The Criminal Intelligence Function:
Toward a Comprehensive and Normative Model

by Stephen R. Schneider

INTRODUCTION

The increasing complexity and sophistication of organized crime means that the need for an effective criminal intelligence function has taken on a heightened importance. However, the discipline of criminal intelligence still remains largely misunderstood and under-utilized. In 1987, Martens said that many intelligence programs in the United States "have been abandoned and nearly all have failed to reach their potential" (p. 131). His criticism stemmed from the fact that "intelligence is seldom more than an accumulation of often irrelevant data that serves only marginally useful purposes" (Martens, 1987, p. 134). Sommers argues that these weaknesses arise from a misconception of intelligence analysis which "emanates from a lack of understanding of its functions and benefits to police managers" (1986, p. 25). Nonetheless, criminal intelligence is gaining acceptance as a vital cog in crime enforcement. The commitment to this function, the advancement in the science of criminal intelligence, and the advent and utilization of sophisticated computer technology have furthered this police function. The objective of this paper is to present a normative model of the criminal intelligence function based upon a review of the dominant writings in the field. This model specifies workable guidelines and prerequisites for an effective criminal intelligence function, or at least a framework for this model. It does not purport to be the definitive model of the criminal intelligence function, but provides one framework or blueprint. The paper is demarcated into three parts: the criminal intelligence function, the nine stages of the criminal intelligence process, and organization/environmental factors.

THE CRIMINAL INTELLIGENCE FUNCTION: CONCEPTS AND GENERAL REQUIREMENTS

Criminal intelligence has been defined as "...the product of systematic gathering, evaluation, and synthesis of raw data on individuals or activities suspected of being, or known to be, criminal in nature" (National Advisory Committee on Criminal Justice Standards and Goals, 1976, p. 122). Criminal intelligence can be demarcated into two broad categories: tactical and strategic. Tactical intelligence is collected for the short term in support of an immediate law enforcement objective, such as the successful completion of an active investigation. Strategic analysis looks at both past and current data in support of a law enforcement agency's planning and management (Godfrey and Harris, 1971, p. 2; International Association of Chiefs of Police, 1985, pp. 5-6).

Based on this delineation, a weak intelligence capability can prevent investigators from obtaining information that may aid them in securing arrests, seizures, and prosecutions in active investigations; inhibit the ability of police to accurately gauge the types and extent of organized criminal groups and their activities; and starve police management of the information necessary to do long-term planning of enforcement strategy and resource allocation.

The purpose of the intelligence function is to increase knowledge and understanding of the particular problem under consideration in order that logical decisions may be reached (U.S. Army, 1963, p. 3). In this respect, the intelligence process is no different from basic or applied research; define the problem, collect the data, assess the data, collate and organize the data, and disseminate it to the appropriate person or agency (Martens, 1987, p. 133).

In general, a criminal intelligence project essentially involves four phases: information collection, collation, analysis, and dissemination. Within these broad parameters, a criminal intelligence project must incorporate nine stages in order for it to reach its full potential:

1) Planning
2) Collection of information
3) Assessment of information validity
4) Collation of information
5) Analysis of information
6) Assessment of analytical rigor and value
7) Dissemination of intelligence
8) Application of intelligence
9) Review and assessment of criminal intelligence project/function/unit.

This intelligence process is succinctly captured by Godfrey and Harris (1971) and is shown in Figure 1. That there is a critical need for a criminal intelligence function in organized crime and drug law enforcement has been well-
The first step is determining the methodology to be used in the intelligence process. A suggested methodology for a tactical or strategic assessment is encompassed in this nine-step model. Within the planning stage, there are four inter-related methodological components: 1) conducting an environmental scan; 2) choosing a topic for inquiry; 3) defining the problem; and 4) developing a collection plan. Information collected and formulated in each of the four planning steps should be presented in a detailed project proposal for approval by supervisors and management, prior to initiating the project.

1) **Environmental Scan** - The first requirement of the planning activity is developing a wide-ranging awareness of the environment surrounding the intelligence function. This means focusing on the complete problem rather than zeroing in on specific matters at this early stage. A total problem-solving approach starts from the broadest practical base to understand the special and distinct characteristics of the issue to be examined (McDowell, Wardlaw and Schmidt, 1991, p. 11). An environmental scan includes identifying and examining factors such as demographic characteristics (age, population size, racial and ethnic composition of population, etc.), overall crime rate, general enforcement objectives and strategies, and economic, socio-economic, and physical conditions. In all of these categories, trends should be identified and extrapolated into the future. An environmental scan should also include identifying relevant national and international issues which impact on the police agency's constituency and intelligence or enforcement responsibilities. In general, within the intelligence unit, there must be a capacity for an ongoing and systematic scanning of the environments that critically impact on the police agency's constituency. The results of scanning must not only be used as a basis for intelligence, but must also be articulated to management on a regular basis.

2) **Choosing a Topic** - Once the general parameters are laid out through the environmental scan, the next step is to choose a topic to analyze. Topics for analysis result from a variety of sources, including the environmental scan, executive management policy, recent events, analytical queries, or standard operating procedures (Peterson, 1991/92, p. 24). The inquiry should be answerable within the constraints of available resources. Generally, the narrower the topic, the better. Limiting it to a specific crime type or group is wise. An even more focused approach is concentrating on a given group's involvement in a specific type of crime within a particular jurisdiction (Sommers, 1986, p. 34).
3) Problem Definition - Once a general topic has been chosen, a specific problem must be defined. According to Dintino and Martens, until law enforcement precisely defines the problem, there can be no strategy (1981, p. 58). What is involved at this point is an examination of the issues subsumed within the topic, considering it from several viewpoints and, ultimately, breaking it down into a set of questions or a working hypothesis to be proved or refuted by the intelligence project (Sommers, 1986, p. 34). For example, an hypothesis for a strategic assessment might be: has organized crime infiltrated legitimate business in this community? The problem definition and hypothesis formation is critical for it will serve to guide the collection and subsequent analysis of information.

4) Developing a Collection Plan - To prevent the intelligence system from becoming inundated with detailed and unimportant information, the collection process must be planned, directed, and coordinated (Wolf, 1978, p. 17). According to Dintino and Martens, a collection plan is one of the most important phases in the intelligence process in that it represents the only rational mechanism to manage the intelligence officer's collection effort (1983, p. 77). The collection plan includes the analyst's research methodology. It serves as a tool that directs and focuses collection resources needed to prove or refute a hypothesis, thereby ensuring that the collection effort is suited to the requirements of the intelligence task. It establishes precise pieces of data necessary to accomplish the overall goal of the project and provides the intelligence officer with an understanding of how the data fits into the larger puzzle (Dintino and Martens, 1983, p. 77). Without the employment of a collection plan, intelligence officers are left with their own predilections, collecting data that they believe are relevant to the organization and intelligence unit. The results are non-direction, misdirection, and a totally inefficient and ineffective utilization of collection resources (Andrews, 1990, p. 40). A collection plan should logically flow from the problem definition. It does not have to follow any prescribed format and can range from single worksheets to long, detailed plans (Andrews, 1990, p. 43). It must be flexible and responsive to changing developments in its environment and the intelligence process (McDowell, Wardlaw and Schmidt, 1991, p. 13). However, a collection plan should minimally include: 1) a description of the data to be gathered, 2) the sources of the data; 3) the steps to be taken to obtain the data; and 4) the specification of the completion date for each stage of data collection (Sommers, 1986, p. 34).

**Stage Two: Data Collection**

Once planning is complete, information collection is the next step in the intelligence process. The truism "garbage in garbage out" expresses the importance of the collection process to the overall intelligence function. Effective organized crime control requires collecting the most important and most relevant information. Without quality, pertinent data, no amount of analysis will create accurate and purposeful intelligence.

Data collection must be clearly focused rather than permitting the random collection of data which may be irrelevant or nonessential. To establish a well-defined collection effort, the problem definition must guide data collection. This allows the collection of data that are both goal-oriented and clearly relevant to the criminal activity/network being examined (Martens, 1987, p. 132).

Data are collected in a number of ways and from a number of covert and overt sources. The tools and/or sources within organized crime investigations are: (1) on-file data and intelligence; (2) investigators; (3) informants; (4) undercover operations (infiltration, stings, etc.); (5) surveillance (physical and electronic); (6) other police operational units, police forces, or intelligence agencies; (7) other government agencies; (8) public information sources including the media, public data bases, public registries, telephone books, etc.; (9) concerned citizens, including crime victims, complainants, and witnesses; (10) scholarly works; and (11) arrested persons (Godfrey and Harris, 1971; International Association of Chiefs of Police, 1985).

The management and control of information sources is key to the collection process. A comprehensive understanding of the likely sources of different types of data must exist. The intelligence unit must maintain a clear, visible, and legitimate profile to engender the level of trust and awareness necessary to encourage the source to pass over information (McDowell, Wardlaw and Schmidt, 1991, p. 22).

Wolf recommends that an intelligence unit draft guidelines which provide for the establishment of a Criminal Source Control Office (CSCO) to manage a system which formalizes and maximizes the intelligence unit's capability to use informant data. Among the critical considerations to be included in these guidelines are the processing, registering, and payment of informants. Processing informants should be performed to insure that a permanent pool of criminal information is available to an intelligence unit, to have a record available of the identity of informants to protect intelligence officers from utilizing unreliable information; and to prevent duplication of effort. The purpose of the CSCO is to enable an intelligence unit to have a reasonable expectation of becoming the recipient of high grade information (Wolf, 1978, p. 18).

Finally, all information should enter through a single point in the intelligence unit and be logged in. This logging should show the date and time the data was received, the source of the information, a title of the information which sufficiently describes it, handling instructions, and document number. Logging of information can be performed by the analyst or an on-call duty officer (Godfrey and Harris, 1971, pp. 42-43).

**Stage Three: Verification of Information**

As data are collected, they are evaluated. The objective is to verify the validity and accuracy of the raw data as well as the efficacy of the collection effort. Moreover, it ensures that the data are consistent with the mission of the intelligence unit, management policy,
and ethical standards. Finally, this stage ensures that the data are, in fact, useful for an investigation, strategic planning and/or management decisions. The absence of this phase, or the lack of any standard of quality assurance, will result in the collection and filing of raw data which can potentially result in misguided policies and enforcement efforts, a waste of resources, and serious privacy issues (Dintino and Martens, 1983, p. 90).

According to Wolf, the verification of information must be based on its pertinency, reliability, and accuracy:

- **Pertinency**: New information should immediately be examined to determine the degree to which it is relevant, urgent, and valuable. The examination asks three questions: 1) Is this information relevant to the subject of a specific investigation(s), defined problem, or strategic planning? 2) Is this information needed immediately, and if so, by whom?; and 3) Is this information of possible present or future value? If so, to whom? If the information is not substantially relevant to a specific analytical project, or future potential project, it should be discarded.

- **Reliability**: Information found to be pertinent is next judged on the reliability of the source of information and on the reliability of the agency and/or individual who collected and reported it. The source of the data, its past reliability, and the motives of the source (particularly if it is an informant) must be critically evaluated. The principal basis for the determination of the reliability is previous experience with, or knowledge of, that source. Additional questions on the reliability of the source are: 1) Under the conditions existing at the time, was it possible for this information to have been obtained?; and 2) Would the source have had access to the information reported?

A reliability classification code should be applied to all reports. One set of reliability classification codes which could be applied is as follows:

<table>
<thead>
<tr>
<th>Reliability</th>
<th>Code</th>
<th>Substantiation</th>
<th>Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>Highly Reliable</td>
<td>H</td>
<td>Substantiated</td>
<td>S</td>
</tr>
<tr>
<td>Reliable</td>
<td>R</td>
<td>Unsubstantiated</td>
<td>U</td>
</tr>
<tr>
<td>Unknown Reliability</td>
<td>U</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

These codes should follow the relevant information stored on file and be contained in an intelligence assessment or report.

- **Accuracy**: Information is also judged for its accuracy or its truth and completeness. Accuracy is judged by answering the following questions: 1) Is the reported fact or event at all possible? 2) Is the report consistent within itself? 3) Is the report confirmed or corroborated by information from different sources or agencies? 4) In what respects does the report agree or disagree with other available information, particularly information known to be true? and 5) If the information does not agree with information from other sources or agencies, which is more likely to be true? (Wolf, 1978, pp. 18-22)

Dintino and Martens recommend that the verification task be assigned to a collator. Regardless of who performs this role, it is important that they be a senior, experienced individual. They should also be cognizant of the unit's goals and must ensure that the pre-established standards of quality control are being applied (1983, pp. 90-91).

**Stage Four: Collation of Information**

Collation is the next step. Essentially, it involves the orderly organization and arrangement of collected information, so that relationships between apparently disconnected data may be established, and the placement of data in a system which facilitates its rapid retrieval and analysis (Wolf, 1978, p. 22).

How intelligence information is organized is of critical importance. Data can be organized around specific categories, such as crime groups or networks (e.g., Asian organized crime or motorcycle gangs), criminal specialties (e.g., drug trafficking or loansharking), modus operandi, or geographic territory. Through this categorization of data, patterns and trends may become more obvious. These patterns or trends should then be used to stimulate a more intensive data collection effort directed at an above-mentioned category that may raise a new set of questions that deserve further investigation (Martens, 1987, p. 133).

The importance of categorizing data is based on the critical priority of organizing the intelligence unit's data base so that it can be manipulated in a number of ways. The effective and efficient collation of information is dependent upon a filing or data base system from which information cannot only be easily retrieved, but, as importantly, which provides for the capacity to cross-reference each data element. First and foremost, according to Godfrey and Harris, this will mean setting up functional files—on businesses, city sectors, popular meeting places of suspects—and cross-referencing them to biographic files. By themselves, biographic data are of only marginal value, but when combined with pools of knowledge about activities, localities, associates, movements, etc., all manner of associations and patterns of criminal or suspicious behavior may emerge (1971, p. 8).

Critical to the organization stage is how the information is stored. Today, computerized data bases are widely used to store information. The storage and analytical capacity of these computer systems are crucial for intelligence work (see Technology below).

A set of standards is necessary to maintain a successful intelligence unit data base/filing system. The standards of such a system should include:

1) Guidelines with responsibility for determining:
a) the kind of information which should be kept in intelligence files;
b) the method of reviewing the material as to its usefulness and relevance; and,
c) the method of disposing of material purged from intelligence files;
2) Systematic flow of pertinent and reliable information;
3) Uniform procedures for validation, evaluation, cross-indexing, and storing information;
4) A system for proper analysis of information;
5) A system capable of rapid and efficient retrieval of all information;
6) Guidelines for disseminating information from files; and
7) Security procedures (Harris, 1976, p. 16).

Stage Five: Analysis

Once the data are organized and stored, they are analyzed. The analytical phase is the backbone of the intelligence process. Here raw data are transformed into intelligence to be used by investigators and police management. Without the performance of this function, the intelligence unit becomes nothing more than a file unit (Harris, 1976, p. 27). However, despite its importance, this stage is the least understood and used by police departments (Dintino and Martens, 1983).

The intelligence unit must have both a tactical and strategic analytical capacity. Tactical intelligence contributes directly to the success of an immediate law enforcement objective (Wolf, 1978, p. 8). A tactical analyst dissects and reassembles the pieces of data gathered through the collection effort, recreating a story, scenario, or description of the inter-relationship of a criminal network. The analysis is guided by the objectives of the investigation. Moreover, the tactical analyst should be concerned with translating this information into a broader understanding of the criminal network, not just for prosecution purposes, but also for developing strategy and policy for the future (Dintino and Martens, 1981, pp. 61-62).

A police agency must also incorporate a strategic intelligence function which acts in support of management’s policy-making function, strategic planning, and enforcement goals. Unlike tactical intelligence, strategic analysis is proactive in nature. It must look beyond the immediate period, detect patterns of criminal activity and use these patterns to predict where future criminal activity will occur (Sommers, 1986, p. 27). Strategic analysts must see past the “making of a criminal case” and deduce from this data a broader understanding of the phenomenon or activity in question (Dintino and Martens, 1983, p. 100). The ultimate objective of strategic intelligence is to contribute to the reduction of the level of power and influence of crime in society (Stier and Richards, 1987, p. 73).

Using the analogy of a puzzle, Peterson (1990) identifies three steps which make up the complete tactical analysis phase: arranging the pieces (collection and collation), examining each piece for clues about its role or placement in the puzzle (analysis) and assembling the puzzle (case analysis or synthesis). In accomplishing these three general steps, Peterson argues for the use of a “Case Analysis Model.” This model, with particular emphasis on the analytical portion, is presented in Figure 2.

Analytic activity must focus on the hypothesis which was formulated, in conjunction with the problem definition, during the planning stage. Intelligence must be produced which relates specifically to the substance of the hypothesis and the pre-defined problem. Using the social scientific model, analysis should attempt to refute the hypothesis. This orderly approach to refining hypotheses has as its result the survival of only the strongest, best-founded and most convincing conclusion (McDowell, 1991, pp. 16-17). In testing hypotheses and drawing conclusions, the analyst, in turning information into intelligence, must use both inductive and deductive reasoning (Wolf, 1978, pp. 24-26). Once a conclusion has been drawn, the strategic analyst must make predictions and suggest alternative investigative, enforcement, or policy strategies.

It is the responsibility of the analyst to assemble all relevant data in a logical manner and identify any and all information gaps. Once identified, all missing data elements must be obtained and integrated into the analysis (Wolf, 1978, p. 24). Where data are fragmentary, conflicting, or incomplete, an analyst cannot draw clear-cut conclusions. To make interpretations, the analyst must rely on tentative assumptions and cautious inferences. The analyst must distinguish assumptions and inferences from facts to avoid misleading both the analyst and the decision-maker. If several courses of action follow from the facts, a competent analyst is obligated to present all the feasible alternatives for management’s consideration. Analysts can place a numerical estimate (such as 90 percent, 50 percent, or 10 percent) on the probability of the stated conclusion being true (Sommers, 1986, p. 38).

To ensure an independent and sound analysis, the intelligence analyst must: 1) avoid co-option by either management or operational elements in the agency; 2) constantly challenge and reassess the problem of organized crime and police strategies to address the problem; and 3) avoid the tendency to become engulfed in the legal technicalities of organized criminal activity (Dintino and Martens, 1983, pp. 103-104).

The criminal analyst must have a sound theoretical body of knowledge upon which to examine the problem, the capacity to conceptualize experience and the ability to develop models of organized crime based on a myriad of social, scientific, operational, and investigative theories (International Association of Chiefs of Police, 1985). The theoretical and methodological base for a comprehensive study of organized crime groups and their activities must be interdisciplinary. Predominant disciplines, complete with examples of their applications, include the following:
Flowing from these disciplines, McDowell, Wardlaw, and Schmidt (1991) argue that intelligence is concerned with determining four major parameters in respect to any identified group: capabilities, intentions, limitations, and vulnerabilities. According to the International Association of Chiefs of Police, strategic intelligence should be used for the following:

- to identify principals and their associates, including current and emerging leaders;
- to provide their descriptions and activities within a given jurisdiction;
- to identify the extent to which organized crime has developed within a given jurisdiction and its relationship to organized crime participants and activities in other jurisdictions;
- to assess organized crime’s capabilities, its direction, and its growth potential within a given jurisdiction;
- to determine the nature and extent of criminal infiltration into legitimate business;
- to identify those business enterprises and public officials which are controlled or directly influenced by criminal elements; and,
- to identify the economic, social, and governmental problems created by organized crime and suggest methods by which these may be impacted (1985, pp. 39-40).

In particular, collection requirements and analysis which examine organized crime groups and activities should address the following issues:

- illegal activities;
- territorial allocation and control;
- hierarchical structure of criminal group(s);
the economics of legal and illegal market(s);
financial flows/strength/net worth/asset identification;
allegiances and loyalties of participants in criminal networks
weak links in chain to exploit vis-a-vis informants/witnesses/undercover,
vigilance and corruption indicators,
composition (ethnic or otherwise) of the group and/or network;
recruitment and mobility practices,
competitor/complementary criminal networks;
psychological profile of boss/leader,
socio-cultural mores and values that govern ethnic crime groups and interpersonal relationships.

More specifically, Sommers (1986) provides a blueprint for analytical assessments which lists general questions to be answered (and data to be collected) for the completion of an analysis. She recommends that questions be formulated with reference to criminal groups and categories of criminal activity. Under each subheading, the analyst should examine the issue vis-a-vis 1) past and present; 2) future; and 3) enforcement alternatives. This is seen in Appendix A.

Analytical Assessments

In order for intelligence to be used in a strategic or tactical manner, the analyzed information must be presented in a functional assessment package. An effective intelligence unit must be able to perform a number of different, yet inter-related, strategic intelligence assessments. These analyses can be disseminated separately, depending on the needs of the investigator or police management, or as a whole. Examples of standard assessments include premonitories, threat assessments, aggressiveness analysis, market analysis, vulnerability analysis, estimates and general strategic assessments.

Premonitories are short-range assessments which bridge the gap between investigative and strategic intelligence; they use a strategic approach but are completed to generate investigative targets. The distinction between this and other types of strategic analysis is the time frame. Premonitories are generally done on potential subjects of investigation immediately prior to initiating an investigation whereas other forms of strategic intelligence products are more long-range (Peterson, 1991/92, p. 18).

Threat assessments analyze what organized crime groups and operations are costing the community, directly and indirectly, and what groups and operations are most threatening to the peace and stability of the community. This type of analysis can also be proactive when it attempts to predict the vulnerability of a community to organized crime (Lupsha, 1980; Miron and Douglas, 1975).

Aggressiveness analysis studies the aggressiveness, adventurousness, and expansionist tendencies of organized crime groups and their operations. This includes examining the use of lethal violence by a group (Lupsha, 1980, p. 38).

Market analysis examines a market for a particular product or service (both legal and illegal). The objective is to determine the interactions within the market, its size and value, consumers, the involvement of organized crime groups, etc. It may also attempt to predict the potential market for a new illegal product or service. Central to analyzing illegal markets is the use of economic theory and analytical models which center around the demand and supply of a product or service (Peterson, 1991/92; Reuter and Reuben, 1982; Schelling, 1967).

Vulnerability analysis examines the internal characteristics of an organized crime group to identify the individual points of weakness and vulnerability to interdiction.

Estimates are a compilation of data which measure the historical occurrence of criminal activity and include trends and forecasts based on that historical data (Peterson, 1991-92, p. 19). One example of a strategic intelligence estimate is the RCMP National Drug Intelligence Estimate which includes information on drug supply, routes, prices, source country production, availability, and future trends.

General strategic assessments are an overview of all known information on a criminal group or criminal activity with conclusions about the group and recommendations concerning possible enforcement measures against the group, network, or criminal activity (Peterson, 1991/92, p. 19). As the name indicates, these assessments are broad in nature and often summarize intelligence contained in other analyses.

Organized Crime Analytical Models and Charting Techniques

Intelligence analysis employs analytical models which detail information for tactical and strategic intelligence assessments. These techniques allow complex associations, activities and relationships existing in a criminal network or market to be displayed clearly and simply (Stockley, 1988, p. 299). Organized crime analytical models include the following.

Telephone Record Analysis - Also known as telephone toll analysis, this technique involves the identification, recording, and compilation of telephone company, long-distance service, and/or dialed number recorder information to highlight the telephone contacts of a suspect under investigation. It is also useful in identifying criminal accomplices and for future investigation or surveillance. The products of a telephone record analysis include a written report, charts, listings, and matrices (Peterson, 1990, p. 32 and 85-115). A telephone record chart is displayed in Figure 3.

Flow Analysis - This includes event flow and commodity flow analysis. Event flow analysis views the chronology of the criminal
activity while commodity flow looks at the flow of goods, services, or currency within a criminal network. A chart of the chronology of an event flow chart may show the events which led up to a mob murder, or the various substantiated crimes committed by a syndicate (Stockley, 1988, p. 299). A simplified commodity flow chart is displayed in Figure 4.

**Network Analysis** - Network analysis is the “bread and butter” of intelligence units (Martens, 1986, p. 8). It consists of dissecting the internal hierarchical structure, management, and roles of individuals within criminal organizations in order to arrive at a complete picture of an organized crime group. In addition, network analysis develops and lays out the linkages, associations, and interactions of all known members of an organized crime group with the other organized crime groups and operations in the jurisdiction and elsewhere. The connections between and interaction of individuals and organized crime groups is referred to as the criminal network (Lupsha, 1980; Ianni and Reuss-Ianni, 1990; Sparrow, 1992).

Link charting is a technique which graphically displays the known or potential relationships and/or links between subject(s). An example of a link chart is seen in Figure 5.

**Financial Analysis** - Analysis is used to assess the financial affairs of a subject involved in illegal activity. A financial analysis may involve using fundamental accounting techniques such as balance sheets and income statements. One purpose of a financial analysis is the determination of a net worth statement which attempts to identify the illegal earnings of an individual by demonstrating the discrepancy between legitimate earnings and net worth. This technique is particularly useful for proceeds of crime and money laundering investigations (Sommers, 1986, p. 28). In addition to net worth analysis, check analysis and business record analyses are important types of financial analysis (Peterson, 1990, p. 36).

**Content Analysis** - Content analysis is used in the course of reviewing written or oral information which requires some summarization, interpretation, comparison, and conclusion drawing. It may be performed on transcripts, testimony, written documents, periodicals, or books (Peterson, 1990, p. 36).

**Crime Analysis Composite Table** - A crime analysis composite table is produced by breaking down incident data into its elements and then performing frequency distribution analysis in reference to those elements. The incidents are reviewed for what elements are common to the particular type of data being treated. Common crime analysis elements include date, location, violator data, victim data, method of operation, use of weapons, etc. The information is placed into a composite table for easy review and analysis. An example can be seen in Figure 7.

**Suspect Chart** - A suspect chart may be used to compare the possible suspects in an investigation. It can include the names of the suspects, potential motives, and their opportunities to commit the crime. It facilitates comparison among the suspects by arranging the data into a simple format (Peterson, 1990, p. 38). A suspect chart can be used to identify an individual (e.g., in the case of a homicide or robbery), or criminal organizations in cases such as large-scale importation and trafficking of drugs.

**STAGE SIX: ASSESSMENT OF ANALYTICAL RIGOR AND VALUE**

Once the analysis stage has been completed and prior to the dissemination of intelligence to investigators or management, the intelligence estimate must be scrutinized and verified for the rigor of its analysis and its analytical value (i.e., that it meets the tactical and strategic intelligence needs of investigators and management). This type of scrutiny should be performed by intelligence unit management or a senior analyst.

Analytical products are assessed to ensure that only accurate, well-written, thoughtful, and meaningful intelligence flows to management or investigators. If there were little rigor used in the analysis, the value of the assessment would be greatly compromised. It would be of little utility to, or would not be used by, police management. Worse, an inaccurate assessment may result in misdirected or erroneous policies and investigations.

In assessing the analytical rigor and value of strategic intelligence assessments, the following criteria should be used:

- To what extent was the past understood? Are present trends discerned and their significance noted?
- To what extent is the present state understood? Are present trends discerned and their significance noted?
- To what extent are future trends, particularly those that can simply be extrapolated from the past and present, logically and consistently derived?
- To what extent has there been an attempt to look for the new or unusual, which will bear significantly on future trends?
- Is the estimate interdisciplinary in the sense that a comprehensive approach to all kinds of evidence—political, economic, cultural, and social—is attempted?
- If future trends were accurately identified and their direction adequately perceived, were predictions made? And however
imprecise, how accurate were those predictions? (Sullivan, 1980, pp 50-51)

If the intelligence information does not directly address the needs of the client or there is some doubt as to the analytical rigor used, the analysis or presentation of the intelligence estimate must be revised.

**STAGE SEVEN: DISSEMINATION**

Once the information is analyzed, it is disseminated to the client. The client can be one of many different users including individual investigators, prosecutors, management and other police or government agencies.

The manner in which intelligence information is presented when disseminated is critical. Intelligence should be disseminated in a report or assessment which should be a logically structured product embodying strong writing skills (McDowell, Wardlaw, and Schmidt, 1991, p. 18). The report should be concise, while encompassing a thorough analysis of the issues and ensuring that all the details which either support or refute a particular hypothesis or argument are included. An intelligence report must be as objective as possible to encourage decisions which are based on accurate information and sound analysis. The report must distinguish between verified information and hypotheses, hearsay, or inferences. The writing style should be clear, avoiding “bureaucratic jargon” when possible. All sources of information should be noted in the report (Dintino and Martens, 1983, p. 128). It is also important that there be liberal use of analytical models and charting techniques in the report.

The format and content of the report should cater to the interests and specific needs of the intended recipient (Wolf, 1978, p 28). To this end, specific assessments (threat assessment, market analysis, etc.) can form the framework and substance for specific intelligence reports. Emphasis should not be placed on producing quantity, but producing quality on which cases can be built and strategic plans made. Reports must be disseminated to clients in a timely manner.

There are three types of intelligence reports: strategic (the result of the interpretation of certain data indicating general background information, trends, patterns, forecasts, or possible courses of action), tactical (pertaining to a specific event or situation which requires immediate or future action by a police department); and informational (intelligence which is not immediately relevant to a tactical or strategic project but which is to be retained in a file for future reference) (Wolf, 1978, p. 28).

Dintino and Martens suggest that a preliminary tactical assessment include:

1) Abstract of findings
2) Historical overview of the criminal organization

Source: Peterson, 1990, p 32
Figure Four: Flow Chart of Gary Hendin Money Laundering Operation

Legend

Legend

Flow of Illicit Money

Source: Beare and Schnieder, 1990, p. 318
Figure Five: Sun Yee On Triad

Heung Chin, Founder
(Deceased)

Heung Wah Yim
Dragon Head
(Convicted of triad crimes in 1987 in Hong Kong) (1)

Kong Kwai Wing
Incense Master
(Convicted of triad crimes in 1987 in Hong Kong) (1)

Cheung Yan Lung
Legislative Councilor
Father of Cheung Leung Sing

Thomas Heung
aka Heung Wah Wing

Andy Heung
aka Heung Wah Kwok

Francie Heung
aka Heung Wah Boor
(Convicted of gambling fraud in US in 1989)

Benny Heung
aka Heung Kwong

Heung Wah
Mah

Heung Wah
Kwai

Jimmy Heung
aka Heung Wah Shing

Charlie Heung
aka Heung Wah Keung
(Convicted of triad crimes in 1987 in Hong Kong) (1)

Edmund Cheung
aka Cheung Leung Sing

Son of Cheung Yan Lung
(Convicted of triad crimes in 1987 in Hong Kong) (1)

Lee Cheung On

Vong Cheong Ying
aka Wong Chun
Thailand/Vietnam
(Fugitive from US extradition request related to heroin smuggling)

Lee Man Yung
Australia

Ma Tak

Ah Lun
Australia

Eddie Chan
aka Chan Ka Ho
Australia

Vincent Lew
Former Leader
Wah Ching Gang
San Francisco
(Fled to Far East)

Clifford Wong
aka Wong Chi Pai
Tung On Tong
President
New York

Tony Young
aka "Sweet Plum"
Current Leader
Wah Ching Gang
Los Angeles

Steven Wong
aka Wong Chi Keung
aka "Tiger Boy"
Tung On Gang
(Convicted of heroin trafficking, 1990)

Chen Kai
Chan Kin Chung
Chan Man Kwon
Pang Chi Sum
Wong Ko
Wong Yan
Ng Kam Lau

Other office bearers convicted of triad crimes in 1987 in Hong Kong. (1)

Prepared by: United States Senate Permanent Subcommittee on Investigations

(1) Reversed on appeal.
A final tactical assessment should reflect the results of the intelligence assessment/investigation and the impact upon the problem, and it should recommend future policy/strategy alternatives (Dintino and Martens, 1983, p. 129).

The following report format is suggested when presenting a strategic assessment:

I. Executive Summary
   A. Objectives of Assessment
   B. Problem definition/hypothesis
   C. Research methodology/collection plan
   D. Scope and limitations of new assessments
   E. Review of previous assessments/Literature review

4) Network analysis
6) Indicators of corruption or violence
8) Vulnerability assessment
III. Analysis
   A. Introduction: scope of analysis/analytical methods used
   B. Description of findings
   C. Analysis of findings

IV. Conclusions/Recommendations
   A. Conclusions
   B. Policy/Enforcement Alternatives
   C. Recommended Policy/Enforcement options
   D. Prediction of policy implications (on enforcement target and police resources)

V. References
   A. Primary sources (informants, data bases, investigators, etc).
   B. Secondary sources (newspapers, magazines, other intelligence assessments, etc.)

Notwithstanding these standardized report formats, intelligence personnel must always explore ways to deliver their product in a form that will be most useful to the purpose or situation at hand. In addition to written reports, oral reports must also be well-structured and delivered using effective briefing techniques (McDowell, Wardlaw, and Schmidt, 1991, p. 18).

Prior to dissemination, the intelligence unit administrator should review the report to ensure that: 1) the information contained is reliable and accurate; 2) it does not divulge the identity of a source of information if confidential; 3) it is consistent with unit and agency guidelines; 4) it is legally permitted (or not prohibited by law); 5) it has been properly classified; and 6) it is appropriately recorded (Dintino and Martens, 1983, p. 130).

To effectively control and standardize the process of safeguarding and disseminating intelligence information, a sensitivity classification system should be adopted for all intelligence reports and documents. When possible, the time frame for the sensitivity code should be indicated. A date should be determined when the original sensitivity classification would no longer be binding as in an active or pending investigation. A Security Control Officer should advise and represent the Commanding Officer of the agency about safeguarding all classified information; recommend procedures for the proper instruction of all persons who are to handle classified material; maintain a program for declassification, downgrading and destruction; and supervising or conducting security inspections and spot checks to insure compliance with the procedures (Wolf, 1978, pp. 20-22.)
Beyond the immediate client for whom the report is being prepared, two concepts should guide an intelligence unit in its dissemination of intelligence to other units of its police department or to other agencies: "right to know" and "need to know." These two criteria ensure that only those who possess the legal right to intelligence and demonstrate a need for this intelligence are allowed to get it (Dintino and Martens, 1983, p. 130). Further, all of the following factors should be kept in mind when evaluating requests for intelligence from members of the department or external agencies: 1) the nature of the information; 2) the source of the information; 3) classification of the information; 4) the rank, assignment, and identity of the members of the department requesting the information; and 5) reason for the request and nature of the investigation being conducted by the requesting member of the department (Wolf, 1978, p. 30).

### Stage Eight: Application of Intelligence

This stage involves the use of the intelligence by investigators and police management. It is the stage where the intelligence is applied for investigative, operational, or management purposes.

The intelligence unit should monitor the application of intelligence. It must ensure that the intelligence estimates are thoroughly understood and applied to the objectives, investigations, and strategic plans to best maximize the value of the information. Ideally, in the case of tactical intelligence, an analyst should be working actively with investigators, thereby allowing for advice and the monitoring of the application of intelligence. There must be constant feedback between those who use the intelligence and the analyst and intelligence unit manager.

### Stage Nine: Review/Evaluation

The final stage of the criminal intelligence process is the review. This stage can be either the review and evaluation of a specific intelligence project or the periodic review and evaluation of the general criminal intelligence function of the police agency.

Through a credible evaluation, an intelligence unit is able to determine if it is accomplishing its objectives and identify its strengths and weaknesses. The outcome of an evaluation is the ability to continuously update an intelligence unit's operational and procedural requirements. If the unit is found to be deficient or operating inefficiently, the unit administrator will be able to address these deficiencies and redirect resources towards more productive and cost-efficient programs (Dintino and Martens, 1983, pp. 131-132).

Following the completion of a specific intelligence project, including the dissemination and application of intelligence to an investigation, strategic policy, or prosecution, a review is appropriate in order to determine if it met the tactical and strategic objectives of the investigator, manager, or prosecutor as well as the overall effectiveness of the intelligence process. To this end, the intelligence unit should develop a systematic mechanism to automatically review and evaluate an intelligence cycle.

A review often entails an assessment of the results of the intelligence project against the parameters of the original task. Strategic intelligence cannot be measured by the traditional "body count" such as number of arrests, number of successful prosecutions, etc. Rather, police management should think in terms of capability, for example, testing the ability of the system to produce analyses with a minimum of file-search time. The evaluation may analyze the operation in terms of its ability to detect new operations of the organized criminal before they start or before anybody else detects them. This is difficult, but the function of intelligence is to warn of new developments and to suggest areas where organized crime groups might turn next (Harris, 1976, p. 133). In short, the proof of a strategic assessment's worth lies in its ability to predict the future (Peterson, 1991-92, p. 27) and as such, it should be evaluated accordingly.

In addition to the evaluation of specific intelligence projects, a continual review of the effectiveness of the intelligence function and operation must be exercised (Wolf, 1978, p. 15). The evaluation should be a formal, directed, self-examination of the successes, failures, and general operation of the unit. It should result in a report on gains and losses, and suggestions for improvement. This evaluation report should be reviewed and steps taken to address the weaknesses in the intelligence function (Harris, 1976, pp. 133-134).

The continuous self-evaluation program could include monthly meetings where the unit commander discusses various issues with all personnel, for instance: Does the unit know more about crime activities and threats to public order in its area of jurisdiction than it did a month ago? If the answer is yes, then: What has been learned? How was it learned? Could more have been learned by better approaches? What is being done to exploit the gain in knowledge? If it was strategic intelligence, can some specific cases be developed? Should there be a shift in the investigative effort? If the answer is no, then why not? Are analyses failing to keep track of activities of major criminals? Are investigators focused only on low-level operations? Are there reports of rumors of organized crime activities or other subversive elements that the unit itself has no other information about? What has been done to check out the rumors? What developments in major crime have been reported by neighboring (or other) jurisdictions? Have persons on patrol been responsive to the unit's request for information? Have the reports been followed up? Has the filing system been responsive to questions directed to it? Have there been questions that have not been answered because of the filing system? Have analysts noted the need for other categories? For more extensive cross-filing? Have the consumers been queried as to the usefulness and the material being on target? Have there been any leaks? What questions should be asked next month (Harris, 1976, pp. 133-134)?

The choice of an evaluator is also critical. Hansen suggests that responsibilities for an external audit may be entrusted to a local prosecutor and/or delegated from a legislative body serving as an oversight committee (1977, p. 3). Whether an evaluation is carried out by an external auditor or from within the police agency, the auditor must: 1) be independent of command influence; 2) possess the skills and expertise to perform valid, reliable, and fair in-house evaluations; and 3) be required to submit a detailed report to the agency.
administrator (Dintino and Martens, 1983, p. 149). Finally, there is a need for a level of freedom for the intelligence unit to develop and conduct its assessment activities separated from pressures related to information collection activities or operational urgencies that occur in existing law enforcement agencies (McDowell, 1991).

ORGANIZATIONAL/ENVIRONMENTAL FACTORS

Organizational and environmental factors critically impact upon the criminal intelligence function. Indeed, Reuter contends that the failure of law enforcement to come to terms with the need for intelligence is a direct reflection of the inadequacies of the police environment (1983, p. 186). The following environmental and organizational factors are considered: intelligence unit structure, management, resources, analyst recruitment and training, investigator/analyst relationship, technology, ethical standards, jurisdictional issues, legal environment, and support programs.

Intelligence Unit Structure

The intelligence unit should be a staff organization situated so the unit commander reports directly to the agency head (Godfrey and Harris, 1971). An example of the internal structure of an intelligence unit is provided by Prunckun (1990) and shown in Figure 8. Within each of the tactical intelligence teams there should be a project manager (an analyst), two to three intelligence officers (information gatherers), one or two intelligence analysts, and a data processing operator. Several tactical intelligence teams, each focused on different targets or subject areas, would be under the direction of a Chief Project Officer (a senior analyst). The Strategic Intelligence Team, which would be responsible for taking tactical intelligence and converting it for strategic purposes, would also report to the Chief Project Officer. The Chief Project Officer would report to the Director of the Intelligence Unit. The Assistant Director would be responsible for the Intelligence Support Group which, in turn, is responsible for coordinating all aspects of data collection (including equipment, securing warrants, etc). Finally, the Information Manager would have the overall responsibility for the unit’s data base and computer systems (Prunckun, 1990, p. 21).

Contrary to Prunckun’s compartmentalization of the analysis function into strategic and tactical teams, Wolf (1978) argues that the basis of organization for intelligence operations should be exclusively by the subject area (e.g., drugs, gambling, organized crime group, etc.) and not the eventual use of the intelligence itself (i.e., tactical or strategic). In other words, intelligence teams would be responsible for both tactical and strategic intelligence.

Notwithstanding the important debate surrounding the structure and organization of the intelligence unit, whether teams are organized along subject areas, strategic, or tactical purposes, or both, there must be links established across each of the subject areas or teams. Finally, the essential objective of the unit organization is to ensure that the intelligence process is executed with the utmost effectiveness and efficiency.

Other issues which are central to the structure and operation of an intelligence unit include an effective command structure, the control of information security (Godfrey and Harris, 1971, pp. 92-106), systems support and maintenance, a logical division of labor to expedite collection and analysis, and adequate administrative and logistical support (Prunckun, 1990, pp. 7-8).

Police Management

Police management, including intelligence unit supervisors, operational managers, and police agency executives, represents a pivotal force in determining the effectiveness of the criminal intelligence function. It is up to the policy management to create an environment conducive to the maximum effectiveness of the criminal intelligence function. The intelligence function must be legitimized within the organization in such a way that it has an obvious mandate to call upon organizational resources to gather and process information in pursuit of meeting the needs and expectations of its clients.

Police management must demonstrate a willingness and a commitment to have intelligence guide them in their decision-making process and in policy making, especially in resource management and strategic planning (McDowell, Wardlaw, and Schmidt, 1991, p. 20). Among senior management, the intelligence function should be accorded equal parity in the development and implementation of organized crime control policy and strategy (Dintino and Martens, 1983, p. 77).

Police managers must not only provide adequate physical and financial resources, but perhaps of greater importance, intellectual rigor (Martens, 1987, p. 131). There must be an environment that encourages the intelligence officer’s imagination, creativity, and persistence (McDowell, Wardlaw, and Schmidt, 1991, p. 20). It is the responsibility of the intelligence unit supervisor to develop an environment which places greater incentives upon the skills for acquiring knowledge than the skills for acquiring arrests (Dintino and Martens, 1983, p. 67).

Managers must be sensitive to the dynamics of the process, know the correct questions to ask, and acquire an appreciation for the need to base enforcement policy and practice on empirically-supported assessments and studies (Martens, 1987, p. 146). An intelligence unit supervisor must demonstrate a willingness to use intelligence as a reflective and critical questioning tool even when the process challenges or refutes traditional police wisdom or existing policy (Dintino and Martens, 1983, p. 138). It is also the manager’s role to ensure that awareness of corporate activities (relevant to the intelligence topic) is communicated to the intelligence officers.
and efficiency, police management must seek to minimize the bureaucratic, operational, and authoritarian constraints that are prevalent in other phases of policing (Martens, 1987, p. 138).

It is also the responsibility of the unit supervisor to construct standards and goals for intelligence units. Standards relate to the level of expertise, thoroughness, and professionalism used in the execution of all intelligence duties as well as the overall operation of the unit. They also relate specifically to ethical standards which an intelligence unit must uphold when carrying out their highly intrusive activities. (For more detail on ethical standards, see below.) While these standards may be brief, they must be substantive, clearly articulated to unit staff, and assurances must be made that both the individual and the unit as a whole are committed to them. The unit supervisor also has responsibility for formulating goals and objectives for the unit and the intelligence function in general. These goals should be expressed in clearly-defined terms and should be articulated to all staff. They relate to both the achievement of standards, as well as specific products or output. These goals and objectives should be formulated in collaboration with unit personnel, senior police management, and the clients of the intelligence.

In short, with respect to the criminal intelligence function, it is the responsibility of police management to: 1) channel police discretion in accordance with the real threat to society; 2) minimize the unnecessary intrusion of personal privacy through intelligence gathering; 3) provide for meaningful enforcement strategies and realistic policy; 4) set rigorous standards and provide a measurable indicator of success; 5) legitimize the intelligence function in a liberal democracy; 6) be proactive—operate not merely on a case by case

Figure Eight: Internal Structure of an Intelligence Unit

working on the project (McDowell, Wardlaw, and Schmidt, 1991, p. 21). For an intelligence unit to attain its maximum level of effectiveness basis, but in the long term; 7) generate intense critical dialog in a nonthreatening, constructive manner; 8) consistently challenge the accepted, obvious, or known, and 9) reward the free exchange of ideas (Dintino and Martens, 1983).

**Resources**

Worthwhile intelligence cannot be produced without a cost. The overall cost associated with intelligence work is potentially quite extensive and may include (but is not limited to):

- human resources
- training and development
- equipment
- administrative funds
- time
- information collection mechanisms
- dissemination and reporting resources

(McDowell, 1991, n.p.).

One of the most important organizational requisites for a successful intelligence function is that sufficient resources be dedicated to an intelligence unit in order for it to operate effectively. However, in this age of shrinking police budgets, it is often unrealistic for the management of intelligence units to expect a full complement of resources.

Because of limited resources, an intelligence unit must be able to prioritize. In arriving at a cost-beneficial approach to resource allocation, the unit supervisor must incorporate a number of variables. Dintino and Martens formulate some preliminary inquiries that will permit the administrator to arrive at a prudent decision with respect to allocating the unit’s resources:

- What is the tentative scope and dimension of the problem to be assessed?
- What resources are currently available to address the problem?
- Are the priorities established consistent with those of the organization?
- What are the apparent social, political, and/or economic implications of the problem?
- What will be the projected impact upon the problem? (1983, pp. 73-75).

**Analyst Recruitment and Training**

The most important resource of an intelligence unit is the analyst who is the backbone of the criminal intelligence process. Staffing the intelligence unit is critical to an effective intelligence function. The objective of the staffing process is to create a unit of specialized, critically-thinking analysts and develop a career corps of trained intelligence analysts. The ethos that any police officer can perform any police task is not applicable to intelligence work. Specialists are an inevitable by-product of advancing knowledge, and as our knowledge of organized crime grows, it is imperative that there be a cadre of intelligence specialists that remains knowledgeable (Martens, 1987, p. 146).

There should be selection criteria for each category of intelligence professional within the intelligence unit. Arbitrary or subjective criteria for the selection of staff must be avoided and policies centering around arguments like "we have always done it this way" must be examined closely (Prunckun, 1990, p. 8).

Recruitment of analysts preferably should come from: 1) experienced intelligence personnel; 2) university graduates; and 3) enforcement personnel (McDowell, Wardlaw, and Schmidt, 1991, p. 24). The unit must recruit a staff with a diverse range of background, including technical, social scientific, computer, police operational experience, etc. The unit must have a mix of both police and civilian personnel. Emphasis should be placed on recruiting police personnel with operational experience in the issue area, while civilian recruits should have university degrees (at the graduate level) with strong research backgrounds.

Analysts must be well versed in organized crime theory, research methodology, and policy analysis (Martens, 1987, p. 146). Most importantly, whether an analyst has a policing or an academic background, and regardless of academic background, it is essential that intelligence officers have highly developed analytical skills. An analyst must be able to apply sound judgements in the development of conclusions leading to the outcomes of the activity (McDowell, 1991, p. 23). Analysts must also have an imaginative and creative approach to developing working hypotheses, plus the ability to see issues in a wide context.

The ability to fill these skill levels should be foremost in an agency’s search for suitable applicants. The characteristics of a good criminal intelligence analyst do not necessarily center around law enforcement conditions per se, but analytical ability and communications skills (Prunckun, 1990, p. 8). For example, Frost (1985) puts forward the following list of necessary attributes essential for a criminal analyst:

**Background Factors**

- broad range of interests
- developed research ability
- previous experience helpful to issue area

**Mental Traits**

- intellectual curiosity
- rapid assimilation of information
- keen recall of information
- tenacity
- willingness and capacity to make judgements
In addition to recruiting qualified candidates, there should also be comprehensive training programs specific to the criminal intelligence analysis field. The training of personnel for criminal intelligence is a highly specialized undertaking. These training courses should be a prerequisite for the issuing of a certification requirement necessary for all law enforcement intelligence analysis positions. A certification program should be offered nationally and encompass national standards. Analysts should be required to have completed a certified intelligence training course and be certified as bona fide intelligence analysts prior to being employed in an intelligence unit. These courses should impart the conceptual, technical, and operational skills required of analysts (Peterson and Ridgeway, 1990, p. 16). In addition to the initial certification programs, there must also be an ongoing comprehensive training and education program in place for analysts, supervisors, and mid-level managers. These programs must be offered in-house as well as externally and offer training and education in the latest intelligence issues and techniques. Peterson and Ridgeway provided a listing of courses offered throughout North America (1990).

Training should also be made available to patrol officers and police management. The former should emphasize a better understanding of what the intelligence process is and where the inputs of non-intelligence officers can be inserted in the process. Training of patrol officers is especially critical in those forces which emphasize community-oriented policing. For police management, the main objective should be to demonstrate what intelligence can do for management and what assets the intelligence unit should have at its disposal to do the necessary job of strategic support for decision-makers (Godfrey and Harris, 1971, p. 74).

Finally, it is argued that the analytical component of a police agency should not be integrated into the traditional promotional structure of the agency. Promotional incentives for analysts should be distinct from those for other personnel (Dintino and Martens, 1983, p. 127).

In sum, the recruitment of candidates for analyst positions requires a sensible balance between knowledgeable, experienced, enforcement practitioners and others outside of the enforcement field who demonstrate the potential to bring intelligence and analytical professionalism into the craft. In any case, both groups ultimately need further development; the former needing advanced analytical training, and the latter requiring familiarization across the enforcement arena. As such, according to McDowell, Wardlaw, and Schmidt, the ultimate answer rests with providing training and development opportunities within the intelligence community (1991, p. 25).

Investigator/Analyst Relationship

The relationship between the criminal investigator and the intelligence analyst is critical for all stages of the criminal intelligence process, particularly in the context of tactical intelligence and criminal investigations. There must be a close, reciprocal relationship between the intelligence analyst and the operational unit, in particular the criminal investigator. It is important that management encourage interaction and ongoing dialog between intelligence analysts and operational personnel (Dintino and Martens, 1983, pp. 124-125). While the analyst may be able to develop suggested avenues of investigation and research, it often requires the services of a trained investigator to obtain information (Godfrey and Harris, 1971, p. 27). If a separate position is used for the collection of information (i.e., an intelligence officer), this individual must also be included in this close working relationship.

It has often been recommended that the operational unit include the analyst (and intelligence officer), in some form or another, in the active investigation. The most effective use of a tactical analyst is to have the analyst actually participate in data collection or the investigation as it develops. The data generated in the course of information gathering or an investigation is managed by the analyst, who monitors all the reports, subpoenaed records, laboratory analyses, and the like. Analyses are created as needed for the investigators charged with maintaining up-to-date case overviews (Sommers, 1986, p. 31).

Using the investigator-analyst relationship as a basis for maximizing an effective tactical intelligence system, Metzdorff recommends the "Module Concept." This system of intelligence processing goes one step beyond Prunckun's intelligence team and is premised on the analysts and investigators working together as a regular unit (1975, pp. 52-53). This unit could potentially even go beyond a simple analyst-investigator relationship to one which encompasses an analyst, an intelligence officer (information gatherer), a criminal investigator, and a prosecutor.

It is essential that the client of the intelligence unit articulate the requirements clearly in terms that identify the subject and scope for intelligence examination, at the same time indicating the use to which the intelligence assessment is expected to be applied. Both the client and the intelligence staff need to discuss and negotiate the issue (McDowell, Wardlaw and Schmidt, 1991, p. 12). Ways have to be found to orient the users of intelligence to convey their needs effectively to intelligence units and to orient their own staffs in the uses of intelligence information (Edelhertz, Cole, and Berk, 1984, p. 43). However, rather than merely wait for inquiries from an investigative unit, the intelligence unit must anticipate and ultimately direct the investigator and the course of the investigation (Martens, 1987, p. 132).
Technology

Computer technology is increasingly proving to be invaluable for criminal intelligence collection and analysis. Police departments utilize both personal computers and mainframes and a vast array of software which is both easily accessible and user-friendly. This software should run the gamut from databases, spreadsheets, word processing, statistical analysis, graphics packages, and those more specifically suited to intelligence needs such as artificial intelligence programs. These computer systems must also maximize the ability of intelligence units to collect information from many different on-line information services, electronic Bulletin Board services, and government data bases (e.g., motor vehicle registry).

One of the most productive uses of computers in intelligence work is in the collation stage. Artificial intelligence (AI) systems are often key for criminal intelligence analysis and have proven to be an especially useful tool for identifying criminals for targeting and helping to predict criminal activity (Peterson and Ridgeway, 1990, p. 16). Computers use AI to solve problems in a way that simulates the processes of human intelligence (Reboussin and Cameron, 1989, p. 13). Experience and information of investigators and analysts should be entered into a collective repository, such as an AI system, so that unique individual knowledge can become collective, transferable knowledge. In other words, intelligence units should actively seek to have their experts state, share, and record their years of tactical insights which then would be filed for future use as an AI application (Lupsha, 1980, p. 37).

Computer software which makes the analyst more effective and efficient in presenting intelligence assessments is also important. This is especially true in creating charts and other types of graphics. Various commercial packages, generic and intelligence-specific, are available which turn the once-laborious chore associated with manually-drawn charts into an easy and efficient computer-driven application. Computer Assisted Graphics Evidence (CAGE) for example, allows the analytical staff to construct various types of visual aids more effectively. CAGE increases charting efficiency and productivity which allows analysts to meet an increased workload. The Advanced Targeting, Analysis, and Graphics System (AdTags) is a program that allows an analyst to view all significant sub-groups in a criminal organization. Morehouse (1991/92, p. 15)

There should be a capacity within the unit to constantly scan the technological market for hardware and software appropriate to its needs. However, despite the importance of computer and electronic technology for data collection and analysis, it will not take the place of the analyst (Peterson and Ridgeway, 1990, p. 16). Indeed, computer technology represents only a part of the overall analysis, emphasis must continue to be placed on the quality of the analyst (Lupsha, 1980, p. 37).

Inter-Jurisdictional Cooperation and Coordination

There are jurisdictional issues which often separate and obfuscate the necessary cooperation between all types of public and private agencies which deliver law enforcement and policing services and these hinder information sharing.

On the first level, there must be a strong foundation for cooperation between police agencies. The sharing and coordination of data and intelligence with other police forces or relevant government agencies is critical. Because organized crime and its activities are national and international in scope, there must be sophisticated, formal methods of intelligence sharing and coordination; intelligence systems cannot and must not be constrained by artificial geographic boundaries (Martens, 1991, p. 103). At the operational level, the need for inter-agency cooperation is already recognized in the large number of formal and informal joint task force operations.

There should be ways to make all intelligence units within and among police forces work together most effectively, to avoid turf dispute and unnecessary duplication of effort (Edelhertz, Cole, and Berk, 1984, p. 43). An overall sense of informal or formal cooperation between intelligence units among different police agencies must be present. The relevant agencies should be brought together on a periodic but regular basis to share, exchange, discuss, and record their intelligence, ideas, insights, strategies, etc. (Lupsha, 1980, p. 37).

Ideally, there should be a national structure which institutionalizes and facilitates the uniform collection, analysis, and dissemination of intelligence information. It must have a mandate among all police intelligence units and be viewed as the competent centralized institution with which to share raw data and intelligence. Moreover, such a national structure should be accompanied by national standards which ensure that there is a uniformity in all aspects of the criminal intelligence function, from collection, to analysis, to dissemination. To facilitate communication and input into the database, there must be standardized data elements which are followed by the operational and intelligence units of all police forces.

At another level, there is a great need for the coordination of information between all relevant agencies. This not only includes public police forces, but also private policing, government regulatory bodies, and private sector firms. The need for a greater coordination and cooperation among all these different agencies lies in the reality that organized criminal activities transcend the responsibility of police and the criminal justice system. As such, an intelligence system in particular must include information from a diverse range of sources in many different agencies in both the public and private sector.

In sum, the national coordination of intelligence information is critical to an organized crime control strategy. This coordination requires a nationally institutionalized structure with a clearly defined and unique mandate which complements the existing intelligence functions of police agencies throughout the country.
Legal Environment

The legal environment refers to laws facilitating the surveillance of suspects, the collection of information, and the application of intelligence to a criminal investigation and court proceedings. Due to the contentious nature of this area, and the myriad judicial decisions interpreting the use of information collection for law enforcement purposes, it is beyond the scope of this paper to provide a detailed explication of the ideal legal environment for this area. The most important criterion is the balancing of the individual's right to privacy against the ability of law enforcement to effectively protect the public. In its most general and simplistic form, this point of equilibrium is a legislated requirement which stipulates that prior to any type of information collection which involves surveillance, a police agency must first receive authorization from a lower court judge who, in turn, bases his/her decision for authorization on the standard of "solid ground" for suspicion. Moreover, to maximize the use of information collection for intelligence purposes, this authorization should be applicable to both evidence-gathering surveillance (i.e., for tactical investigations where police must articulate a suspected offense before an interception is made) and intelligence-gathering surveillance (i.e., where no specific crime is committed; often pejoratively referred to as a "fishing expedition").

Ethical Standards

Related to the legal environment is the internal policy of police agencies with respect to the ethics of information collection. The International Association of Chiefs of Police recommends that in order to guard against the possibility of allegations of unethical conduct, and to protect the rights of individuals not involved in criminal acts, a set of rules and standards should be adopted to deal with the recording and purging of intelligence information (1985, pp. 8-9).

In general, these guidelines urge that when an individual's associations are not criminal in nature, or criminally-related, the information should not be recorded. Likewise, in the case of organizations, unless an organization's ideology advocates criminal conduct and its members have planned, attempted, or performed such criminal conduct, it is both unnecessary and wrong to gather such information. Further, information about an individual's sexual, political, or religious activities, beliefs or opinions, or any dimension of private lifestyle should not be collected or recorded in intelligence files unless that information is material to a criminal investigation or strategic planning (Los Angeles Police Department, 1984, p. 2; Prunckun, 1990, pp. 15-16).

Hanson suggests that a police force must follow a number of steps that will lead to a public confidence in the criminal intelligence function. These are: 1) the police executive must be in charge of criminal intelligence operations, 2) every local department should adopt specific guidelines for the conduct of criminal intelligence operations; 3) a local legislative body to review and make recommendations regarding operations and policy should be encouraged; 4) an outside audit procedure, perhaps conducted by a local prosecutor or other pertinent state official, should be established; and 5) the police executive must be willing to explain to the public the nature and function of the criminal intelligence unit (1977, p 3).

Support Programs

An effective criminal intelligence function must be part of an overall organized crime enforcement strategy. Criminal intelligence certainly feeds into such a strategy, but the relationship is also reciprocal. Criminal intelligence is only successful in so far as it supports general enforcement policy and strategy. These strategies must be forged at the local, regional, and national levels. In addition to the importance of an overall organized crime control policy and strategy, there must be available specific programs which support the criminal intelligence function, particularly in the collection of information. An example of this type of support program is witness protection.

CONCLUSION

Criminal intelligence is just one part of organized crime and drug law enforcement. Its ability to serve the short and long term objectives of government organized crime control strategy is contingent upon other aspects of enforcement policy and the interaction among all enforcement functions. However, in the face of growing power, sophistication, and globalization of organized crime, juxtaposed against the limited budgets of government law enforcement agencies, the role of criminal intelligence is arguably now more important than ever. Indeed, according to Dintino and Martens:

The future of law enforcement in its role against organized crime is dependent upon intelligence. Intelligence will permit an organization to meet future challenge with an awareness and allows for the development and implementation of viable control policies. Without intelligence there is no strategy. The intelligence process is central to the development of effective organized crime control program (1981, p. 59).

In order for a criminal intelligence function of a police force to reach its true potential, management and operational personnel must bestow upon it a priority which is commensurate to its vital importance in organized crime enforcement and equivalent to the emphasis given to the operational and enforcement functions. The commitment to an effective criminal intelligence function must be accompanied by an appropriate institutional and legal environment which promotes its effectiveness. As importantly, a police force must be diligent in assuring that a criminal intelligence project encompasses all the essential stages of the intelligence process.
and that each stage is executed with the utmost professionalism and competence. The omission of or haphazard approach to any of these stages jeopardizes the true effectiveness of the intelligence function.

The resources required for an effective intelligence function must be balanced against the fiscal restraint imposed on police agencies. However, it is crucial to note that a primary purpose of intelligence, in particular strategic intelligence, is to provide the capacity to prioritize enforcement functions and allocate resources in the most effective and efficient manner possible.

Moreover, there is constantly a need for a periodic and systematic review of organized crime control policies and strategies. The intelligence process can contribute to this examination by elevating the level of dialog, refining and clarifying the goals of an organized crime program, and addressing the implications and consequences of its enforcement (Dintino and Martens, 1981, p. 64).

In sum, the need for government to address organized criminal activities is clear and convincing. Until the criminal intelligence function can realize its true potential, organized crime law enforcement will irrevocably suffer

Stephen R. Schneider worked with the Ministry of the Solicitor General of Canada between 1988 and 1993 as a researcher and policy analyst within the Drugs and Major Crimes Section. He holds a B.A. in Political Science, an M Sc. in International Economic Development and is a Ph D. candidate in the School of Community and Regional Planning at the University of British Columbia. He currently works on contract with the Canadian government participating in the evaluation of the RCMP’s Integrated Anti-Drug Profiteering Units.
Appendix - Blueprints for Assessments

Assessing Criminal Group Activity

**Section A: Past and Present**

1) Membership of group; identification and biographical data on all members of group; Length of membership in group. Note any trends such as criteria for membership, number of members.

2) Geographic data on group, headquarters, location of members, geographic range of their legal and illegal activities.

3) Hierarchy of group past and present. Is there a hierarchical structure to the group? If yes, what is it? Is there a known philosophy of current or past leaders relative to violence or criminal activities? Who appears to be rising through the ranks?

4) Criminal activities of group: all known or suspected illegal activities. Dates of criminal occurrences should be included to show possible changes or trends.

5) “Legitimate” business activities of group members: all known or suspected involvement with “legitimate” businesses including employment history, ownership of or investments in businesses, past and present. Look for hidden ownership through fronts and paper corporations. Again, look at possible trends or changes.

6) Financial health of group members: any information that shows evidence of financial condition of members or group—real estate, vehicles, travel, and other conspicuous consumption. Analyze tax and/or bank records of group leaders. Trends and changes should be noted.

7) Connections to other groups: is this group working with other criminal groups? Is the relationship between this group and another group equal, superordinate, or subordinate? Is “tribute” paid to another group? Does each group have an established territory? Have any changes occurred in these network connections?

8) Connections to the government structure: are there government agencies that regulate the general activity area in which the types of crime are being committed (police, licensing, or regulatory agencies)? Do any known connections/relationships exist between group members and persons involved in these agencies or governmental bodies, including political figures?

9) Previous work in the system: have any enforcement actions been taken against the group, either for criminal or civil violations, by any agency?

10) Has any agency conducted tactical investigative or strategic analysis on the group? If yes, what were the results?

11) What has been and is the social, economic, political, and criminal climate in the area(s) in which the group operates? Are other groups perpetrating the same criminal activities? Is there a strong enforcement presence? Is there strong community opposition to the criminal activity?

**Section B: Future**

Based on data collection under Section A, predict

1) Future group membership;

2) Future geographical impact;

3) Growth potential for the direction of the criminal activity;

4) Growth potential for “legitimate” business activity;

5) Future financial position;

6) Possible future changes in relationships with other groups;

7) Potential for future relationships with or corruption of government officials.

For each of the above, estimate the probability of the prediction.

**Section C: Enforcement Alternatives**

Based on data developed in Sections A and B, evaluate feasible alternatives and make recommendations regarding investigative actions that could be taken to prevent further growth and/or success of this group. For each alternative, indicate the probable effectiveness.

Assessing Categories of Criminal Activity

**Section A: Past and Present**

1) Statistical data, occurrences of crime over past “x” years. Trends? Changes?

2) Geographical range of criminal occurrences. Where is it the heaviest? Weakest? Have there been changes? Trends?

3) Criminal techniques used modus operandi. Are there new techniques? Is violence a key or ancillary ingredient to the crime?

4) Known relationships between this crime and any other crimes.

5) Individuals and/or groups involved in this criminal activity: is this enterprise shared by several groups, perpetrated by unconnected individuals, or part of a monopoly? Changes? Trends?
6) Connections to “legitimate” business: are businesses used as fronts for illegal activities? Are they used to launder illegal profits?

7) Financial. what is the estimated monetary value of this crime per year in this jurisdiction? Are profits rising or falling? What are the costs of doing business? Are the costs rising or falling?

8) Where do the profits go? Is there a criminal hierarchy to which a “tribute” is paid? Have there been changes in this?

9) What is the market for this criminal product? What is the size of the market in human and economic terms? Who buys or uses the product? Is the market shrinking or expanding?

10) Connections to the government structure: are there government agencies or bodies that regulate the activity area in which the crime is being committed? Are there any known or suspected connections between perpetrators and persons involved in these government agencies or bodies?

11) What has been and is the social, economic, political, and criminal climate in the area in which the crime is occurring? Is there a strong enforcement presence there?

12) Has any agency conducted an investigation, tactical or strategic analysis on this criminal activity? If yes, what were the results?

Section B: Future

Based on data developed in Section A, predict the future of this activity, including:

1) Prevalence,
2) Geographic range,
3) Impact of evolving techniques;
4) Groups taking over, if any;
5) Potential profit structure;
6) Potential government corruption hazards.

For each, estimate the probability of the prediction

Section C: Enforcement Alternatives

Based on data developed in Sections A and B, recommend alternatives regarding investigative deployment, enforcement, and other actions that could be taken to prevent further growth and/or success of this criminal activity. For each alternative, indicate a probable level of effectiveness resulting from the action (Sommers, 1986, pp. 34-37).
References


