Intelligence Led Policing: Getting Started

Professionalizing Analysis Worldwide

Table of Contents

Published by the International Association of Law Enforcement Intelligence Analysts, Inc. (IALEIA)
under title "Guidelines for Starting an Analytic Unit", printed September, 1997; Second Edition "Starting An Analytic Unit for Intelligence Led Policing," printed July 2001.
Third edition, "Intelligence Led Policing: Getting Started," published January 2005.

IALEIA, P.O. Box 13857, Richmond, VA 23225.

Original Booklet Committee
Marilyn B. Peterson, Intelligence Management Specialist, New Jersey Division of Criminal Justice
Robert C. Fahlman, Assistant Director, Interpol - ICPO
Simon Robertson, Head of Analysis, Europol - Drugs Unit
Leo M. Jacques, Ph.D., Criminal Analyst Supervisor, Arizona Department of Public Safety
Danny L. Taylor, Jr., Information Services Supervisor, National White Collar Crime Center

2nd edition Committee
Marilyn B. Peterson, CCA, New Jersey Division of Criminal Justice
Leo M. Jacques, Ph.D., CCA, Arizona Department of Public Safety
Ritchie A. Martinez, CCA, Arizona Department of Public Safety

3rd edition Committee
Marilyn B. Peterson, CCA, New Jersey Division of Criminal Justice
Lisa Palmiei, CCA, IALEIA President, Massachusetts State Police
Leo Jacques, Ph.D., CCA, Arizona Department of Public Safety

Introduction

Intelligence led policing (ILP) is the model which brings intelligence and analysis to the forefront of police operations. It allows for the efficient use of resources, the production of workable strategies and the successful completion of investigations and prosecutions. Originating in the UK, it has translated into the *National Intelligence Model* there and into the *National Criminal Intelligence Sharing Plan* in the U.S. Canada has also been working to develop an intelligence strategy.

A lesson learned by the U.S. on September 11, 2001 was that intelligence is integral to preventing terrorist attacks. Since then, more and more U.S. police agencies have adopted the intelligence led model, and intelligence units have been established worldwide. Intelligence led policing uses analysis in a pro-active way to effectively target criminal groups and activities. This front-end application allows agencies to assess the needs and resources of the organization and

jurisdiction, placing viable alternatives in the hands of decision-makers. Strategic targeting allows the agency to prioritize cases with the highest probability of success.

This booklet is designed to assist the development of intelligence led policing in police departments, sheriffs' offices, prosecutors' offices and other criminal justice agencies. It can also provide guidance to intelligence efforts in the private sector.

Hopefully, through this, and similar writings, more organizations will experience, first-hand, the benefits of intelligence and analysis.

Mission, Goals and Objectives

The mission of an intelligence unit is to provide quality intelligence products in support of the agency's mission. Thus, the work that is performed reflects the priorities and goals of the specific agency or organization.

As an example, the mission of the Criminal Analysis Branch of the Royal Canadian Mounted Police is:

> *To provide an effective and efficient intelligence capability in support of the overall RCMP Criminal Intelligence Directorate's mission to provide a national program for the management of criminal information and intelligence which will permit the RCMP to detect and prevent crime having an organized, serious or national security dimension in Canada, or internationally as it affects Canada.*

Based on the mission, goals should be established for the unit. They can include:

- To support the intelligence function through the analysis of data gathered and the completion of assessments on crime groups which are prioritized as threats to the jurisdiction;
- To support investigations through the provision of analytic services and products for cases designated as a priority;
- To support overall operations of the department by providing focus to the assignment of tasks; and
- To support strategic planning by providing analyses of past and current crime trends to target future crime.

Objectives would then be developed based on those goals that would quantify or clarify the number and types of cases or studies that would be supported for the year by the unit.

As former Chief Louis R. Anemone of the New York City Police Department noted, "Accurate and timely analysis is the most critical building block in crime prevention and crime fighting strategies."

Role in Department

Within the ILP model, the role of the intelligence unit is to produce intelligence–that is, ***analyzed*** data–for decision-makers so that appropriate criminal activity is targeted and law enforcement efforts focus on established priorities.

Analysis is the heart of the intelligence process. Without analysis to derive meaning from the data, the information does not become intelligence. Intelligence summaries and reports are products of analysis. Both tactical and strategic intelligence studies are most effective when completed by persons trained in analytic techniques.

Analysis is also used throughout the investigative process. Investigative plans are best prepared with analytic input. The data that are collected through search warrants, subpoenas, surveillance, interviews, Internet searches and other investigative means must be organized and analyzed. The

proofs necessary to prosecute a defendant are gathered, summarized and organized by analysts. Analysts also provide courtroom graphics and can give testimony in trials.

Analysis and intelligence can support the operations of the law enforcement agency and should be viewed as "mainstream' within the department. Effective intelligence operations receive raw data from all sections of the department and provide knowledge products in return.

Key to the thorough use of intelligence within the department are two factors. First, the support of top-level management is imperative. Second, intelligence will be better understood and accepted throughout the department if the other members of the organization-wide staff are provided with a seminar highlighting its benefits.

Staffing

A 'typical' intelligence unit might have a manager or supervisor, three to 12 intelligence officers and a similar number of analysts. This formalized intelligence unit might be found in agencies or organizations with 75 or more sworn officers. In a smaller agency, analysts could be in a unit without designated collectors while investigators in other units provide them with data. In even smaller agencies, one or two individuals, sworn or non-sworn, could be used to perform rudimentary analysis and serve as intelligence liaison personnel. In the larger agencies, one possible ratio of analysts to investigators would be one analyst to 12 investigators or detectives. In agencies specializing in sophisticated crime, the ratio could be one analyst to five investigators.

Ideally, the intelligence unit manager or supervisor should be an experienced intelligence professional. In agencies which require the unit manager be sworn and in rotation through the unit, this may not be possible. In this case, there should be an experienced lead analyst to manage the day-to-day operations of the analysts.

Intelligence personnel may have a variety of work experience, training and education. In the U.S.,where many police agencies require their recruits to be college graduates; analysts generally have four-year or post-graduate degrees. In other countries, law enforcement experience is more the norm than are advanced degrees.

The more experienced intelligence personnel would best be used to support the strategic targeting and prioritization function while the less experienced personnel can become more seasoned while involved in case support.

Key skills and traits for intelligence officers include: ability to work independently, persistence, good communication skills and a thorough knowledge of police practices. Intelligence analysts' skills and abilities include: excellent research and writing skills; computer literacy; creativity; ability to work independently; logical thought processes; persistence; ability to think critically; willingness to make judgments; and visualization skills. Previous analytic-based work experience could be in law enforcement or in journalism, research, the social sciences or another related field. Analysts must be self-directed and intellectually disciplined in their work habits, initiating lines of investigative inquiry and identifying resources that will assist the investigation or study.

The analysts may be specialists in particular areas within the field due to their experience or training. Some may focus on financial, strategic, or crime analysis. Or, their jobs might be organized by types of criminal activity (e.g., narcotics or white collar crime), or by criminal groups (e.g. Cosa Nostra or Russian Mafia), or by geographic unit (e.g., country, region, or county).

The intelligence unit should have adequate data entry support. Entering data into computerized data bases is a time-consuming task that is best done by trained data entry specialists. Using support personnel for data entry provides for a more efficient use of analysts and investigators.

The hiring process for analysts often includes the successful completion of a practical exercise. This test could require an analyst to draw a simple chart and conclusions based on a few pages of investigative material. Depending on the level of the analyst to be hired, the completion of a more in-depth practical exercise, along with graphic products, conclusions and investigative recommendations, could be required. Psychometric tests and logical reasoning tests are also given. If the agency does not have experienced analysts on its staff, it may want to invite an analyst from another agency to assist in the evaluation process. In this instance, IALEIA can provide the names of analysts within a geographic area who might serve as evaluators.

Analysts' Compensation, Benefits and Funding

As analysts' value have been realized by law enforcement managers, their salaries have risen. In 2004, salaries reported in an IALEIA survey ranged from an average of $45,790 to an average of $64,267; * however, these averages may not tell the whole story as some analysts make less than $35,000 while others make over $100,000.

The adoption of the intelligence led model in the corporate world has had an impact on public sector salaries for analysts since private sector salaries can be considerably higher. Some agencies are experiencing considerable 'turnover' in analysts who take higher paying jobs after receiving training and a few years of experience. Clearly, this is not cost-efficient.

Analysts' pay should be at least commensurate to that of law enforcement officers who have the same number of years of experience. This recognizes the value of analysis and provides parity. In some agencies, both sworn and civilian personnel perform the same analytic duties; their pay should be equal.

Employee benefits are often dictated by union contracts, but analysts' benefits should be similar to officers' whenever possible. This includes the assignment of agency vehicles and laptop computers to analysts.

Career paths have not been as broad in scope for civilian analysts within a law enforcement agency as they have been for sworn officers. Some agencies are now accepting analytic experience as a qualification for management positions. This is expected to increase as more departments benefit from the skill sets analysts bring to all positions.

* Informal data from Howard Atkin, IALEIA vice president and manager of the 2003-2004 analysts' survey completed by IALEIA.

Analysts should be encouraged to take pride in their profession and become certified analysts. Agencies should consider adopting certification as a criteria for hiring or promoting within their organizations. The Society of Certified Criminal Analysts is the official certification arm of IALEIA. (See page 21 for information on certification.)

Analytic units can be funded through a number of funding streams which currently support priority police initiatives. From SHOCAP (serious, habitual offender comprehensive action program) to community/problem-solving policing, to police computerization projects, to strategic planning components, analysts are a necessity. Many of the grants from the U.S. Department of Justice, Bureau of Justice Assistance, require an analytic component. Grants through the Department of Homeland Security also require analytic capabilities to perform threat and risk assessments.

Whether the analytic unit is funded through the agency or by a grant from another source, it should not be considered an "extra" or a "frill." Analytic support for law enforcement work generates faster and more successful investigations and prosecutions. In some agencies, a broader use of analysis has been initiated in the face of cutbacks as a more effective use of limited resources.

Intelligence Procedures

The intelligence unit should have a regularized method of information collection, collation, evaluation, storage, analysis and dissemination. Written standard operating procedures should be developed to guide this process.

Under information collection, standards should refer to the need for legal acquisition of data and the evaluation of data as to its reliability and validity. For example, data should be collected in accord with applicable state and federal laws and regulations. The two most broadly disseminated standards in the U.S. are those promulgated by the federal government to cover the Regional Information Sharing Systems and other information systems undertaken with the use of Federal funds (*28 Code of Federal Regulations* 23.20) and the *Law Enforcement Intelligence Unit (LEIU) Guidelines*. Both of these rely on data evaluation criteria and an audit trail to ensure data entering the systems are appropriate and dissemination of the data is authorized.

Written procedures for an intelligence unit could also detail the types of analytic products that may be provided to investigators, the method by which an analysis should be requested and what feedback requirements the agency has designed. This document can be provided to the managers of all divisions or bureaus within the law enforcement agency so everyone is aware of the procedures.

An overall view of how intelligence and analytic units function is seen in *Intelligence 2000: Revising the Basic Elements,* a 240-page book on intelligence and analysis, available from IALEIA. Its appendices include varied guidelines and standards for intelligence, including the above mentioned LEIU guidelines and 28 *C.F.R*. 23.20. Another resource is the CD ROM, *Turnkey Intelligence: Unlocking Your Agency's Intelligence Capabilities,* which includes sample policies and products along with numerous pieces on intelligence topics.

Intelligence Training

Analysts and intelligence officers should have as broad a range of intelligence training as possible. This should include training in varied techniques used in intelligence as well as elements on different crime groups and criminal activities.

There are different training standards in different countries. In the U.S., *Minimum Criminal Intelligence Training Standards for U.S. Law Enforcement,* were issued in September 2004. Those standards recommended training for police executives, intelligence officers, patrol officers, intelligence supervisors and intelligence analysts.

The U.S. standard for basic intelligence officer training is a one week course on the intelligence process, legal restrictions, sources of information, file management, analytic techniques and collection plans. In some agencies, a second week focusing on practical exercises in surveillance and other covert operations is also given. Minimum standards for analytic training reflect a one week course on sources of information, legal restrictions, the intelligence process, basic analytic techniques including report writing, association analysis, telephone record analysis, flow analysis, inference development, critical thinking and financial analysis.

Analytic training has been available through Anacapa Sciences, the Federal Law Enforcement Training Center, police agencies in various countries, states and provinces, the RISS centers and certain private vendors. Within the last two years, a Foundations of Intelligence Analysis (FIAT) course was developed by a partnership of IALEIA, LEIU, the RISS centers and the National White Collar Crime Center (NW3C). That course is offered through all the consortium members at varied locations around the U.S., in Canada, Europe and South Africa.

Advanced analytic training has been less standardized. Anacapa Sciences, for example, offers computerized analysis and a financial analysis course. The Royal Canadian Mounted Police/Canadian Police College and Istana Enterprises offer strategic analysis courses. The New Jersey Division of Criminal Justice offers computerized analysis, financial investigative analysis and strategic analysis courses. Other courses are available through specific agencies or vendors.

Some agencies, including the Royal Canadian Mounted Police, have internship programs that combine formalized training with on-the-job training over a two-year period, culminating in the award of an RCMP certification. A less formal program within an organization with several analysts would be to pair more experienced analysts with younger analysts to help guide their development ('mentoring'). The Canadian Police College provides the standard analytic training course in Canada.

In the United Kindom, a series of intelligence courses have been developed, or are in the process of being developed, in support of the ***National Intelligence Model*** (NIM). These training courses focus on the core products in the NIM (strategic assessments, tactical assessments, problem profiles and target profiles) and include topics such as historical perspective, role of the analyst, glossary of terms, thinking processes, evaluation, link charting, flow and event charting, case analysis, behavioral analysis, comparative case analysis, volume crime analysis, open sources, investigative techniques, report formats, written and oral skills and documentation.

U.S. standards for intelligence manager training is a 24-hour seminar including the intelligence process, training, evaluating and assessing intelligence functions, personnel selection, intelligence policies, security, legal and privacy issues, intelligence products, information sharing systems, collection plans and handling sensitive information.

Law enforcement executive training on intelligence should be at least four hours and include the *National Criminal Intelligence Sharing Plan*, intelligence led policing, the intelligence process, legal and privacy issues, and information sharing networks and resources.

Recruits and currently-serving police personnel should receive a two-hour intelligence awareness training on the intelligence process, indicators of criminal activity, legal issues, and information systems and resources.

IALEIA maintains a listing of all known analytic-related training on its web site, www.ialeia.org. Another source of intelligence training is through conferences held by IALEIA and LEIU (See page 27 for more information on LEIU).

Intelligence Products

There is a range of intelligence products which are the result of careful and thorough analysis of varied documents. In the past, the most noticed of these products were often the most graphic, e.g., charts and summary tables. But the most important products are threat assessments, warnings, financial analyses, and other written products that not only display data, but also interpret their meaning.

The intelligence manager should be familiar with the standards of quality in these products so that their accuracy and value can be ascertained. This is one reason why all intelligence managers should receive training in analytic techniques and methods. (See training, page 11-12.)

Intelligence products must support the mission of the organization and provide viable recommendations for action regarding crime control. There is a broad range of intelligence products that can be used for strategic or tactical purposes.

Overall, the intelligence manager must first be aware of the analytic process which provides the context for the products. The analytic process consists of organizing information, ascertaining its meaning, determining what is there, and identifying what needs to be there to complete a thorough analysis or investigation. Simply, analysis could be thought of as a series of questions which may begin with "what happened?" but do not conclude until the investigation is resolved.

Intelligence Products to Expect or Request

The analytic manager can expect to receive:

, threat assessments on crime groups or activities that may pose a threat to the jurisdiction. These assessments should include:

-historical information on the group or activity and its primary actors

-its location(s)
-sources of income (legal and illegal)
-size of group
-ties to other groups
-ties to other illegal activities
-biographical data on leaders
-potential threat to the jurisdiction
-possible vulnerable sectors of the jurisdiction
-conclusions
-recommendations for action

, vulnerability assessments on events including political rallies or dignitary visits, which could include:

- potentially vulnerable locations along the travel route or at the site of speeches
- possible local groups which may disrupt the proceedings including a brief report on their ideologies, potential for violence, histories, memberships, etc.
- possible outside groups which may disrupt the proceedings including material described in threat assessments

Vulnerability assessments can also be done on locations such as critical infrastructure sites that may be targeted by domestic or international terrorist groups.

- risk assessments on the likelihood of a particular group or person mounting a criminal action against a particular target
- action plans for law enforcement activity regarding the threat posed by a particular crime group or criminal activity.
- premonitories - overview assessments of particular crime groups which have a negative impact on the jurisdiction including:
  -its leadership
  -its past criminal activities
  -its business participation
  -its geographic spread/territory
  -its members and their vulnerability to enforcement action
  -its structure and its vulnerability to undercover operations and/or informant

- policy analysis on laws, regulations or guidelines (or their absence) that may result in a change (or creation) of policy.
- association analyses including: link chart(s); biographical summaries on all major figures; summary of the chart; any insights gained into the structure of the organization; and what impact that structure has on the criminal actions occurring or on the investigative steps that might be taken; conclusions about the organization or linkages that can be drawn; and recommendations for further action, which may include electronic or physical surveillance, undercover operations, informant development, or specific targeting.
- telephone record analyses including: telephone record chart(s); subscriber information; criminal history record information and background information on all major contacts; primary and unusual sources of incoming calls; written reports including primary numbers called; unusual calls; calls by date and hour or by state or other region; patterns in calls; conclusions and recommendations including requests for the subpoena of additional records or a request for electronic surveillance on certain phones. This analysis may be used for probable cause for an electronic surveillance.
- flow analyses (event, activity, commodity and visual investigative) including: flow chart(s); biographical information on all major figures; summary of the chart; any conclusions that can be drawn about the activities occurring; and recommendations for further action. These charts often point to missing information or presumed occurrences about which more proofs should be gathered.
- financial analyses (bank record, net worth, business record, source and application of funds and financial statement analysis) including: summaries of financial activity; tables; graphs; commodity flow charts; conclusions; and recommendations for further action. Recommendations often include requesting the subpoena of additional records, corporate checks or criminal history record information checks, interviewing bank personnel or accountants, and pursuing 'proceeds of crime' legal actions.
- case analyses including a variety of analytic products based on the overall data generated by an investigation. These products are summarized in a written report and include conclusions

and recommendations. Case analyses often result in uncovering new leads in an investigation.

- crime pattern analyses - looking at the similarities and differences among incidents to determine if they have been committed by the same individual or group and when further similar incidents will occur
- manual or computerized maps reflecting geographic particulars of criminal activity and/or calls for service in the jurisdiction
- crime summaries and charts which analyze criminal activity and indicators to support community and problem-oriented policing
- problem profiles - products that look at the symptoms of criminal activity as well as its underlying problems and identify ways to intervene in the problem and thus eliminate the symptoms (problem oriented policing)
- target profiles - comprehensive views of specific individuals or entities that are suspects with all known data on those arranged into varied summaries, both written and graphic.

Threat Assessment Model

*One model for completing a threat assessment of an extremist or terrorist group shown below, was developed within the California Department of Justice. **

Group Characteristics Evaluation

The first step in preparing threat assessments is to determine whether the groups are, in fact, criminal extremist groups. Four basic characteristics lend themselves to such a determination:

- *Ideology - The groups exist and are determined, motivated, and focused.*
- *Field of Operations - The groups have a geographical area of activity and access to targets.*
- *Tactics - The groups have patterns of behavior or preferred methods of operations.*
- *Membership - The members are committed to the groups and have the capability of committing acts of violence in support of the groups' goals or beliefs.*

Criminal Predicate Analysis

The second step in preparing threat assessments is an analysis of the known, suspected, or potential crimes associated with criminal extremist groups. Four categories assist in that analysis:

- *Types of Crimes - The groups are involved, suspected of being involved, or demonstrating a willingness to become involved in crime.*
- *Capability Factor - The groups are capable of criminal activity, and there is a pattern or history of criminal activity.*
- *Probability Factor - There is a reasonable probability the groups will commit crimes.*

* *"Threat Assessment Guide*: ***Evaluating and Analyzing Criminal Extremist Groups****," Jerry Marynik for California Department of Justice, Sacramento, CA, 1998.*

- *Violence Potential Level - The groups have a propensity for committing acts of violence and have stated intentions of committing violence*.

Target Analysis

Analyzing or reviewing potential targets is the third step in preparing threat assessments. Understanding relationships between criminal extremist groups and targets help law enforcement authorities prepare for a tactical response. Five considerations must be given to analyzing or reviewing potential targets?

- *Target Identification - Who or what are the potential targets? The groups' activity is indicative of preparing for acts of violence against the targets.*
- *Vulnerability - The targets are susceptible to acts of violence.*
- *Probability of Attack - The targets will probably be attacked.*
- *Damage Potential - If attacked, the damage could be significant.*
- *Consequence of Intervention - There are adverse implications for law enforcement authorities responding to the threat.*

* * * *

Threat Assessment Report Model

EXECUTIVE SUMMARY

REPORT

- Group Characteristics
  - Ideology
  - Field of Operations
  - Tactics
  - Membership
- Criminal Predicate
  - Types of Crimes
  - Capability Factor
  - Probability Factor
  - Violence Potential
- Warning Signs
  - Weapons and Explosives
  - Cellular Structure
  - Military-Style Training
  - Intimidation
- Potential Targets
  - Target Identification
  - Vulnerability
  - Probability of Attack
  - Damage Potential
- Consequence of Intervention
- Conclusion

Evaluation of Intelligence Unit

The products and successes of an intelligence unit must be describable and measurable if they are to be judged properly by management. To say that the intelligence process is an intellectual one is true, but it produces results that can be quantified.

Many intelligence supervisors require weekly progress reports from analysts on work assigned. While supervision of intelligence is essential, intelligence officers and analysts are often well-trained, independent thinkers who may respond more favorably to collegial, rather than hierarchical, management.

The mission of the intelligence unit sets the framework for the duties of the officers and analysts and for the expected results. If the mission is to provide accurate, timely and actionable information in support of law enforcement operations, then its success in providing the data in that manner can be observed.

The 2004 update of the *National Criminal Intelligence Sharing Plan* included two documents to assist in the evaluation of products of the intelligence unit and its operations. The first is *Law Enforcement Analytic Standards* which provides 25 standards for analysts and analytic products. The second is the *LEIU Intelligence Unit Audit Checklist,* which covers other areas of the intelligence cycle. The *Analytic Standards* can be used as part of an evaluation of analysts, while the *Audit Checklist* can be used as part of an evaluation of an intelligence unit.

Analyst Certification

In 1990, the Society of Certified Criminal Analysts (SCCA) was developed to establish and apply standards to delineate professional analysts. SCCA was accepted as the official certification arm of IALEIA in 1996.

Its Board of Governors (ten analysts) sets criteria for certification and administers the process and certification testing. There are two levels of certification: regular and lifetime. Regular certification, which is valid for three years, requires: at least two years of college, completion of a basic analysis course, membership in IALEIA, two years experience in law enforcement, military or international security analysis, and approval by the Board of Governors.

Lifetime Certification requires: at least four years of college, 10 years experience in analysis, membership in IALEIA, completion of a basic analysis course and approval by the Board of Governors.

A five-hour test is mandated for all those applying for certification. The first section includes objective questions taken from six standard analytic texts. The second half is a practical exercise which requires the analyst to review several pages of data, to prepare analytic products and to arrive at conclusions and recommendations about the material.

Since 1994, the SCCA has given one award per year for Lifetime Achievement. All Lifetime Certified Criminal Analysts are eligible to be nominated for the award.

As growing numbers of analysts become certified, certification should become the standard for hiring and promotion of analysts. In some agencies, certification is already a requirement for promotion or hiring.

The SCCA website is at www.certifiedanalysts.org and includes a dowloadable application form along with specific criteria and application guidance.

Some Resources in Literature

Andrews, Jr., Paul P. and Marilyn B. Peterson, ***Criminal Intelligence Analysis.*** Orangevale, CA: Palmer Press, 1990.

Clarke, Ronald V. and John Eck. ***Becoming a Problem Solving Crime Analyst in 55 Small Steps***. London, UK: Jill Dando Institute, 2003.

Europol, ***Analytic Guidelines***. The Hague, Europol, 1999.

Global Intelligence Working Group. ***National Criminal Intelligence Sharing Plan.*** Tallahassee, FL 2003. October 2003 and 2004.

Godfrey, E. Drexel and Don R. Harris, ***The Basic Elements of Intelligence***. Washington, DC: Law Enforcement Assistance Administration, 1971. (out of print)

* Gottlieb, Steven, Raj Singh and Shel Arenberg, ***Crime Analysis: From First Report to Final Arrest***. Montclair, CA: Alpha Publishing, 1994.

* Heuer, Richards, ***The Psychology of Intelligence Analysis***. Washington, D.C. Government Printing Office, 1999.

International Association of Chiefs of Police, ***Criminal Intelligence.*** Gaithersburg, MD: 1984.

---- ***Criminal Intelligence Policies***, February, 1998 and 2003.

International Association of Law Enforcement Intelligence Analysts, ***Successful Law Enforcement Using Analytic Methods***. South Florida, FL: IALEIA, 1996.

---- ***Intelligence Led Policing.*** Lawrenceville, NJ: IALEIA, 1998.

---- ***Intelligence Models and Best Practices.*** Lawrenceville, NJ: IALEIA, 1999.

---- and Global Intelligence Working Group. ***Law Enforcement Analytic Standards***. Tallahassee, FL 2004.

Interpol Crime Analysis Working Group, ***Crime Analysis Booklet, 2nd edition***. Lyon, France: Interpol, August, 1996.

Kedzior, Richard, ***Criminal Intelligence Analyst: A Growing Profession in Law Enforcement to Support Police Executives***. Toronto: Criminal Intelligence Service Ontario, March, 1997

Law Enforcement Intelligence Unit, ***Intelligence Into the 21st Century***, various authors. Sacramento, CA: L.E.I.U., November, 1995.

Marynik, Jerry, Threat Assessment Guide: ***Evaluating and Analyzing Criminal Extremist Groups***. Sacramento, CA: California Department of Justice, April, 1998.

* McDowell, Donald, ***Strategic Intelligence***. Australia: Istana Enterprises, 1999.

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

* ---- ***A Guide to the Financial Analysis of Personal and Corporate Bank Records***, Richmond, VA: National White Collar Crime Center, 1996 and 1998.

* ----, Bob Morehouse and Richard Wright, eds. ***Intelligence 2000: Revising the Basic Elements A Guide for Intelligence Practitioners.*** Lawrenceville, NJ: IALEIA, 2001.

Rabon, Don. ***Investigative Discourse Analysis***. Durham, NC: Carolina Academic Press, 1994.

Ratcliffe, Jerry, ed. ***Strategic Thinking in Criminal Intelligence***. Annandale, Australia: The Federation Press, 2004.

Reuland, Melissa Miller. ***Information Management and Crime Analysis:***

Practitioners' Recipes for Success. Washington, DC: Police Executive Research Forum, 1997.
Rossmo, D. Kim. ***Geographic Profiling.*** New York: CRC Press, 2001.
van der Heijden, Toon and Emile Kolthoff. ***Crime Analysis***. ISBN 90-74555-01-2, The Netherlands.

* Books used as basis for SCCA objective test, see p. 21..

For a more expansive listing of books, visit the IALEIA website at www.ialeia.org.

Analytic Software

Analysts should have appropriate hardware and software for databases, spreadsheets, data and/or text mining and visualization of information. Some analysts are constrained to using "off the shelf" software including Microsoft Office 2000 products such as - Excel and Access, or Visio for charting.

More sophisticated products for analytic use are made by companies including:

ClearForest (text mining)
Environmental Systems Research Institute, Inc. (Arc View mapping)
i2, Inc. (Analyst's Notebook, ibase, and other products)
Intelligence Technologies (In-Tel-All database and telephone record analysis)
Memex - (Intelligence Manager database and Intelligence Analyst text mining products)
Pen-Link Ltd. - (database)
Verint Systems, Inc. (communication data analysis)
Visual Analytics - (VisuaLinks charting and Digital Information Gateway text mining)
Xanalys - (Watson database and other text mining products)

It is important to note that purchasing analytic software is no substitute for having analytic staff. Hardware and software are tools which, in the hands of a professional analysts, can be of great assistance to law enforcement.

IALEIA

Founded in 1980, the International Association of Law Enforcement Intelligence Analysts, Inc. (IALEIA) is a non-profit association with the mission to bring excellence and professionalism to law enforcement intelligence analysis worldwide.

IALEIA has about 1,800 members in the United States and more than 40 other countries in North America, Europe, South America, Australia, Africa, India and Asia.

Its annual training conference, often co-hosted by an IALEIA chapter, allows analysts to receive more in-depth training in new or advanced analytic methodologies. These have become an international meeting ground, with numerous countries and agencies sending participants. The Annual Training Conference and General Meeting has been held in locations including the Washington, DC area; Sacramento, CA; Boston, MA; Chicago, IL; Ottawa, CAN; and New York, NY.

A large part of IALEIA's role relates to training and outreach within the law enforcement community. To further this, IALEIA maintains a presence at the International Association of Chiefs of Police annual conference each year. This provides its leadership with the opportunity to meet with police executives from around the world. It also participates in other conferences and training sessions hosted by international, federal, state and local law enforcement organizations and agencies.

IALEIA publishes overviews and examples of analytic techniques in its annual *Journal*. Shorter items of interest to analysts and officers (training schedules, local chapter meetings, job openings, etc.) are found in the *Intelscope* newsletter, published electronically three times yearly, or on the IALEIA web site (http://www.ialeia.org) Submissions to both publications are encouraged.

An annual awards program provides recognition to analysts, authors, and police executives. These awards, begun in 1985, encourage excellence in law enforcement intelligence analysis.

IALEIA also has Supporting Member agencies which encourage analytic effort and professional participation. A listing of supporting agencies is found on page 29.

Membership in IALEIA is open to all law enforcement analysts, supervisors and managers, as well as military, international and private sector criminal analysts and officers. For more information, write IALEIA, P.O. Box 13857, Richmond, VA 23225 or call IALEIA at (804) 565-2059. In Canada, contact IALEIA regional director Jenny Johnstone at the Royal Canadian Mounted Police, johnstone@ialeia.org; in Latin America contact regional director George Gelman-Kipnis at kipnis@ialeia.org; in Europe contact Kate Pearce at pearce@ialeia.org and in South Africa, contact regional director Dalene Duvenage at duvenage@ialeia.org.

LEIU

The Law Enforcement Intelligence Unit (LEIU) was formed as a result of the recognized need for a coordinated exchange of criminal information among local law enforcement agencies on traveling criminals. Twenty six (26) law enforcement agencies met in San Francisco, California on March 29, 1956 to discuss problems and possible solutions. The most important result of that meeting was the creation of LEIU and the development of an organizational purpose that still survives. The purpose of LEIU is to gather, record, and exchange confidential information not available through regular police channels, concerning organized crime and terrorism.

LEIU is an association of state and local police departments. It has no employees and no capability as an entity to conduct any investigation or law enforcement activity of any kind. Each member agency is bound by, and acts pursuant to local law and its own agency regulations.

The LEIU is divided geographically into four (4) Zones, they are: Eastern, Central, Northwestern, and Southwestern. Each Zone elects a Chair and Vice Chair to serve as Zone Officers. Internationally, LEIU elects a General Chair, Vice General Chair, and designates a Secretary-Treasurer and a legal advisor who serve as International Officers. The International Officers, Zone Officers, past General Chair and two representatives from the Central Coordinating Agency make up the Executive Board. The Executive Board is the governing body of LEIU, and as such establishes policy and passes upon the admission of all members. The Executive Board is governed by a Constitution and Bylaws.

LEIU members are law enforcement agencies of general jurisdiction having a criminal intelligence function. Exceptions must be approved by the Executive Board. Associate Membership is available to former law enforcement officers who have served as an LEIU primary representative or who represented a LEIU member agency at two (2) or more National or Bi-Zone training seminars. Any person who meets this criteria can make application to become an associate member. Exceptions must be approved by the Executive Board.

IALEIA Supporting Member Agencies

Arizona Department of Public Safety
Australian Institute of Professional Intelligence Officers
Australian Federal Police
California Department of Justice, Sacramento, CA
Canadian Police College
Criminal Intelligence Service of Canada
Federal Bureau of Investigation, Washington, DC
Financial Crimes Enforcement Network, (FinCEN), Vienna, VA
Illinois State Police
Insurance Fraud Bureau of Massachusetts, Boston, MA
Iowa Department of Public Safety
Middle Atlantic-Great Lakes Organized Crime Law Enforcement Network (MAGLOCLEN), Newtown, PA
Mid-States Organized Crimes Information Center (MOCIC), Springfield, MO
National Criminal Intelligence Service of the United Kingdom
National Drug Intelligence Center, Johnstown, PA
National White Collar Crime Center, Richmond, VA

New England State Police Information Network (NESPIN), Needham, MA
New Jersey Division of Criminal Justice, Trenton, NJ
Organized Crime Agency of British Columbia
Pennsylvania State Police
Regional Organized Crime Information Center (ROCIC), Nashville, TN
Revenue Canada Customs
Rocky Mountain Information Network (RMIN), Phoenix, AZ
Royal Canadian Mounted Police
University of Manchester, United Kingdom
US Secret Service
Western States Information Network, Sacramento, CA
West Yorkshire Police, United Kingdom

IALEIA Chapters

Chapter 1 - Golden West
Chapter 2 - South Florida
Chapter 3 - Mid-States
Chapter 4 - Northern Florida
Chapter 5 - Washington, D.C.
Chapter 6 - Mercyhurst College
Chapter 7 - Mid-Atlantic
Chapter 8 - New England
Chapter 9 - Empire (New York)
Chapter 10 - Canada National Capital
Chapter 11 - United Kingdom
Chapter 13 - International War Crimes
Chapter 15 - Chapitre d'Haiti
Chapter 16 - Southwest
Chapter 18 - Land of Lincoln
Chapter 19 - Southwest Ontario
Chapter 21 - Western Pennsylvania
Chapter 24 - Northwest
Chapter 26 - Interpol
Chapter 27 - Sweden
Chapter 28 - Mexico
Chapter 29 - Western Canada

IALEIA Board of Directors (2004-2005)

Lisa M. Palmieri, C.C.A., President
Howard N. Atkin, C.C.A., Vice President
Paul G. Zendrowski, C.C.A., Secretary
Danny L. Taylor, Jr., Treasurer

Ritchie A. Martinez, C.C.A., Executive Director

Directors

Edward Feingold, Jr., C.C.A., Awards
Leo Jacques, Ph.D., C.C.A., Bylaws, Ethics, Elections
Hank Brightman, Ed.D., Fundraising, Corporate Liaison
Merle Manzi, Organizational Liaison
David Jimenez, C.C.A., Training, Education, Career Development
Melissa Johnson, C.C.A., Membership
Mark Massop, Member/Chapter Liaison
Michael J. Hall, C.C.A., Communications
Mary B. Vaughan, Marketing

Jenny Johnstone, Canada
George Gelman-Kipnis, Latin America
Dalene Duvenage, Africa, India, Asia and Australia
Kate Pearce, Europe