UNODC
United Nations Office on Drugs and Crime

Criminal Intelligence

Manual for Front-line Law Enforcement

UNITED NATIONS OFFICE ON DRUGS AND CRIME
Vienna

Criminal Intelligence

Manual for Front-line Law Enforcement

UNITED NATIONS
New York, 2010

This publication has not been formally edited.

Publishing production: English, Publishing and Library Section, United Nations Office at Vienna.

Contents

1. An introduction to intelligence

FROM INFORMATION TO INTELLIGENCE

Before we can properly discuss and explore information, intelligence and analysis in theoretical and practical terms, we need to have some common understanding as to what these terms mean. Some definitions of these three key terms are as follows:

Information

- Knowledge in raw form

Intelligence

- Information that is capable of being understood
- Information with added value
- Information that has been evaluated in context to its source and reliability

Analysis (of either information or intelligence)

- The resolving or separating of a thing into its component parts
- Ascertainment of those parts
- The tracing of things to their source to discover the general principles behind them
- A table or statement of the results of this process

Understanding properly the difference between these terms and how they interact is important, however even at this early stage, these definitions point to key differences. Information is quite simply raw data of any type, whilst in contrast intelligence is data which has been worked on, given added value or significance.

INFORMATION + EVALUATION = INTELLIGENCE

The way in which this transformation is made is through evaluation, a process of considering the information with regard to its context through its source and reliability.

In its simplest form, intelligence analysis is about collecting and utilizing information, evaluating it to process it into intelligence, and then analysing that intelligence to produce products to support informed decision-making.

All these decisions involve applying our natural ability to "analyse" information, an overall process which can be usefully broken down into a series of stages, or questions we ask of ourselves, as follows:

- What exactly is the problem; what decision do we have to make and why is it significant or important?
- What information do we already have or might we reasonably obtain that could be relevant to the problem in hand. Where is it/how can we get it?
- What meaning can we extract from the information; what does it tell us about what's going on?
- Is there only one possible explanation, or are there other alternatives or options. Are some more likely than others?
- How do these affect the decision we have to make, are some options potentially better than others; do some carry greater risk of success and/or failure?
- Are we ready to take action with a reasonable level of confidence, or do we need to gather more information first? If so, what else do we need and where/how can we get it?

The process of applying these questions, evaluating the answers, and then choosing how to respond, to act, is the essence of what analysis is about.

By bringing this process under our conscious control, we can monitor it, develop and improve it, and subject it to quality checks which can be quite complicated to grasp. Beginning that development of awareness and skill is critical. The practical advantages of developing an individual's analytical skills are many, but can be summarized as follows:

ANALYSIS GOES BEYOND THE FACTS

It can tell you how good (or poor) your information/intelligence is

It can tell you things you didn't know before

It can tell you what you need to know to understand a situation

It can tell you where to look further

It can help you to communicate your understanding to others

The origins of intelligence analysis

Knowledge has the potential to be equated to power. The concept of collecting and utilizing information to support decision making in some formal, structured way is nothing new. In order to obtain advantage over adversaries, it is imperative to possess the most up-to-date, accurate information regarding amongst other things, their intentions and capabilities. This rule applies in every field, be it politics, business, military strategy, or criminal intelligence. In addition, it is a process that has always been, and still is, continually developing and evolving, in response to changes in social/cultural factors, technology, organizational needs, and new/higher levels of analytical skill.

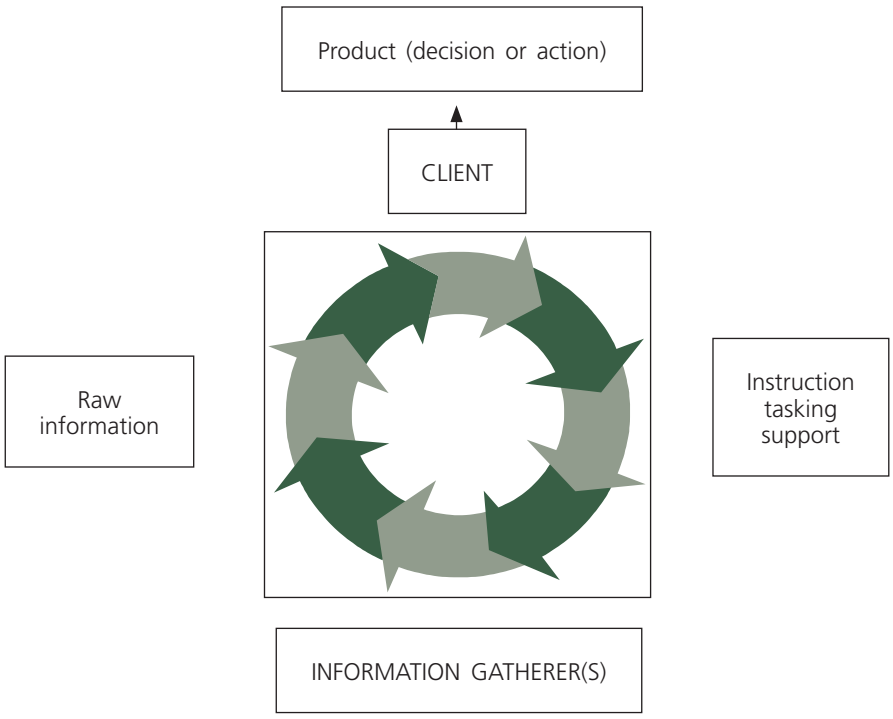
Reviewing the historical background, the "roots" of intelligence and analysis as a process and as a profession is a useful and important exercise. Raising our understanding of the origins of intelligence and analysis helps us to understand both where we are now and how/why we

arrived at this point. It also raises our awareness of how intelligence analysis is a continually changing, evolving practice, which if it is to remain relevant and useful in a practical sense constantly needs a fresh, flexible approach, new ideas, new skills, new techniques. The one constant for the professional intelligence analyst is that no two tasks or projects are ever exactly the same; every new piece of work requires a fresh approach.

There are many examples throughout history of military, religious and community leaders actively tasking individuals with information-gathering exercises and then basing their decisions on the information obtained in this way. Perhaps the earliest recognized text on the subject of information gathering and intelligence-based actions is "The Art of War, The Art of Strategy" written in the 5th Century BC by Sun Tzu, a Chinese mercenary warlord. He was renowned for his ability to command military campaigns whose success owed a lot to his effective information-gathering and intelligence-led decision-making. It says much for the quality of this work that it still remains in print today, and is essential reading for military and corporate strategists and intelligence operatives worldwide. From these early beginnings throughout history until relatively recent times, employing information-gatherers for primarily military goals has been a common trend.

What is more, a methodology arose from this process that basically involved direct contact between the information gatherer(s) and the client/decision-maker, as illustrated on figure 1-1:

Figure 1-1. Basic tasking model



This method had certain notable features:

1) The sheer logistics involved (no real technology for transport or communication) created a massive time delay between the tasking of the information gatherer, the obtaining of the information, and the delivery of the information to the "end-user".

2) Using information collectors who operated by visiting locations and witnessing events either personally or through intermediaries guaranteed that the information collected would be limited by their senses and their ability to remember accurately what they saw; such information would thus always be highly subjective, and tend towards being based on opinion rather than fact.

3) The volume of information collected in return for such a large investment of time and resources would be extremely small.

Any investigation generates vast amounts of information; the larger the enquiry, the more information the investigator has to deal with. The problem for investigators is that no matter how good the system used to store all this information, they are always limited by their own mental capacity to embrace the information as a whole, to "take it all in" at once.

This understanding of the whole of the information is crucial to valid decision-making. Fully understanding a small part of the whole information available means that in fact the investigator only has partial understanding of the whole situation.

PARTIAL UNDERSTANDING MUST INCORPORATE A DEGREE OF MISUNDERSTANDING. MISUNDERSTANDING LEADS TO POOR CONCLUSIONS.

It might reasonably be taken as some measure of the importance and value of intelligence and analysis that despite these potentially crippling limitations the process still proved to be a decisive factor in the success of military and political campaigns throughout these times.

Methods in acquiring information changed only slowly throughout history until towards the end of the last century. The massive growth in technology that began then, and still continues today, brought about what has proved to be a massive change in methods of information-gathering, which in turn created a demand for new approaches to analysis and intelligence.

This process began in the late 19th Century with the advent of telegraphy and telephony, which allowed for messages to be sent almost instantaneously over greater and greater distances. At a stroke this removed the resource and time problem that the former methods suffered through their need for the information gatherer to move between source and client. This change carried with it a number of benefits.

Firstly, the "response time" between a client asking for information and receiving the result was vastly reduced; this represented a clear benefit in that it improved the clients' ability to react quickly on the basis of such information. In addition, this development also had a knock-on benefit in that there was less time for the information source to "forget" or "lose" information whilst they were in transit, thus the quality of information also improved. Similarly, the lack of need for the information to be physically carried back to the client created a vast saving in resources; information gatherers were able to spend less time travelling/passing on information, and thus more time collecting information.

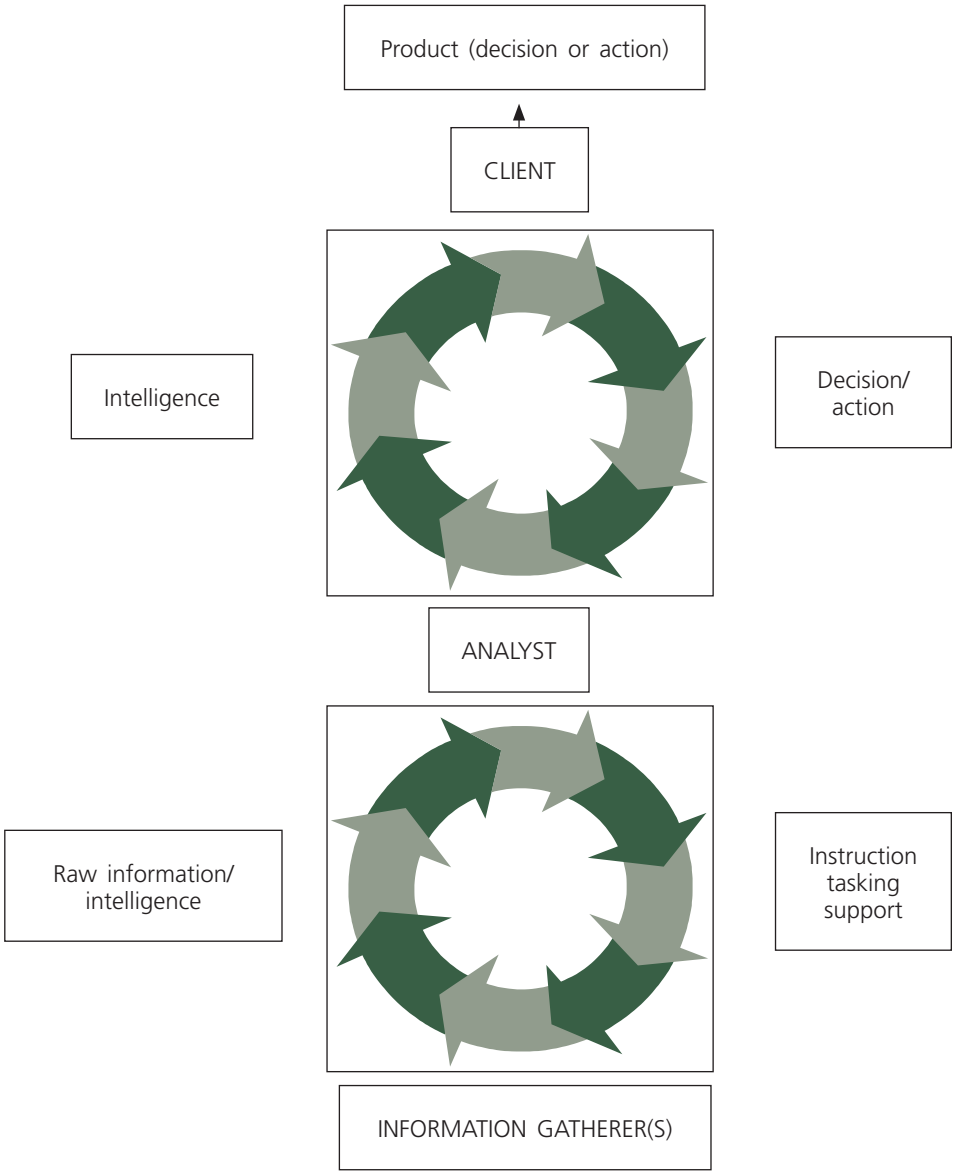
The overall result of this change was ironically that these benefits also carried with them a new problem for the client. Much larger quantities of information were gathered, far more quickly than before, and the reaction time for making decisions was reduced. In addition, controlling the process of information-gathering itself became a problem, with a new need for more emphasis on new tasks and orders for information-gatherers created as a result of their new, improved performance.

Thus where before the process involved information passing between information gatherer and client, because the new system created an information "overload", a new problem arose in that the client simply was unable to process all the information received effectively and quickly and then react to it.

The analyst

A necessity arose for the client to return to a situation that enabled speedy interpretation of information and decision-making. This created a need for an intermediate stage between the information gatherer and the client, where the bulk of the information could be received, recorded, evaluated and examined to interpret and extract meaning, before the result of this process was passed to the client. This was the origin of the function of an analyst, and the process remains in essence the same today, as illustrated on figure 1-2:[1]

Figure 1-2. Developed tasking model



[1] The analyst may be supplied with raw information or with evaluated information in the form of intelligence, or with both.

The core function of the analyst can be broken down into a three-phase process, as follows:

- To gather information, to understand it and the relevance or relationship of each piece to all of the others.
- To develop this information objectively to arrive at an understanding of the whole.
- To communicate this understanding to others and so to put the intelligence process to practical use.

The problems

As this new methodology developed, and the variety, range, and accessibility of information sources expanded, the result was that relatively speaking, the "analyst" function grew in size, number and influence. Simply put, as more information was passed back to the "centre", and more reliance placed on intelligence-led decision-making, organizations found that more and more people were required to evaluate information in order to generate, disseminate and analyse intelligence.

This ongoing situation has implications for today's intelligence units and analytical staff. The more information that is collected, the more it aids analysis and thus decision making. However it also increases the subsequent workload, which in turn forces an increase in staff and productivity or a loss of effectiveness. In simple terms the increase in information to be analysed combined with the increased need for analytical product tends to always exceed the improved efficiency that having more/better trained analysts can offer. In other words, effective, professional analytical process tends to bring more work upon itself.

Criminal intelligence analysis

What is "criminal intelligence"? To most people, including criminal investigators, the term conjures up images of collator-style systems used to store and retrieve the information we collect about crime and criminals. As the volume and variety of the information we collect has expanded, we have gradually introduced more and more complex systems to assist with its storage and retrieval. Viewed in this limited context, the introduction of information technology (IT) has been a notable success; the use of IT for the storage and retrieval of crime information is now almost second nature to the operational criminal investigator, and there is no doubt that without these tools, as a service we simply would not be able to cope with the task of recording and collating criminal information.

Collecting information in itself does not result in obtaining intelligence. Information must be properly evaluated before it can be acted upon. The value of criminal intelligence can be enhanced further by analysis. When available intelligence is too complex and large in volume for simple action, it must be analysed in order for meaningful results to be obtained.

Currently, insufficient use can be made of the information we collect on crime or criminals to develop real "criminal intelligence" , either by intelligence units themselves or by their customers, the operational criminal investigators. Even with all the new systems for storage and easy access to criminal intelligence, investigators can still fail to make real use of this invaluable resource other than as a "ready reference" to the facts unless they properly evaluate this information and use analysts to analyse the intelligence that this process produces.

Criminal intelligence analysis (CIA) is a philosophy which sets out how we can approach the investigation of crime and criminals by using the intelligence and information that we have collected concerning them. It provides techniques that structure our natural deductive powers and thought processes, the "natural intuition", which proficient investigators use subconsciously all the time. It also provides tools that help us to understand the information we collect, and to communicate that understanding to others.

The way forward

The criminal intelligence analyst is every bit as much an investigator of crime as the operational investigator. The key to CIA being of value as an operational tool is that the results of analysis have to be of direct value to the investigation. It follows then that the best results can only be achieved when the analyst and investigator work together in partnership, integral parts of the same team.

In the same way, the analyst and detective need to share many of the same skills needed to be good criminal investigators. The basic problem for intelligence analysts is putting intelligence and information together in an organized way so that the difficult task of extracting meaning from the assembled information is made easier. Only when the proper explanation of what the original information means has been derived can this intelligence be put to practical use. The techniques and systems embodied in this manual are practical tools, which can be of value in any investigation.

Intelligence analysis and organized crime

The advent of criminal intelligence analysis is directly linked to the transformation of individual crime into organized or group crime. The effective use of intelligence is crucial to a law enforcement agency's ability to combat criminal groups. Intelligence analysis also provides the agency with the knowledge required for effective management of its resources. With appropriate tasking, the products of intelligence analysis can assist in developing strategic plans to tackle current problems and prepare for future anticipated ones.

Criminal intelligence analysis permits law enforcement authorities to establish a pro-active response to crime. It enables them to identify and understand criminal groups operating in their areas. Once criminal groups are identified and their habits known, law enforcement authorities may begin to assess current trends in crime to forecast, and to hamper the development of perceived future criminal activities. Intelligence provides the knowledge on which to base decisions and select appropriate targets for investigation. While the use of criminal intelligence analysis is appropriate to support investigations, surveillance operations and the prosecution of cases, it also provides law enforcement agencies with the ability to effectively manage resources, budget, and meet their responsibility for crime prevention.

At the dawn of the last century, "organized crime" was synonymous with the Cosa Nostra. The picture of organized crime today is quite different. Many of the new criminal groups, with well-developed organizational structures, are established for obtaining power and wealth. These groups include outlaw motorcycle gangs, Russian organized crime, Asian organized crime, African organized crime, drug cartels and a myriad of street gangs—Asian, Korean, Hispanic, black, white supremacy, to name just a few. Levels of complexity are increasing even further with fluid almost structure-less networks evolving, such as West African criminal networks. It should be noted that cooperation between different organized crime groups and networks is commonplace.

Criminal groups continue to be involved in ventures such as trafficking in human beings, drug trafficking, extortion, fraud and murder. Some are now moving into new criminal enterprises such as high-technology crime. The explosion of Internet resources in the last few years has opened new opportunities for financial gain for criminals. This escalation of high-technology crime is a challenging and relatively new arena for law enforcement.

Criminal organizations are more sophisticated and dynamic than ever before. The challenge for law enforcement is to be prepared for this increasing sophistication in order to reduce the impact of criminal activities on our communities.

In order to accomplish this, law enforcement agencies need forward looking, assertive, and comprehensive strategies to counteract the threat of organized crime groups. Criminal intelligence analysis, when tasked and used effectively, can be a major asset in the law enforcement arsenal. Countries with greater experience within criminal intelligence, such as the United Kingdom, have developed national intelligence models to help standardize how criminal intelligence is used.

Information technology is very much key to intelligence sharing. Particularly in this age of sophisticated multinational crime, including terrorism, a failure to share intelligence and information effectively limits the efforts of all states in combating it.

2. The intelligence process

INTELLIGENCE

The word intelligence can be used to describe the process of interpreting information to give it a meaning. It has also been used to describe a group or department that gathers or deals with such information or to describe the product of such activity or department. At its simplest, intelligence might be described as processed information. Narrowed down to law enforcement use, "intelligence" could be described as information that is acquired, exploited and protected by the activities of law enforcement institutions to decide upon and support criminal investigations.

INTELLIGENCE: KNOWLEDGE (PROCESSED INFORMATION) DESIGNED FOR ACTION

Intelligence always involves a degree of interpretation resulting in an inevitable degree of speculation and risk. The amount of speculation and risk is dependent upon the quality and quantity of information. Intelligence is usually divided in two main areas:

Strategic intelligence: Focuses on the long-term aims of law enforcement agencies. It typically reviews current and emerging trends changes in the crime environment, threats to public safety and order, opportunities for controlling action and the development of counter programmes and likely avenues for change to policies, programmes and legislation.

Operational intelligence: Typically provides an investigative team with hypotheses and inferences concerning specific elements of illegal operations of any sort. These will include hypotheses and inferences about specific criminal networks, individuals or groups involved in unlawful activities, discussing their methods, capabilities, vulnerabilities, limitations and intentions that could be used for effective law enforcement action.

A good knowledge of operational intelligence is a highly recommended prerequisite to developing strategic intelligence capability. The development of operational intelligence in itself will provide an important source of intelligence to consider from a strategic perspective.

INTELLIGENCE VS EVIDENCE

It is important to emphasize that a state's national legislation will dictate the way intelligence can be used for law enforcement purposes. The process of intelligence gathering in relation to a specific investigation is usually a prelude to any evidence gathering phase. Legislation will also dictate whether intelligence material gathered during the course of an investigation is protected from disclosure in criminal proceedings

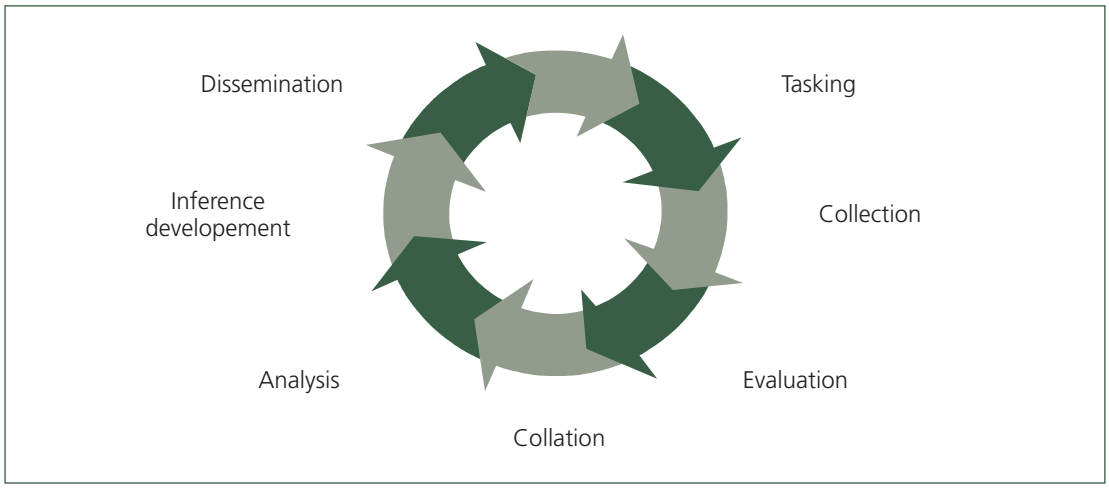
EVIDENCE: DATA FROM WHICH TO ESTABLISH PROOF

This part of the investigation responds to reported events and explains what took place and who was involved. Intelligence analysis aids investigations by helping to target available resources and identifying information gaps to focus the investigation more clearly. It also helps to avoid duplication of effort and prevent straying into areas of no relevance. To obtain maximum benefit, an analysis capacity should be employed at the earliest possible stage of an enquiry, preferably at the beginning, although, logistically this is not always possible.

THE INTELLIGENCE CYCLE

The concept of the intelligence cycle is broadly recognized as the foundation of the intelligence analysis process, at both operational and strategic levels.

Figure 2-1. The intelligence cycle



Direction/tasking

Intelligence analysis is driven by the needs of clients, i.e. consumers of the analytical product. The analytical effort is thus often directed through tasking by these clients. They take the initiative at this stage of the cycle, but the principle of partnership requires that both they and the providers share a responsibility for working together to ensure that the requirements for the analytical product are clearly defined and understood by both sides.

The initial questions that have to be asked are:

- Who tasks?
- How do they task?
- Why do they task?
- What tasks are set?

In general these questions will be answered within the environment in which the analyst sits and therefore no hard and fast rules can be given in this respect. It is essential that a good client/analyst relationship exists in order for tasking to function effectively. The analyst must be objective, not influenced by preconceived ideas, but at the same time willing to accept the task without prejudice.

Tasking can take two basic forms:

- The client expresses a requirement for an analytical product focusing on a subject or a range of subjects of concern.
- The client formulates a general expectation for the analytical provider regarding an area of risk, threat or opportunity.

After the task has been clearly defined, the analytical unit commences its own planning for the remaining phases of the intelligence cycle.

Collection

The intelligence process relies on the ability to obtain and use data. However, the first and most basic problem to overcome lies with the collection and storage of this data which comes in many forms, from electronically retrievable to "hard copy".

COLLECTION: THE GATHERING OF DATA

Care must be taken at this early stage to avoid data overload which is always a problem for any agency but data ignored because the provider believed it not to be relevant can cause problems later on.

COLLECTION PLAN: A FORMALLY DEFINED APPROACH TO DESCRIBING THE INFORMATION NEEDED AND MEANS OF ACQUIRING IT

The issue of planning all the activities in the intelligence process is particularly significant in the collection phase. In both operational and strategic intelligence analysis the topics and the scope of the analysis should be clear before considering further actions to be undertaken. A collection plan in which the information needed is identified, and the means of acquiring it are laid out, is imperative to ensure the orderly and precise collection of relevant information.

The collection plan should include the information categories that are important to the analysis, the specific data items needed to do the analysis, possible sources of information and sources to be contacted with specific requests, and a schedule to indicate when the information was requested and when it is needed by. In order to avoid "chaos", a structured collection plan approach where the analyst is proactive, imaginative and explores all avenues to gain information is vital.

The three main types of sources of information are open, closed and classified.

- *Open source (OSINT)* is information that is publicly available. One very notable subset of open source information is so called "grey literature". It can consist of research, technical, economic reports, "white papers", conference documentation, dissertations and theses, discussion papers, subject-related newsletters, etc. One of the main difficulties in working with this type of source is evaluation as information available in the public domain can frequently be biased, inaccurate or sensationalized.
- *Closed source* is information collected for a specific purpose with limited access and availability to the general public. Closed source information is often found in the form of structured databases. In the context of criminal intelligence analysis, these databases will largely include personal data collected as part of ongoing targeting operations, or broader criminal records, vehicle registration data, weapons licensing, etc.
- *Classified* is information collected by specifically tasked covert means including use of human and technical (image and signals intelligence) resources. Use of classified information can significantly enhance the quality of an analytical product, as it is usually highly accurate; however, it can also make an analytical product significantly less actionable due to restrictions on dissemination.

The intelligence analyst must become an all-source analyst, i.e. selecting information sources for their relevance for the project rather than for availability or ease of access. An all-source analyst must avoid becoming a victim of a traditional concept that only closed or classified data sources are useful and contain valid and relevant data. The use of open sources often gives additional credibility to the final product or triggers off collection of further closed or classified information.

Selection of sources can also be regarded from the angle of cost effectiveness. Use of open sources instead of deploying expensive covert assets may significantly reduce the budget for a collection exercise, or alternatively, permit the acquisition of more information within an established budget. Use of open sources can also help protect or conserve sources of closed and classified information. At the same time, as exploration of open sources often requires handling extremely large data volumes, an analyst involved in OSINT should receive specialist training in the subject or be supported by an OSINT expert.

The ultimate objective of an operational intelligence analyst is to bring about the arrest of the criminal(s) under investigation and/or the disruption of a criminal group's activities. The aim of the team should therefore be to develop the most useful sources and collect the information most likely to produce successful results. A common starting point is to identify the criminal's associates—however, the objective should always be to identify relationships between individuals and their roles in the criminal activities, rather than identifying associates for their own sake.

A major issue in a collection exercise is the language of the source. Intelligence analysis is particularly appropriate for investigations of organized crime activities, which very often have a cross-border dimension. Exclusion of information (including open source information) purely on the basis of language can have a seriously damaging effect on the quality of an analytical product. Language training of analysts is one solution. Use of translation software is another.

An intelligence collection plan may contain the following elements:

- *Problem definition*—the intelligence problem needs to be precisely and clearly formulated
- *Project aim*—ideally a one-sentence definition of an intelligence requirement
- *Project scope*—it expands the definition of the project aim and sets out the actions expected from the analyst. It also contains a detailed description of the scope and purpose of collection measures and sources.

Evaluation

The validity of an inference is directly linked to the quality of the data behind the inference. Thus data evaluation is a key element of the intelligence cycle. It should be conducted simultaneously with or immediately after its acquisition, to ensure that the evaluation takes place within the context in which information had been acquired (as it is difficult to evaluate information that has not been submitted correctly within a local environment). Evaluation requires a separate assessment of the reliability of the source (the provider of the information) and validity and accuracy of the information.

EVALUATION: AN ASSESSMENT OF THE RELIABILITY OF THE SOURCE AND THE QUALITY OF THE INFORMATION

The source and the actual information must be evaluated independently of each other and therefore it is imperative that the person completing the report has a sound knowledge of the evaluation system. The two most widely used systems are 4 x 4 and 6 x 6 (See chapter 4 "Evaluation of source and data" for further details of this key process).

Collation

Collation is transfer of collected information and/or intelligence into a storage system (be it a filing cabinet or a computerized data base) in a structured (indexed, cross-referenced) format that permits rapid and accurate access. It is not equivalent to bulk filing of every bit of information or document acquired during collection. Irrelevant, incorrect and otherwise useless information is weeded out.

COLLATION: THE ORGANIZATION OF THE DATA COLLECTED INTO A FORMAT FROM WHICH IT CAN BE RETREIVED AND ANALYSED

Data integration and analysis

The analysis stage of the intelligence process is a key one. Analysis can be described as in-depth examination of the meaning and essential features of available information. Analysis highlights information gaps, strengths, weaknesses and suggests ways forward.

ANALYSIS: THE CAREFUL EXAMINATION OF INFORMATION TO DISCOVERS ITS MEANING AND ESSENTIAL FEATURES

The analytical process is aimed at the use and development of intelligence to direct law enforcement objectives, both for short-term operational aims and for long-term strategic reasons. The scope of analysis and its overall credibility depends on the level and accuracy of acquired information, combined with the skills of the analyst. Analysis is a cyclical process, which can be performed to assist with all types of law enforcement objectives. Different types of crimes and criminal operations require different scenarios, but in all cases the information used should not be pre-filtered through an artificially and arbitrarily imposed selective grid.

Data integration is the first phase of the analytical process. It involves combining information from different sources in preparation for the formulation of inferences. Various techniques may be used to display this information, the most common being the use of charting techniques.

- *Link charting*—to show relationships among entities featuring in the investigation
- *Event charting*—to show chronological relationships among entities or sequences of events
- *Commodity flow charting*—to explore the movement of money, narcotics, stolen goods or other commodities
- *Activity charting*—to identify activities involved in a criminal operation
- *Financial profiling*—to identify concealed income of individuals or business entities and to identify indicators of economic crime
- *Frequency charting*—to organize, summarize and interpret quantitative information
- *Data correlation*—to illustrate relationships between different variables

The next step in the analytical process is interpretation or logical reasoning, which requires going beyond the facts. The disciplined approach to analysis requires the maximum amount of information to be assessed at the time of integration to determine its relevance. Excluding information at the beginning of the process can easily lead to the significance of a vital piece of information being overlooked. This can lead to incorrect analysis, which can ultimately jeopardize an enquiry.

Analysis often identifies additional projects that are tangential to the original one. In the past, it was usual to undertake these projects simultaneously and in conjunction with the main one. This approach led to dispersing of resources, delays and overall lower quality of the final product(s). Through experience, it has now become accepted that analytical projects should be undertaken sequentially, one at a time, or by independent teams of analysts.

Data description and integration techniques, like link analysis, are not an end in themselves. They are simply tools used by analysts in the process of deriving meaning from information. The first truly analytical product is an inference. An inference comes from the premises—one common mistake is to intuitively develop an inference and then look for premises that would support it. This emphasis on the primacy of premises should be reiterated by means of a statement such as "the premises that led me to my inference are…" and not "the premises supporting my inference are…" (When presenting results, however, the starting point is the inference—the big idea—followed then by premises from which it came).

A "premise" in inference development is used to identify facts or pieces of information that go together to make a particular point. Premises are the first and key stage in the true process of data analysis as against data description. Understanding how premises are identified is crucial to developing inferences.

Premises are the closest link to the described information, and thus are the most objective and accurate representation of data. For any given set of premises derived from a particular set of information, the premises may be combined in different ways to suggest different inferences.

There are four types of inferences:

- *Hypothesis*—a tentative explanation, a theory that requires additional information for confirmation or rejection.
- *Prediction*—an inference about something that will happen in the future.
- *Estimation*—an inference made about the whole from a sample, typically quantitative in nature.
- *Conclusion*—an explanation that is well supported.

It should be noted that all inferences require testing in some manner before they can be accepted as fact.

Dissemination

An intelligence analyst has the responsibility of disseminating analytical products to targeted audiences, as appropriate. Much of the routine dissemination may be conducted by way of short notes. But intelligence analysts should be able to give oral briefings on larger investigations and write structured reports detailing the currently available information.

DISSEMINATION: THE RELEASE OF THE RESULTS OF ANALYSIS TO THE CLIENT

Throughout the whole process the client will have been in close consultation with the analyst, and would have been asked on numerous occasions to answer questions relating to the particular project.

The dissemination process can take various forms, such as:

- Structured formalized reports
- A structured and formal oral presentations with supporting documentation
- Weekly overviews in the form of bulletins
- Ad-hoc briefing to intelligence and investigative teams

The dissemination phase completes the initial cycle of the intelligence process.

Re-evaluation

Re-evaluation involves a continual review of the whole intelligence cycle to identify ways in which any stage of the cycle can be improved. To be of most value, re-evaluation should occur throughout the process, not merely be left to the last stage of the cycle. Re-evaluation can be directed at:

- Process
- Analytical product
- Use of the analytical product
- Effectiveness of reporting

- Staff deployment
- Priority setting
- Analyst's perspective
- Client's perspective

Intelligence activity is a collective process, as opposed to something one person or a group of people do as individual entrepreneurs.

3. Example of a national intelligence model: the United Kingdom

The National Intelligence Model (NIM) of the United Kingdom is based on two premises:

1. There are three levels of crime in the United Kingdom: single-jurisdictional, multi-jurisdictional, and international.

These are designed to impact on criminal business on all three levels:

- *Level 1—Local issues*—usually the crimes, criminals and other problems affecting a basic command unit or small force area. The scope of the crimes will be wide ranging from low value thefts to murder. The handling of volume crime will be a particular issue at this level.
- *Level 2—Cross-border issues*—usually the actions of a criminal or other specific problems affecting more than one basic command unit. Key issues will be identification of common problems, the exchange of appropriate data and the provision of resources for the common good.
- *Level 3—Serious and organized crime*—usually operating on a national and international scale, requiring identification by proactive means and response primarily through targeted operations by dedicated units and a preventive response on a national basis.

2. The desired outcomes of law enforcement are: community safety, crime reduction, criminal control and disorder control. The Model achieves this through four prime components which are fundamental to achieving the objective of moving from the business of managing crime, criminals, disorder and problems to the desired outcomes of community safety, reduced crime, and controlled criminality:

- Tasking and coordinating process
- Four key intelligence products
- Knowledge products
- System products.

Tasking and coordinating process

Tasking and coordination group meetings are chaired by a senior manager of a command unit who has the authority to deploy the necessary resources and comprise of people with key functional responsibility for the planning and execution of the law enforcement effort.

Strategic tasking is aimed at the setting up or amending the *control strategy* (i.e. priorities for intelligence, prevention and enforcement) and, having set the priorities, to make the principal resource commitments.

Tactical tasking is aimed at commissioning and applying the *tactical menu* to the *control strategy*, responding to new needs and monitoring of implementation of agreed plans. The *tactical menu* comprises four elements:

- Targeting offenders in line with the priorities of the *control strategy*;
- The management of crime and disorder hot spots;
- The investigation of crime and incidents which can be shown to be linked into "series";
- The application of a range of "preventive measures" such as closed-circuit television (CCTV) and lighting schemes or community action initiatives.

Production of the intelligence products—the creation of the intelligence products requires the same commitment to resources and direction from the tasking and coordination group as the drive for intelligence capability.

The key intelligence products are the "deliverables" by which intelligence-led policing can be implemented and its impact measured in terms of crime reduction, arrests, disruptions and enhanced community safety. Intelligence products are the result of the collaboration between analysts and intelligence officers in which the raw information is collected, analysed and interpreted, and represented with recommendations about required decisions or options for action. The intelligence led approach to law enforcement requires only four broad classes of intelligence product as shown in table 3-1 following:

Table 3-1. Four categories of intelligence product

Product	Aim	Purpose	Description
1. Strategic assessment	To identify the longer-term issues in an area, as well as the scope of, and projections for growth in criminality.	To establish law enforcement priorities, determine resource allocations, support business planning and inform senior managers and policymakers; To set a control strategy: priorities for intelligence, prevention and enforcement.	• Aim (terms of reference) • Scope (functional/geographic) • Current situation/survey • Main objectives set/met • Progress since last assessment • Major areas of criminality • Demographic/social problems • Patterns/trends • Resource constraints (overview/ summary)
2. Tactical assessment	To identify the shorter-term issues in an area this, with prompt action, can prevent a situation from deteriorating or developing. To monitor progress on current business in the 'tactical menu'.	To assist in the management of current operations and plans, as well as reallocate resources and efforts according to changing needs and problems.	• Current situation—progress on targeting; crime and other series; hot spots; preventive measures • Options for further action • Advantages/disadvantages. Best courses of action • Timeframe (short/medium) • Resource implications/changes

Product	Aim	Purpose	Description
3. Target profile	To provide a detailed picture of the (potential) offender and his associates for subsequent action.	To assist operational management in selecting targets, guiding investigations, shaping plans and maintaining supervision.	• Personal record • Criminal record • Financial profile • Network/associations report • Communications report • Transport report • Surveillance appraisal • Intelligence gaps
4. Problem profile	To identify established and emerging crime/ incident series and crime hot spots.	To assist management in resourcing investigative needs, targeting, hot spot management, directing crime reduction initiatives and crime-prevention measures.	• Problem identification • Background and causes • Scale of damage • Level of disorder/offending • Perpetrators • Internal/external links • Social impact • Resource implications

Prioritization of intelligence work—a major responsibility of the tasking and coordination group is to resource, direct and sustain intelligence capability. For intelligence work to be fully effective, it needs adequate assets (sources, people, knowledge products, system products) and disciplines which ensure that intelligence activities follow the identified strategic and tactical priorities.

Sources of information should not be limited to either reactive or proactive work. Much valuable data exists within the results of existing reactive work. A sufficient proactive capability is also essential.

An investment in the right people for specific roles is a significant benefit. Three major components of work exist: data management, analysis and specific intelligence collection. The intelligence manager is the essential catalyst for bringing the business of the command unit, the intelligence collection and analysis together. All intelligence work should be supported by knowledge and system products.

Knowledge products

They represent a range of products, either local or national, which define the rules for the conduct of business or best practice by which skilled processes are completed, and under what conditions work between agencies may take place. The "knowledge products" approach also represents a useful way to manage gap analysis in moving personnel issues forward to a more professionally based intelligence regime for law enforcement.

- National intelligence model
- Data protection guidelines
- Codes of practice

- National manuals and standards for:
  - Recording and dissemination of intelligence
  - Surveillance
  - Undercover operations and test purchases - Use of informants
  - Interception and accessing communications related data - - Case law on covert techniques
  - Local research and data access protocols
  - Local inter-agency access protocols
  - Intelligence training

System products

System products enable the collection, reception, recording, storage, use and dissemination of information. Broadly, they can be grouped into three types:

- *Provision of access to means for data storage, retrieval and comparison during the research process* access to large quantities of readily available law enforcement and other relevant data is the backbone of intelligence-led policing. Combination of nation-wide systems with the more local and specialized ones provides enormous potential for sophisticated analysis of criminal and other problems. The key to success, in terms of the quality of the analysed intelligence products, is the ability to access and bring together the data from disparate IS platforms. They may include diverse computerized systems that contain:
  - Crime records
  - Open source data
  - Intelligence files
  - Analysis tools
  - Specialized databases (e.g., firearms registration, driver licensing, criminal records, etc.)
  - Case management tools.

- *Provision of access to facilities or systems for acquisition of new information and intelligence*—the gathering of intelligence to fill identified needs may require the deployment of 'human sources' such as informants or undercover officers, or the deployment of human or technical surveillance resources. At the higher level of operations, there will be a requirement to access sophisticated covert entry techniques or intercept communications. The more intrusive techniques are usually only available in serious crime cases and the requirement to protect the secrecy of methodologies makes it undesirable that they be used where they can not be deployed as such. Mobile surveillance resources are generally expensive and require a sound intelligence case to be made for their deployment.

  At the local level, intelligence units will require possession of technical surveillance facilities commensurate with the investigations pursued at that level, and clear systems in place through which more sophisticated facilities can be accessed when the need arises. Within police forces, the distribution of surveillance resources, and the systems for accessing the more expensive or sensitive, will be policy issues integral to the crime and intelligence strategies.

- *Provision of operational security systems*—intelligence is a valuable commodity and must consequently be handled with care. The "need to know" principle is widely recognized as the backbone of the intelligence doctrine.

  The correct balance to be struck between making information as widely available as possible to maximize its potential benefit, and restricting its availability to protect the security of sources, techniques and information, is critical. A number of access systems and facilities help support the integrity and effectiveness of the intelligence environment:

  - The informant registration system;

  - The provision and use of analytical tools of the right standard;

  - The provision of secure accommodation and secure storage facilities;

  - The provision of appropriate briefing facilities, suitably secure when necessary;

  - The adoption of a national standard intelligence recording form which may incorporate risk assessment and handling restrictions;

  - Controlled access to foreign law enforcement agencies.

Analytical techniques and products

The National Intelligence Model depends upon four key intelligence products as discussed earlier. These products, in their turn, derive from nine analytical techniques and products, which underpin the development of professional knowledge in effective proactive law enforcement techniques.

Table 3-2. Nine types of analytical technique

Product	Description	Purpose
1. Results analysis	Assesses the impact of: • Patrol strategies and tactics • Reactive investigations • Proactive investigation • Crime reduction initiatives • Other law enforcement policies and techniques	• Helping to identify best practice • Areas for improvement • Post hoc debrief of incidents and investigations as an aid to professional development
2. Crime pattern analysis	• Crime series identification • Crime trend identification • Hot spot analysis • General profile analysis	Management decisions about prioritization within the "tactical menu" of : • Hot spots • Crime series identifications • Crime and disorder preventive and diversion initiatives Operationally, they are an aid to investigators and others in identifying new and emerging trends and requirements for further analysis.

Product	Description	Purpose
3. Market profiles	Maintained assessments of the state of the criminal market around a commodity or service—drugs, stolen vehicles, prostitution etc. • Key players • Networks • Criminal assets • Associated trends in criminality These profiles are made up of other analytical products, chiefly from network and crime pattern analysis.	Management decisions about prioritization of criminal and enforcement problems—the identification of targets and reduction opportunities: • The aggregation of standard market profiles maintained locally enables the building of a higher-level view • The profile may trigger more detailed analysis in target profiles, crime pattern analysis or network analysis to support operations
4. Demographic/social trends analysis	• Nature of demographic changes • Impact on criminality or apparently associated criminality • Deeper analysis of social factors which might underlie changes or trends in offenders or offending behaviour Could underpin a crime and disorder audit or research into known or predicted social or demographic changes.	• Strategic decisions about resourcing and priorities in law enforcement • Illuminates where future pressures are likely to arise and informs partners • Use in planning of seasonal or other tactical operations in response to emerging social phenomena or movements of people
5. Criminal business profiles	Reveals detailed operational modality including: • How victims are selected • Technical expertise employed by offenders • Weakness in systems or procedures which are exploited by offenders • Incorporates results from other types of analysis	Highlighting needs for changes in: • Legislation or other form of regulation • Resourcing to meet new threats • Operational planning in ascertaining key points for disruption • Immediate crime prevention/reduction opportunities • Raising knowledge standards through training and briefing products
6. Network analysis	• Key attributes and functions of individuals within the network • Associations within/outside of the network • Network strengths and weaknesses; • Analysis of financial and communications data • Inferences about criminal behaviour in association with target profiles	*Strategically:* • Indicating to management the seriousness of of linked criminality for strategic considerations *Tactically and operationally:* • Informs target operations • Suggests effective lines of enquiry and opportunities for disruption • Highlights gaps in the intelligence so as to drive source deployments
7. Risk analysis	The analysis of comparative risks posed by individual offenders or organizations to: • Individual potential victims • The public at large • Law enforcement agencies	The compilation of risk assessments as a prelude to prioritising intelligence or enforcement work at both strategic and operational levels leads to completion of risk management plans.

Product	Description	Purpose
8. Target profile analysis	Illuminates criminal capability and includes information about: • Associations • Lifestyle • Operational modality • Financial data • Strengths and vulnerabilities • Techniques which have worked or failed against the target in the past • Can cover any form of offending, not limited to purely "criminal" activity	Support target operations by: • Informing target selection • Identifying needs for intelligence • Indicating how sources and resources may be deployed against the target
9. Operational intelligence assessment (research)	The real time evaluation of and research into: • Incoming information on associations • Other phenomena around suspects in a current operation • May or may not be entirely the responsibility of an analyst	The prevention of "mission creep" and the prioritization of investigative needs arising from incoming intelligence during a current operation, together with identification of resultant priorities for ongoing intelligence work.

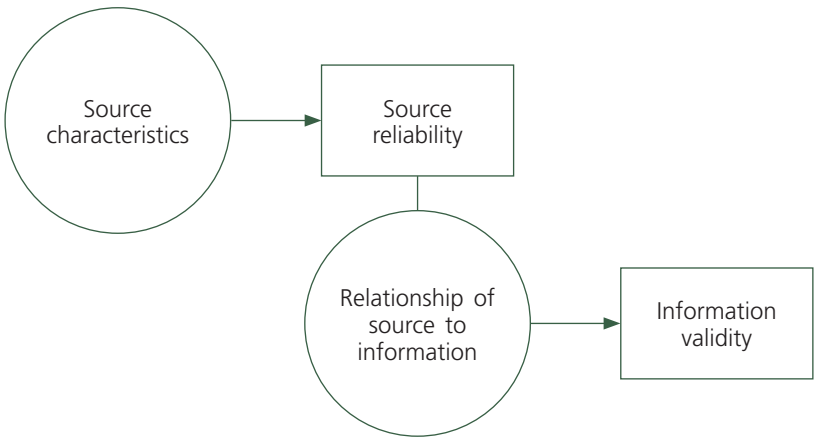
4. Evaluation of source and data

EVALUATION OF SOURCES AND INFORMATION

Once information has been collected it must be evaluated, a stage in traditional law enforcement activity which can often be ignored. A full and proper evaluation requires the assessment of the reliability of the source and the validity of information. This stage is crucial to the intelligence process as a whole and as such necessitates an explanatory chapter of its own.

A standardized system of evaluation has been developed using what is known as the 4 x 4 system, which is now widely accepted as common practice for law enforcement agencies. This system is for example used by analysts at Europol and any information received at Europol that is not evaluated will be assessed according to this system before use.

Other agencies use variants of this system, but each can be easily interpreted by reference to the explanatory tables, and if necessary the information can be converted from one system to another.



Three fundamental principles apply to evaluation:

1. It must not be influenced by personal feelings but be based on professional judgement.
2. Evaluation of the source must be made separately to the information.
3. It must be carried out as close to the source as possible.

Evaluation tables using the 4 x 4 system

Table 4-1. Source evaluation

A	• No doubt regarding authenticity, trustworthiness, integrity, competence, or • History of complete reliability
B	• Source from whom information received has in most instances proved to be reliable
C	• Source from whom information received has in most instances proved to be unreliable
X	• Reliability cannot be judged

Table 4-2. Information evaluation

1	• No doubt about accuracy
2	• Information known personally to the source but not known personally to the official who is passing it on • Logical in itself • Agrees with other information on the subject
3	• Information not known personally to the source but corroborated by other information already recorded
4	• Information which is not known personally to the source and can not be independently corroborated

Evaluation tables using the 6 x 6 system

Table 4-3. Source reliability

A **COMPLETELY RELIABLE**	• No doubt regarding authenticity, trustworthiness, integrity, competence • History of complete reliability
B **USUALLY RELIABLE**	• Some doubt regarding authenticity or trustworthiness or integrity or competence (one count) • History of general reliability
C **FAIRLY RELIABLE**	• Doubt regarding authenticity, trustworthiness, integrity, competence (two counts and more) • History of periodic reliability
D **USUALLY NOT RELIABLE**	• Definite doubt regarding authenticity, trustworthiness, integrity, competence • History of occasional reliability
E **UNRELIABLE**	• Certainty about lack of authenticity, trustworthiness, integrity, competence • History of unreliability
F	• Cannot be judged

Table 4-4. Data validity

1 CONFIRMED	• Confirmed by other independent sources • Logical in itself • Agrees with other information on the subject
2 PROBABLY TRUE	• Not confirmed independently • Logical in itself • Agrees with other information on the subject
3 POSSIBLY TRUE	• Not confirmed • Logical in itself • Agrees somewhat with other information on the subject
4 DOUBTFULLY TRUE	• Not confirmed • Not illogical • Not believed at time of receipt although possible
5 IMPROBABLE	• Confirmation available of the contrary • Illogical in itself • Contradicted by other information on the subject
6	• Cannot be judged

It is apparent that the two above evaluation systems differ by more than simply the number of grades, in particular where evaluation of information is concerned. The 4 x 4 system is based on a simple notion of personal knowledge. Hearsay information is afforded a lower rating. This simplicity has a value in itself, as evaluation becomes less subjective.

Sanitization

Following evaluation, it is advisable to continue with a system of sanitization. This is intended to protect the source or origin of the information from being detectable from the context or wording of the report. It also seeks to protect the circumstances or method by which the intelligence was obtained. To assist in this process the following sanitization guidelines are offered as examples of best practice:

- All intelligence should be accurately recorded. Reports for dissemination should only include intelligence related to the desired purpose of the dissemination;
- Care must be taken to remove from the text all material that in any way identifies the source;
- The timing and place of meetings with human sources may be irrelevant and could lead to the source being identified;
- Repeat intelligence from the same source could lead to the source's identification. The use of a confidential source register, where reference numbers are randomly allocated, reduces this possibility;
- Sanitization should make it impossible for the reader to determine whether the source is human or technical;
- In some circumstances it may be advantageous to reveal a source's true identity in the body of the intelligence without revealing their identity as the source. This may prove necessary, for example, where a source has been seen by other officers or criminals with the group of

named individuals, and not to name the source in the report might raise suspicions about his/her identity;

- Occasionally the intelligence of a single report will contain a range of intelligence material that could only be known by a limited number for individuals. Break this material into multiple reports and ascribe different references from a confidential source register to afford greater security;
- Where an officer is concerned that the contents of a report might indicate the source, reference should be made to a supervisor before dissemination or entry into an intelligence system takes place.

Dissemination

One further process to be completed at this stage, is to give guidance to any recipient on what they may do with the information. This may be done either by assigning a security classification to the report (e.g. secret, confidential, restricted), or by allocating a "handling code" which is a series of permissions and restrictions which determine who has the right or the need to be given access.

The following is an example of a system of handling codes:

Table 4-5. Handling codes

1	Dissemination permitted within law enforcement agencies in the country of origin.
2	Dissemination permitted to other national agencies
3	Dissemination permitted to international law enforcement agencies.
4	Dissemination within originating agency only.
5	Permits dissemination, but receiving agency to observe the conditions specified.

Such handling codes can be added to the codes allocated earlier to the source and information. Thus a code of B24 would translate as:

B - Source from whom information received has in most instances proved to be reliable

2 - Information known personally to the source but not known personally to the person passing it on

4 - Dissemination within originating agency only

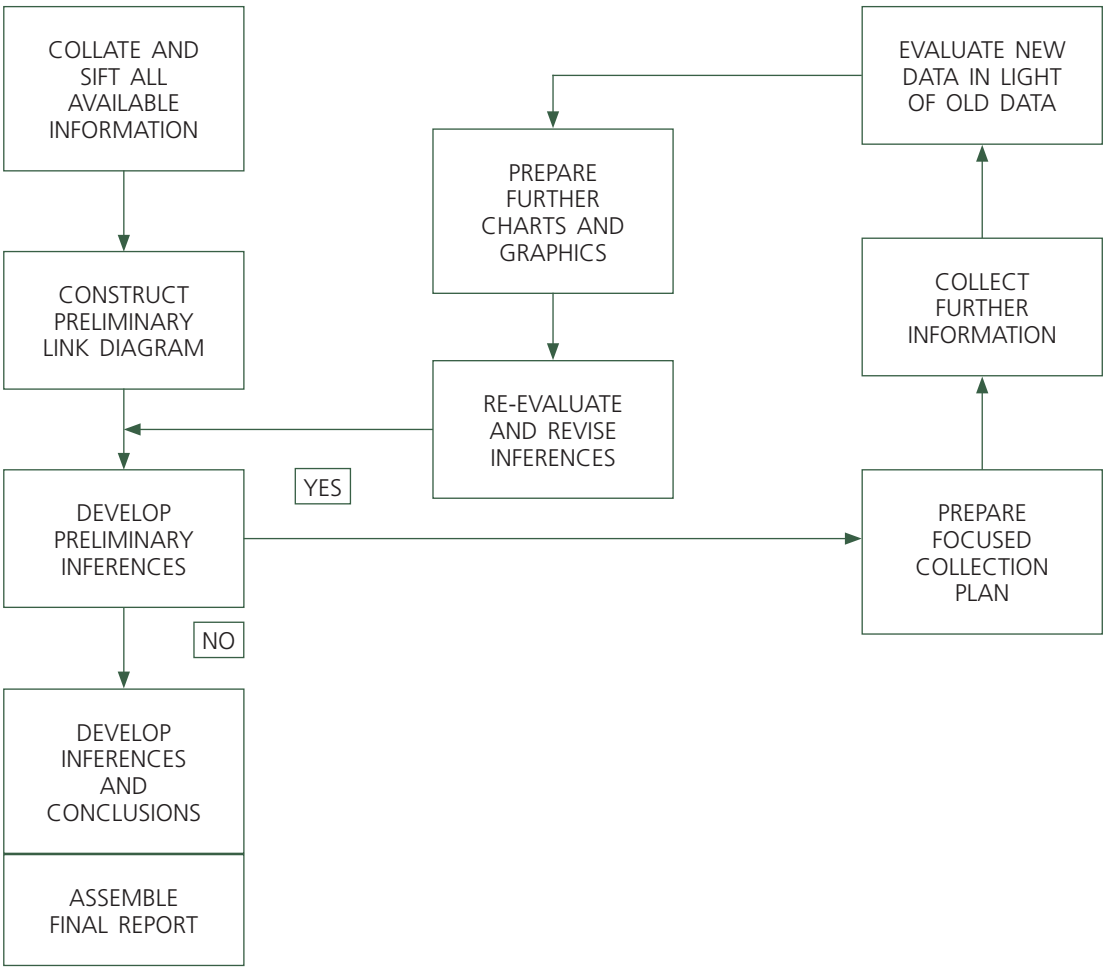
Once intelligence is integrated into an analytical product, it follows that if the product contains any intelligence graded at 'secret', then the whole document would have this protective marking. Similarly if any item was graded with a handling code of 4—dissemination within originating agency only—then the entire product would bear the same restriction.

5. Analysis and analytical process

The analysis stage of the intelligence process is critical for it concerns the examination of the meaning of the available information highlighting the essential features.

Analysis highlights information gaps, the strengths, the weaknesses and pinpoints the way forward.

Figure 5-1. The analytical process



The analytical process is critical to the development of intelligence to direct law enforcement objectives, both for short-term operational aims and for long term strategic reasons. The scope for analysis and its overall credibility is dependent on the level and accuracy of the information

supplied combined with the skills of the analyst. Analysis is a cyclical process, which can be performed on all types of law enforcement objectives. Different types of crimes and operations require different scenarios, but to enable effective analysis the type of information which is used should not be pre-set by artificial measures, but by the availability of the information and the legal restrictions of each country.

Data integration is the first phase of the analytical process combining various types of information from different sources to establish areas of weakness in order to draw inferences for law enforcement action. Careful integration highlights information gaps and weaknesses in the enquiry, thus ensuring that the analyst will continue data collection, even at the earliest stages of analysis work. This stage of the process at the early part of an enquiry also allows the analyst to begin to develop hypotheses based upon limited knowledge.

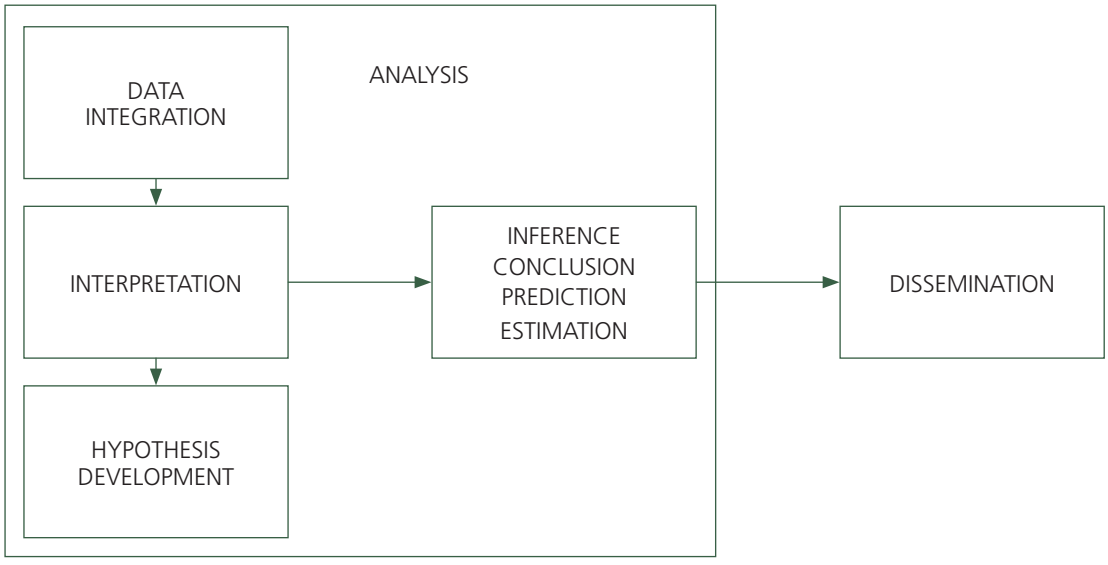
DATA INTEGRATION: COMBINING DATA IN PREPARATION TO DRAWING INFERENCES

The next step in the analytical process is interpretation which frequently means going beyond the facts, asking the "what if" questions. For this phase to be successful, the previous stages must be accurate and complete, to minimize the risk that the analyst takes in making an informed judgement based upon the information available.

DATA INTERPRETATION: GIVING THE DATA A MEANING; GOING BEYOND THE INFORMATION AVAILABLE

By integrating the data usually in the form of charts, but also as tables or maps, the analyst is creating a platform from which interpretation can be carried out. Charts and other products are useful as briefing aids or as illustrations of ideas; however the underlying data and its meaning is what the analysis is all about. The manual will concentrate on these analysis by-products as they are extremely useful in firstly, helping to understand the overall intelligence analysis process and secondly, helping to determine the understanding of a particular problem.

Figure 5-2. The process of analysis



By following the process over and over again, the analyst can begin to either support or refute the hypotheses already developed. It does not matter if an original idea is wrong, the most important aspect is to identify that it is wrong. As the overall enquiry continues the level of degree of accuracy of the ideas becomes stronger and the analyst can then begin to have greater confidence in the hypotheses.

Thus a hypothesis provides a theory that can focus further data collection. The hypothesis or any inference should contain:

Key individual or individuals	- WHO?
Criminal activities	- WHAT?
Method of operation	- HOW?
Geographical scope	- WHERE?
Motive	- WHY?
Time-frame	- WHEN?

The hypotheses or inferences made can be tested by the operational teams and feedback is then essential. Hypotheses contain a great deal of speculation and need to be confirmed, modified or rejected by the findings that come out of investigation. To test hypotheses structured data collection is essential and therefore a collection plan must be developed.

In the process of analysis the following axioms and standards for analysts should be considered.

AXIOMS FOR AN INTELLIGENCE ANALYST

Believe in your own professional judgment

You are the expert. Believe in your work and stand your ground if the intelligence supports your position

Be a risk taker

Do not be afraid of being wrong when forecasting trends or events. Taking risks is part of your job description. Only by taking risks you can maximize your value to your agency.

It is better to make a mistake than to do nothing at all

If you are wrong, and the facts call for it, admit it. Only those who don't do anything make no mistakes.

Avoid mirror imaging at all costs

Mirror imaging is projecting your thought process or value system onto someone else. Your targets are criminals. Their mentality is completely different. You must learn to think like they do.

Intelligence is of no value if it is not disseminated

Communicate the intelligence, conclusions and recommendations clearly and effectively and in a timely manner. What your client does not know has no value.

When everyone agrees on an issue, something probably is wrong

It is rare and not natural for a group of people in the intelligence community to fully agree on anything. If it does occur, it's time to worry.

Your client does not care how much you know, tell them just what they need to know

Excessive details merely obscure the important facts.

Form is never more important than the substance

A professional appearance and appropriately selected formats are important, but they do not outweigh substance. Clients want to know what intelligence means, and they want it when they need it.

Aggressively pursue collection of information that you need.

Never settle for less than all you need. If you fail to get access to the vital data source for any reason, you will be held responsible.

Do not take the editing process personally.

If editorial changes do not alter the meaning of your message, accept them. If they do, speak up. Even then, it might be that a brighter mind has seen what you have missed. Believe in your product, but be self-critical.

Know your intelligence community counterparts and talk to them

You are not competitors; you are of the same breed. Become part of the network. Do not pick up the phone only when you need something.

Do not take your job, or yourself, too seriously.

Avoid burnout. Writing you off as an asset will be a net loss to your agency (although it may not immediately see it exactly like this). The welfare of your family and your health is more important than nailing down a criminal, or scaling another rung on the career ladder. Your role in the larger order of things is not self-important. Your commitment, perseverance and dedication to the job will bring results only over a long term.

TEN STANDARDS FOR ANALYSTS

1. Analysed data (i.e., intelligence) should be used to direct law enforcement operations and investigations

2. Analysis should be an integral part of every major investigation the agency pursues.

3. Analytical products should contain, as a minimum, a written report. Visual products may also be presented, but are only acceptable as an addition to, rather than in replacement of, a written report.

4. Analytical products should contain conclusions and recommendations. These are presented to management for their consideration regarding decision-making.

5. The development of an analytical product requires the application of thought to data. Data compilation that does not reflect comparison or other considerations is not analysis.

6. Analytical products must be accurate. Consumers must be able to rely on the data provided to them by analysts.

7. Analysis must be produced in a timely manner.

8. Analytical products should reflect all relevant data available through whatever sources and means available to the analyst.

9. Analyses should incorporate the best and most current computer programs, compilation, visualization, and analytical techniques available in the analyst's environment.

10. Analyses should both reflect, and be evaluated upon, their qualitative and quantitative contribution to the mission and priorities of the agency or organization for which they are being produced.

6. The role of analysis

Analysis is used in law enforcement investigations and intelligence sections. During investigations, evidence (information) is gathered and reviewed to reconstruct the crime. Analysis is the logical thought process that is applied to the data (Harris 1976:27).

A case should begin by establishing the information needed and planning how to obtain it by asking questions or by executing a search warrant, for example. At the same time, ideas or hypotheses should be constantly developed about who committed the crime and how it was committed. Such hypotheses are the basic tools of the intelligence process as well (Harris 1976:27). This collection planning and analytical approach to investigations places analysts in the role of information or case managers.

In 1976, analysis was "...that activity whereby meaning, actual or suggested, is derived through organising and systematically examining diverse information" (Harris 1976:30). The three steps to completing analysis were shown as summarizing the relevant information, comparing the summary with expectations derived from an initial hypothesis, and explaining the results of this comparison (Anderson and Zeldidch, quoted in Harris 1976:30).

Today, we view analysis as a process which begins with identifying a problem or violation, summarizing and analysing what information is held, and detailing what additional data is needed; repeating those steps until the problem is solved or the investigation is concluded.

Analysis is the key to giving information direction and meaning, or uncovering its meaning. This is not always an easy task. For example, new criminals or criminal activities may not fit known, normal patterns (Harris 1976:30).

The distinctions between analysis and other phases of the intelligence process are not absolute. For example, an intelligence report is the direct result of the analysis of a particular body of information. However, the same report can also indicate (or state) a requirement for information, which leads to a collection activity. Thus, it may seem part of the planning process. Similarly, the difference between analysis and collation is not always distinct. Collation (placing data into formats to assist in their analysis) and analysis are often performed simultaneously.

The role of analysis varies from department to department. In some, cases are opened and immediately assigned to analysts to query databases; make summaries of known facts; and develop investigative plans for investigators to follow. These might be termed "analysis-driven investigations". In other agencies, analysts provide strategic assessments of unfolding problems, which give direction to policy and management. These might be termed "analysis/intelligence-driven agencies". In still others, analysis is used only after investigators have gathered substantial amounts of data; and the analysts are used to review that data and pass leads back to the investigation. These might be termed "analysis-supported investigation". Some agencies use analysis only for charts and graphs. Others have analysis done to support expert testimony in court. Perhaps because of this diversity and the underlying skills it represents, analysis has become a critical part of most major law enforcement not only in many countries. What is clear is that agencies using analysis get a significant return from it.

UNDERLYING ANALYTICAL SKILLS

Although there is a broad range of analytical techniques and products that reflect analysis, these have certain underlying skills as their basis. There are a handful of skills which underpin the analytical process. They include logical thought processes, research and writing skills, computer literacy and visualization skills. Analytical traits include persistence, independent work habits, flexibility and willingness to make judgments.

LOGICAL THOUGHT PROCESSES

The ability to think logically, see trends and forecast a possible future is critical to an analyst. Conversely, those who cannot organize data and "learn" from them will not excel in analysis. Logical thinking may come easier to some than others, but it can be taught. Sharpening one's logic skills can take place through puzzling through clues in literature or in puzzle books, as well as through more intellectual pursuits. Learning from data requires an acceptance of one's fallibility and lack of knowledge. Learning from data allows us to develop indicators and to forecast. (See also Critical Thinking on page 40)

COMMUNICATION SKILLS

The ability to communicate in writing or orally is critical to producing necessary analytical products. Intelligence is worthless if it is not shared with others. It may be easy to explain a complex case to those closest to it; analysts must be able to explain it simply to those who know nothing of it.

Good writing is 65 per cent good organization and 35 per cent concise and clear writing. The same is true of oral briefings, although presentation skills are added in there as well.

POSSIBLE ANALYTICAL UNIT ASSIGNMENTS

Strategic targeting

The unit identifies indicators of criminal activity and criminal capabilities to recommend targeting particular individuals and crime groups for investigation and prosecution. This will include the development of threat assessments and premonitories.

Investigative planning

The unit works with attorneys and investigators to develop investigative plans at the initiation of an investigation. The bureau's participation in the process will include a preliminary summary of all known data (including materials gleaned from public, government and commercial databases), a listing of leads that could be fruitful to follow and a preliminary assessment of the viability of the investigation.

Supporting investigations

The unit shall assign an appropriate analyst to each priority investigation including:

- Developing computerized databases to assist in compiling case data
- Link analysis
- Means of communication analysis
- Financial analysis
- Flow analysis
- Business-record analysis
- Specialized record analysis
- Summary and expert testimony

Analysts may also be assigned to joint investigations with other countries or agencies as requested.

Investigative consulting

The unit should provide investigative consulting on non-priority cases. This consulting may include investigative planning, provision of simplified databases and/or software for investigative use, information management strategies, guidance on simplified analytical products that might be completed in the field, etc.

Training

The unit should provide analytical and related training. To support the use of analysis in the agency, every professional employee should have at least a one-day seminar on analysis.

Liaison

The unit should pursue opportunities to relate with analysts in other law enforcement organizations through formal or informal groups, conferences and outside training sessions. Liaison with the academic community should also be incorporated.

Special projects

The unit should help identify the need for and parameters of data mining to provide early detection and crime prevention systems. Analytical support software testing may also be done by the section as needed. Other special projects may include the development of resource manuals for the department.

COMPUTER LITERACY

In today's environment, analysis must be performed with computers. Whether the analyst is searching for public information over the Internet; preparing a written report in a word processing program; using a proprietary software spreadsheet or database to compile data; using a data mining, or visualization, or mapping program, computers are the third most important skill for law enforcement analysis.

While most colleges and universities today require computer literacy for graduation, applicants are still arriving at law enforcement agencies without an understanding the concepts of relational databases, geocoding and other important computer activities. Computer literacy is a "must" for analysts.

VISUALIZATION SKILLS

Turning data into a visual form can be integral to having people understand it. For many people, analysis is viewed as a set of visual depictions; although, analysts know that this is only one product of the analytical process. Charting allows a simple view of a group, transaction or process. The simplicity of the chart is often a product of the analyst's complete understanding of the data such that it can be reduced to only the visual elements necessary to explain the data. This involves not only an ability to create visual products, but the use of analytical judgment to determine what is important and what can be omitted. While visualization software has become commonplace in the analytical field and is an excellent tool, the analyst still needs to exercise judgment in using that tool to construct such visualizations.

ANALYTICAL TRAITS

There are a number of key traits that can be identified in the best analysts:

Independent work habits

Analysts need to be able to work independently without constant supervision. They must be self-motivating and self-determining; that is, they need to see a problem and figure out how to deal with it. This is particularly true in smaller departments where supervisors have no experience with analysis and the analyst must establish themselves as indispensable to the supervisor.

Flexibility

Analysts need to be able to move with change. Analysts often function at the "cutting edge" of law enforcement. Thus, they must be able to adapt themselves to changes around them while being a catalyst for change themselves.

Persistence

Analysts must be persistent in their efforts to pursue leads and work as an agent of change. In the criminal world, perpetrators count on investigators giving up before catching them. Persistence is what allows us to complete our goals when they seem unreachable.

Willingness to make judgments

Analysts must take stands about their conclusions as the "experts" on the data they have researched and analysed. While previous use of analysts may have asked them to limit their comments to factual reporting, today managers need informed input to their decision-making from analysts. The inability (or unwillingness) to come to a conclusion about the data does not serve the analytical process or the law enforcement agency.

DUTIES OF THE INTELLIGENCE ANALYST

Harris stated that it is the analyst's responsibility to review reports, daily newspapers and other periodicals, to indicate how the report should be indexed and prepare abstracts of longer reports (1976:28). He also said that analysts should develop and maintain lists of names, sources of information/association charts, tentative hypotheses, operating assumptions that help him or her keep up to date on trends and new developments in his or her area of responsibility. The analyst was also responsible for identifying information requirements, performing research and analysis and preparing intelligence reports (Harris 1976:29).

Overall, the activities of an intelligence analyst are as diverse as the number and types of agencies which use them. Analysts work for intelligence, investigative, and regulatory agencies. They work in the private sector, in law firms and in investigative sections of consulting firms.

In the past, the investigator provided the analyst with raw information while the analyst processed the raw information and developed suggested avenues of approach to the investigator. The analyst looked beyond specific cases to ascertain the similarities and differences among many different cases (Harris 1976:30). Today, the analyst has a world of information, through on-line commercial databases and other Internet resources at his or her fingertips. Analysts can do a significant amount of research themselves, without having to leave their desks.

Today's analyst is responsible for performing a wide variety of tasks relating to the processing of new and existing information. The top ten duties that analysts perform—as represented in a survey by the International Association of Law Enforcement Intelligence Analysts (IALEIA) in 1998—were:

- Responding to requests for information/database look-ups (38 per cent)
- Data entry (9 per cent)
- Tactical analyses (9 per cent)
- Financial analyses (9 per cent)
- Preparing reports, bulletins, newsletters (6 per cent)
- Computer research (6 per cent)
- Crime analysis (5 per cent)
- Strategic analysis (5 per cent)
- Support for background investigations (4 per cent)
- Database design and information management (4 per cent)

While this listing represents the reality of analytical work at the turn of the century, some caveats should be stated. First, the practice of having analysts simply responding to inquiries to a database is a waste of analytical skills and talents. Agencies should have investigative assistants or other less skilled personnel filling this function. Likewise, doing simple data entry ("data loading") is not an appropriate primary duty for an analyst.

Finally, the role of analysts is not as in-house graphic artists. Analytical charts and graphs are not pictures to be drawn as a graphic artist might draw them. Analytical charts and graphs are products of a thorough analysis of a data set and represent an accurate and clear analytical portrayal of data according to generally accepted analytical standards. Thus, it is unwise to ask an analyst to put a chart together without his or her thorough review of the facts.

A more appropriate list of duties for an analyst would be:

- Preparing tactical analytical products (30 per cent)
- Performing strategic analysis (20 per cent)
- Preparing reports and bulletins (20 per cent)
- Developing or pursuing training and/or best practice (15 per cent)
- Creating database and computer formats to support analysis (10 per cent)
- Preparing investigative plans (5 per cent)

More advanced analysts would probably be more involved in strategic analysis, training and investigative planning while the newer analyst might be more involved in tactical products and reports. Specialist analysts, with more thorough computer backgrounds, would be more involved in creating databases in support of analysis.

CRITICAL THINKING

A discussion about analysis would not be complete without a discussion of the importance of critical thinking. Critical thinking is simply thinking about what is being done, or seen, or thought. In many cases, people perform their jobs unthinkingly that is, taking the same approach to different problems and then wonder why the same problems recur.

Godfrey and Harris said that the intelligence process is "sometimes physical but always intellectual" (1971:2). What they meant by that is that the thought process always needs to be applied to the data, whether it has just been collected and retrieved or it has been on hand all the while. It is just this thinking process that is being spoken of when "critical thinking" is mentioned.

Applying critical thinking to a situation makes one look at it from other perspectives. Other possible explanations could also exist. Interpreting the data without looking at all the possibilities may cause an inaccurate analysis. Inaccurate analysis of a situation can be a fatal mistake.

UNDERLYING APPROACHES: ONE VIEW

As one approaches an analysis, a starting point must be found. "The most analysis falls into supporting two types of common inquiry or organizational need, the 'bread and butter' of our workload" (Atkin 1998:3). On the basis of their organizational focus, he distinguishes between:

- Inquiries that begin with crime information and seek to link it to known offenders
- Inquiries that begin with a suspect and seek to identify their links to crime.

He then states that after following these two models of inquiry, he divides recommendations into two types: tying up loose ends and lateral thinking. The tying up of loose ends is where the analyst spots information gaps in the data. The lateral thinking takes the analysis into a wider scope. How to develop inferences from premises with respect to these two types of inquiry are shown following.

Development of inferences—a schematic for formulating premises starting from crime information

Premises

1. What change in the environment has created and/or increased the opportunity for this particular grouping or type of crime?
2. What crime has occurred that can be grouped, and what is/are the patterns or common features on which the groupings are made?
3. If the crime is goods-orientated, where are the goods being recycled into the public domain?
4. What is the underlying pattern that links these features?
5. What is the organization behind the pattern?
6. Organizations don't commit crime, people commit crime. Who are the people behind the organization?
7. What is the hierarchy of people in the organization; who are the main/key players and who are less important?
8. What other information do we have and how does it affect the overall hypothesis (eg. previous convictions or involvement in crime, concealed income, etc.)

Development of inferences—a schematic for formulating premises starting from a target or suspect offender

Premises

1. What information do we have about this person, in particular their key associates?
2. What organizations are the target and/or his key associates linked to? What other/seemingly less important people are involved, and what is the structure of any hierarchy?
3. What is the structure of these organizations?
4. What criminal operations are these organizations involved in?
5. What is the particular crime type/pattern the operations target?
6. What factor(s) made this crime type the preferred target for these operations/individuals?
7. What other information do we have, and how does it affect the overall hypothesis (e.g. previous convictions/involvement in crime, concealed income, etc.)?

7. Analytical techniques

In carrying out the general functions of analysis in the intelligence process discussed earlier, the analyst can expect to be called upon to bring some specialized techniques to bear on the problem (Harris 1976:30).

The comparison of data is the critical step in analysis since, through this activity, meaning is derived. The data the analyst has organized and summarized are compared to a set of expectations derived from an initial hypothesis. In addition to imposing a general structure on the analysis, the hypothesis is the source of criteria that determines the significance of observed data. In this stage, statistics may be used. Similarities or regularities in geographic distribution might also be observed. During this step, analysts should always be aware of the differences among the data under examination (Harris 1976:30).

In the comparison step, the analyst asks what is significant. The analyst should determine:

- Whether the data exhibit significant relationships;
- The meaning of the relationships or lack of them in terms of the purpose of the analysis;
- The larger meaning of these findings in terms of intelligence unit;
- Larger meaning from the findings; and
- Requirements for additional information or further analysis (Harris 1976:31)

There have been three general types of analysis detailed but the distinctions among them have been viewed by some as arbitrary. However, the audience for the analytical products may be the easiest way to differentiate among the analysis done in law enforcement. The types are crime analysis, investigative analysis and strategic analysis.

Crime analysis is done most often at a local agency and looks at criminal incidents or crime statistics to determine ways to prevent or deter future crime or identify and arrest its perpetrator(s). Thus, its audience can be patrol management for example.

Investigative analysis is done for all levels of government and focuses on a particular violation of crime, seeking to provide products that will assist in the violator's arrest and successful prosecution. Thus, the audience for this type of analysis is detective supervisors and attorneys.

Strategic analysis looks at overviews of crime groups or criminal activities and seeks to measure the threat that those groups and activities pose to the jurisdiction, now and in the future. Recommendations are made to lessen that threat, often through policy changes. Its audience should be law enforcement agency management.

This is not to say that crime analysis data might not be used to recommend policy changes, or that investigative analysis might assist in crime reduction. All these are possible. In many

small agencies, analysts are full-service analysts and carry the burden of whatever analysis is needed, regardless of its "type".

It is also important to differentiate between an analytical technique and an analytical product. For example, a link analysis might include a link chart; a set of biographic data on the subjects of the chart; a summary of known data; conclusions; and recommendations. The link chart is just one product of the process of link analysis, not an end to itself.

Following is a listing of basic types of analysis that may be done at varying levels of law enforcement. It should be noted that there are several dozen more types of analytical products that are not included here.

Activity-flow analysis

Activity-flow analysis is used to provide a generic view of a set of criminal actions, or modus operandi, to determine what the key actions were and provide an overview of a crime. It looks at the process of an activity and can then assemble necessary components of the crime to explain a complex crime simply. This activity-flow analysis process can also be used to compare to other crimes, to see if there may be a connection between them.

Association analysis

Association, link, or network analysis looks at the relationships among individuals, businesses, locations, groups and other entities involved in a crime; and how those relationships impact on, or are impacted by, the criminal activity. The products of an association analysis may include charts, biographical profiles, chart summaries, conclusions and recommendations for further action.

Bank record analysis

Bank record analysis encompasses any review or analysis of bank records for any purpose. It provides not only a review of activity in an account or set of accounts. It also looks at why the payments were made or received and what indicators of illegal activity may be present.

Business record analysis

Business record analysis is the review of varied business records to compare and contrast them and look for inconsistencies in the records or for other indications of criminal activity. Business records may be generic (e.g., journals, ledgers, invoices, orders, tax filings, etc.) or specific (patient records, inventories, travel records, etc.).

Case analysis (United Kingdom)

Sometimes also known as "decision-tree analysis", case analysis examines the cycle of data-decision-action-new data-new decision that is the essence of any investigative management. Unlike visual investigative analysis, which seeks to "map" the whole investigation, case analysis focuses upon the decisions that were made and the data upon which they were made. With many investigations subject to rigorous review both internally by organizations and through cross-examination in court this technique provides a useful resource for detailing the "what, when and why" of management decisions, and thus justifying every stage of the process and policy of an investigation.

Case analysis (United States)

Case analysis is an approach used to manage the analysis of varied data in support of current or historical investigations. It involves analytical decision-making to determine the appropriate analytical technique to use.

Content analysis

Content analysis is the analysis of the oral or written communication to determine the meaning of that communication. Another term is "investigative discourse analysis": "the close and systematic study of basic linking components of spoken or written communications in order to determine process... occurrence... descriptions... individual involved... evaluation... relationships... reason for specific word selections... truthfulness and deception" (Rabon 1999:11-12).

Commodity-flow analysis

Commodity-flow analysis looks at the flow of goods or services among people, businesses and locations to determine the meaning of that activity. It may give insights into the nature of a conspiracy, a hierarchy of a group, or the workings of a distribution network. It can show the final beneficiary of the criminal act or the final location of assets purchased on his or her behalf.

Crime pattern analysis (Incidents/perpetrators/crimes)

Crime pattern analysis looks at the components of crimes to discern similarities among them. It is used at the varying levels when a series of crimes have occurred. The patterns involved can be based on time, geography, perpetrators, victims, modus operandi, criminal signatures, criminal rewards, or other factors. Within time, the date and day of the week are considered along with the number of days between incidents and the times of day the incidents occurred. The geography can include the locations, the types of activity at the location (residential, commercial, industrial), urban, suburban, or rural, elevation, proximity to other inhabited (or non-inhabited) buildings, etc. It may also be used to draw conclusions about the victimology of the crimes.

Descriptive analysis

Descriptive analysis is the written summarization of an event, activity, group or person that imparts data of an evaluative nature and from which conclusions and recommendations can be drawn. It is used most frequently on information collected through surveillance, interviews and written or oral statements.

Estimates

Estimates tell us what to expect as a result of a past or current activity, such as a projection of the amount of drugs to be available based on current illicit crop production. They can be used to project what the future territory, size, or influence a crime group will have. They usually involve specific numbers or other data.

Event flow analysis

Event flow analysis incorporates event flow and timelines and looks at activities over time. While the traditional look at flow analysis has focused on flow charting, these charts are interim products to assist the analyst in determining what is known and what is missing from the activities or transactions.

Forecasts

Forecasts are a prediction of the future based on an analysis of past and current trends. Forecasting can be done on both numeric and descriptive data. Forecasts are different from estimates in that they can be general, rather than quantitative.

Geographic distribution analysis

Geographic Distribution Analysis looks at the occurrence of something over a particular geographic area to determine what can be concluded about the activity or area. In crime analysis, "hot spots" are targeted after their identification through geographic distribution analysis.

Geographic profiling

"Geographic profiling is an investigative methodology that uses locations of a connected series of crimes to determine the most probable area of offender residence. It is applied in cases of serial murder, rape, arson, robbery and bombing..." (Rossmo 1999:1).

Indicator analysis

Indicator analysis involves the compilation, review, and analysis of the activities that occur around a particular activity to develop a model of what occurrences may be used to predict the presence of that activity in other locations.

Market profiles

Market profiles are assessments of the state of the criminal market around a commodity or service such as drugs, stolen vehicles, prostitution, etc.

Net worth/source and application of funds analysis

Net worth analysis and source and application of funds analysis both include a financial profile of the individual or business and compare those profiles (which are based on slightly different views of the data) to what the individual or business reported as legal income. The difference between the figures is considered as possibly illegal income. Its initial purpose was to determine taxpayers' income tax liabilities, primarily in those instance where no books or records of income and expenses have been maintained by taxpayers from which a determination of tax liability could be made." Its use is now expanded to non-tax related financial crimes.

Premonitories

Premonitories are short-term looks at crime groups or criminal activity with the purpose of preparing to initiate an investigation into that group or activity.

Results analysis

Results analysis is assessing the impact of strategies, reactive investigation, proactive investigation, crime reduction methods, and techniques and policies.

Statistical analysis

Statistical analysis is the review of numerical data to summarize it and to draw conclusions about its meaning. It incorporates a number of different techniques including frequency distribution.

Suspicious financial transaction analysis

This form of analysis is developing as countries adopt suspicious financial transaction reporting. Generally, it is looking at these transactions (and sometimes other types of bank report) to ascertain if financial crimes are occurring.

Telephone analysis

Telephone analysis looks at phone call data to determine associations as well as the activity it encompasses. This has been considered a staple form of analysis and can be used in support of probable cause to obtain an electronic intercept. It can also show the geographic range of a conspiracy and can uncover additional participants in the criminal activity. Today its form should be expanded to cover other means of communication such as e-mail.

Visual investigative analysis (VIA)

Visual investigative analysis is the analysis of the steps taken, or necessary to be taken, in the course of an investigation or in the course of a criminal act. Using VIA, case managers can track the deployment of personnel; see the status of leads; and identify what needs to be done next in the investigation.

Warnings/vulnerability and threat assessments

Warnings may tell of some impending activity that will be a danger to society. Threat assessments are used to evaluate a criminal activity and its impact on society. Vulnerability assessments look at an area, individual, or event in terms of what its vulnerabilities are to criminal activity. An example of an event that would have this type of treatment is the Olympics.

GENERAL STANDARDS FOR ANALYSTS

While they have developed as a profession, analysts have developed standards and criteria by which they can be judged. Some of these are found in professional organizations for analysts that provide advance standing, such as the Society of Certified Criminal Analysts (SCCA). Others are espoused in various government documents.

Godfrey suggested that there were two types of analysts: non-specialists and specialists. The former often came into the field as recent graduates. These analysts were to be intelligent, precise and anxious to explore new areas and would "soon make important contributions to criminal analysis" (Harris 1976:42). Specialist analysts, on the other hand, might be academics on retainer or people from other agencies, which could assist on a specific case.

The intervening years since has shown law enforcement that specialist analysts can be developed and trained through a combination of education and experience within the law enforcement framework. For example, a person with a business or accounting degree could be hired for financial analysis if that was deemed to be appropriate and then trained in the finer points of

analysis over straight accounting (or forensic accounting). Analysts with computer degrees or post-college courses might be best for jobs requiring a lot of database development. Analysts with language specialties are popular in international intelligence settings. The general standards for analysts are summarized in the following paragraphs.

Education

A number of agencies now require a degree level qualification for trainee analysts; some also for trainee police officers. The SCCA requires two- or four-year degrees for certification, depending upon the level of that certification (regular or lifetime). It is hoped that an analyst who is certified with a two-year degree will go on to get a four-year degree before applying for lifetime certification.

The General Counter Drug Intelligence Plan released in February 2000 by the Centre for Narcotics Control in the United States stated that analysts should have four-year college degrees. In several countries, undergraduate and graduate degree programmes in intelligence and analysis are being developed. Some of the graduate programmes do not require a previous four-year degree for admission but are taking experience in the field in lieu of educational qualifications.

Civilian vs. non-civilian background

While the general consensus seems to be that civilians, without prior law enforcement officer training, make the best analysts; sworn intelligence officers are used in a number of settings. Until recently, for example, all Australian analysts were sworn intelligence officers. In Canada, the Royal Canadian Mounted Police uses a mix of sworn and non-sworn analysts.

In the United States, there are a number of sworn officers who are filling the role of crime analyst for their department, particularly in areas where it is difficult to hire non-sworn employees above the clerical support ranks. In general, however, most United States agencies recruit civilians. Some agencies hire retired police officers to fill this role believing their previous enforcement experience will aid their performance of analysis. Others would frown on this supposition, believing that police officers' former training will not provide them with the flexibility and creativity to approach each diverse intelligence problem.

References

1. Atkin, Howard, 1998
2. Criminal Intelligence Analysis (West Yorkshire Police, 1998)
3. Europol Guidelines on Intelligence
4. Europol Analytical Unit, The Hague, 10-21 May 1999 6.
5. Fiora, B. "Writing Intelligence Reports that Get Read" (Competitive Intelligence magazine, Vol.5 JanuaryFebruary 2002)
6. Godfrey, E. Drexel and Don R. Harris *The Basic Elements of Intelligence* (1971)
7. Harris, Don R. *The Basic Elements of Intelligence* - Revised. Washington, DC: Law Enforcement Assistance Administration (1976).
8. ICPO-lnterpol Guidelines on Criminal Intelligence Analysis (Vers.3, 2000)
9. McDowell, D., *Strategic Intelligence* (Istana Enterprises, 1998)
10. Morehouse, R., "The Role of Criminal Intelligence in Law Enforcement" ("Intelligence 2000: Revising the basic Elements, L.E.I.U. -IALEIA, 2000)
11. Rabon, D., *Investigative Discourse Analysis* (1999).
12. Rossmo, D.K., *Geographic Profiling* (1999)
13. UNDCP Intelligence Policy and Training Manual (2000)
14. Wantanabe, 2000
15. West Yorkshire Police June 2002 and Anacapa Life Sciences Inc., 1993.

UNODC

United Nations Office on Drugs and Crime

Vienna International Centre, PO Box 500, 1400 Vienna, Austria
Tel.: (+43-1) 26060-0, Fax: (+43-1) 26060-5866, www.unodc.org

Printed in Austria

V.10-56152—December 2010—200