTA fusion centers house federal, state, and local law enforcement intelligence personnel to coordinate anti-drug trafficking efforts.

In addition to JTTFs, regional and local joint fusion centers serve as terrorism prevention and emergency response centers. These were created through a joint project by the Department of Justice and the Department of Homeland Security between 2003 and 2007. These fusion centers are funded by state and local police departments, and many house federal Homeland Security analysts. Their charters differ depending upon the jurisdiction, and some address all types of criminal activity, not just terrorism.

In 2003, The National Criminal Intelligence Sharing Plan (NCISP) was produced to serve as a model for local, state, tribal, and federal law enforcement agencies to enhance sharing of critical information. According to the Institute for Intergovernmental Research, the NCISP proposes a "nationwide commu-

2. *Law Enforcement Analytic Standards* handbook.

3. Department of Justice.

nications capability that will link together all levels of law enforcement personnel, including officers on the streets, intelligence analysts, unit commanders, and police executives for the purpose of sharing critical data." There is a plethora of intelligence – and investigatory-related data bases and communications systems used for sharing data. For sensitive intelligence the Homeland Security Information Network (HSIN) is a principal mode for pushing national intelligence to law enforcement agencies and for sharing sensitive data between agencies.[4]

Despite these sharing initiatives, law enforcement intelligence agencies and divisions are not without limitations. In many instances, the budgets for law enforcement agencies are too constrained to allow for sufficient intelligence capabilities. Law enforcement intelligence units often cannot analyze collected data because of their limited personnel. Differing federal, state, and local laws and overlapping jurisdictions can inhibit the effective sharing of law enforcement intelligence between the tiers of agencies. Furthermore, as often depicted in popular television shows, organizational and personal jealousies can have negative effects and will never be completely expunged. The inherent secrecy that cloaks intelligence also fosters suspicions of improper behavior by law enforcement and infringements of civil liberties. The political reaction to even perceived violations often constrains law enforcement intelligence activities.

Despite limitations that exist, law enforcement's use of intelligence is expanding. Intelligence has become a major focus for some traditional law enforcement agencies, such as the FBI, and is a vital tool for urban police departments, such as the NYPD that are targets of international terrorists. The walls to sharing vital law enforcement intelligence are crumbling, but progress is often constrained by legal issues. Nonetheless, intelligence-led policing will remain as a central strategy for law enforcement.

Readings for Instructors

Those students who take an interest in this subject should educate themselves in all aspects of the field — the criminal mind; modus operandi of criminals; the planning, training, financing and support functions for criminal organizations; and the available tools and resources that allow law enforcement intelligence personnel to delve deeply into criminals' psychological and cultural makeup. More and more academic institutions are offering criminal justice degrees and certificates, but a caution must be exercisd against relying solely on the output of technology. Technology only manipulates what humans input. Law enforcement intelligence analysts must learn to think critically to apply effectively the intelligence they produce in support of the law enforcement mission.

The following are recommended readings for instructors and interested students:

David L. Carter (1990). *Law Enforcement Intelligence Operations: An Overview of Concepts, Issues and Terms*. Tallahassee, FL: SMC Sciences Inc.

David L. Carter (2009). *Law enforcement intelligence: A guide for state, local, and tribal law enforcement agencies* (2nd ed.). Washington, DC: U.S. Department of Justice, Office of Community Oriented Policing Services. Retrieved from https://intellprogram.msu.edu/resources/publications.php.

Don R. Harris et al. (1971). *The Basic Elements of Intelligence Revised*. US Department of Justice, Law Enforcement Assistance Administration.

International Association of Chiefs of Police (1998, updated in 2003). *Criminal Intelligence: Concepts and Issues Paper*, IACP National Law Enforcement Policy Center.

Mike Maguire, "Policing by risks and targets: Some dimensions and implications of intelligence-led crime control," in *Policy and Society: An International Journal of Research and Policy*, Volume 9, Issue 4, 2000.

Marilyn B. Peterson (1994). *Applications in Criminal Analysis: A Sourcebook*. Westport, CT: Greenwood Press.

US Department of Justice (2009). *Intelligence-Led Policing: The New Intelligence Architecture*. Washington, DC, Bureau of Justice Assistance.

Richard Wright, Bob Morehouse, Marilyn B. Peterson, and Lisa Palmieri (eds) (2011). *Criminal Intelligence for the 21st Century*. Association of Law Enforcement Intelligence Units and the International Association of Law Enforcement Intelligence Analysts (IALEIA).

Joshua Bart is an operations research specialist and intelligence analyst for The Inter-Sec Group in San Antonio, Texas. He is an alumnus of The University of Texas at San Antonio (UTSA) where he studied Political Science, International Studies, and Global Analysis. Mr. Bart is pursuing a Master's certification in Geographic Information Systems from UTSA.

Arthur E Gerringer is the President/CEO of The Inter-Sec Group, which provides anti-terrorism, intelligence, security and training services to the US Government and military. Mr. Gerringer is a 40-year veteran of the military intelligence and law enforcement communities. He has been an intelligence analyst, counterintelligence agent, interrogator, physical security specialist, college adjunct professor, investigator, and trainer. Mr. Gerringer holds numerous certifications and three college degrees.

4. See *http://www.dhs.gov/files/programs/gc_1156888108137.shtm* for a description of HSIN.