UNODC
United Nations Office on Drugs and Crime

# Criminal Intelligence

## Manual for Analysts

UNITED NATIONS OFFICE ON DRUGS AND CRIME
Vienna

# Criminal Intelligence

Manual for Analysts

UNITED NATIONS
New York, 2011

This publication was made possible through funding received from the Government of the United States of America.



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.

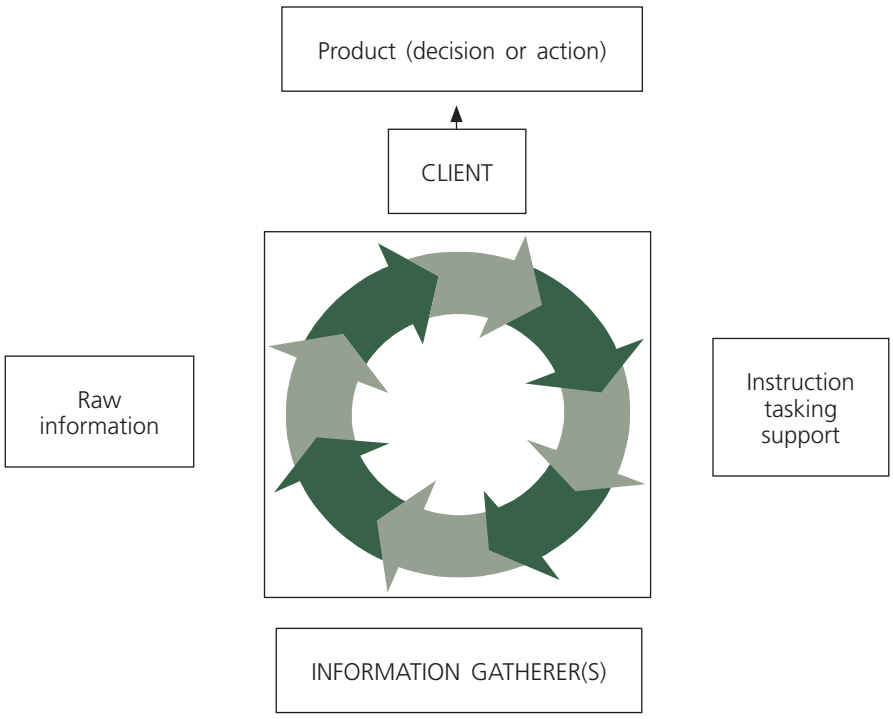
Reviewing the historical background, the "roots" of intelligence and analysis as a process and as a profession is a useful and important exercise. Raising our understanding of the origins of intelligence and analysis helps us to understand both where we are now and how/why we

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.

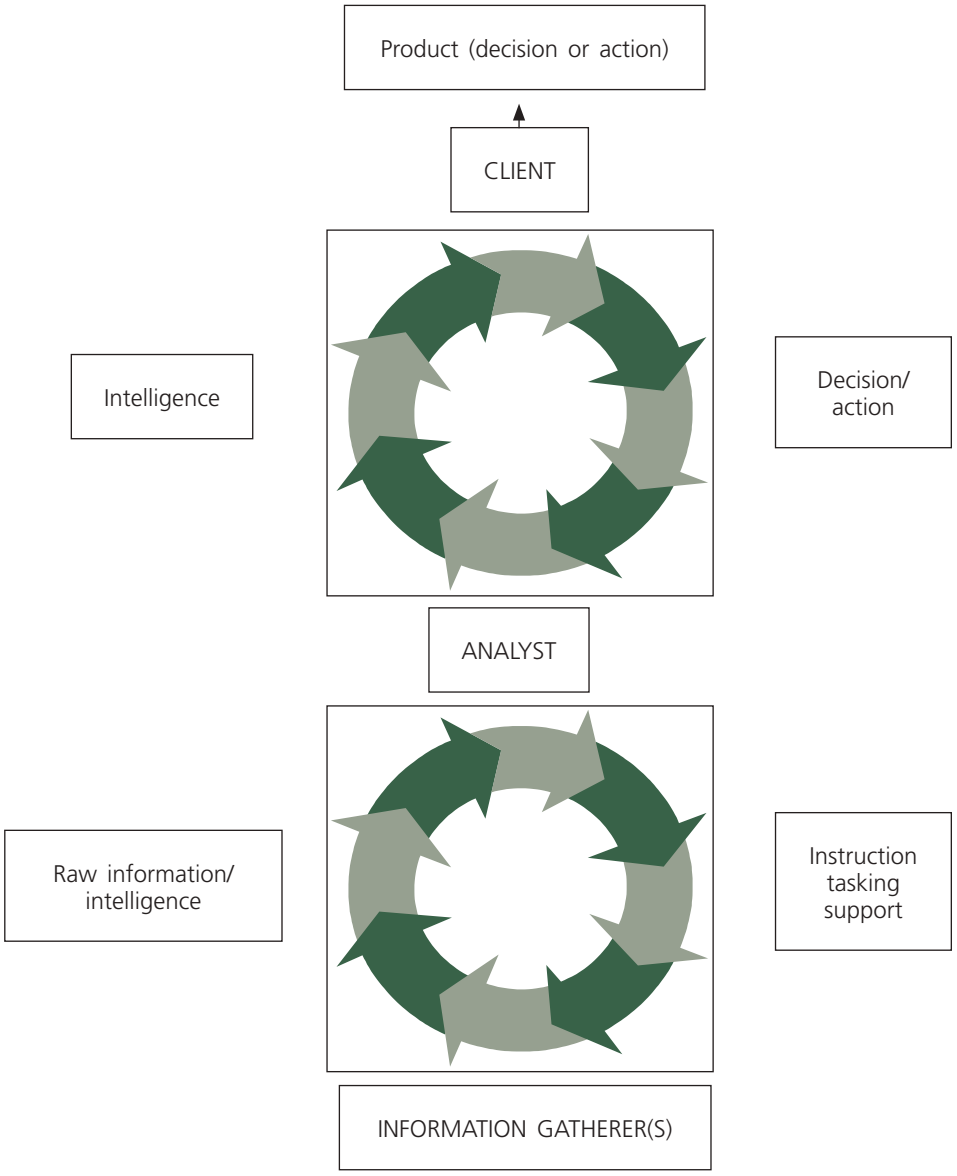
The overall result of this change was ironically that these benefits also carried with them a new problem for the client. Much larger quantities of information were gathered, far more quickly than before, and the reaction time for making decisions was reduced. In addition, controlling the process of 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

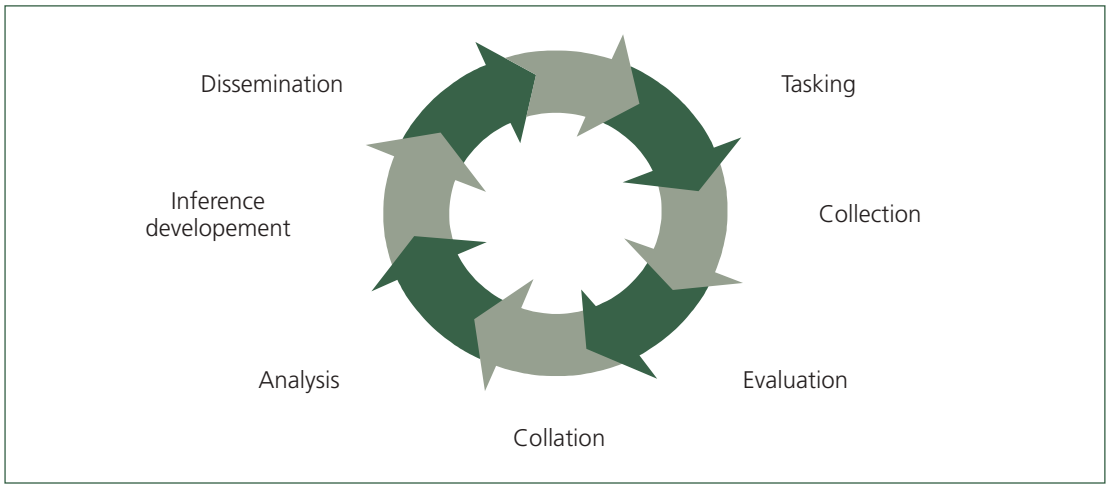
EVIDENCE: DATA FROM WHICH TO ESTABLISH PROOF

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;<br>To set a control strategy: priorities for intelligence, prevention and enforcement. | • Aim (terms of reference)<br>• Scope (functional/geographic)<br>• Current situation/survey<br>• Main objectives set/met<br>• Progress since last assessment<br>• Major areas of criminality<br>• Demographic/social problems<br>• Patterns/trends<br>• 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.<br><br>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<br>• Options for further action<br>• Advantages/disadvantages. Best courses of action<br>• Timeframe (short/medium)<br>• 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<br>• Criminal record<br>• Financial profile<br>• Network/associations report<br>• Communications report<br>• Transport report<br>• Surveillance appraisal<br>• 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<br>• Background and causes<br>• Scale of damage<br>• Level of disorder/offending<br>• Perpetrators<br>• Internal/external links<br>• Social impact<br>• 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:<br>• Patrol strategies and tactics<br>• Reactive investigations<br>• Proactive investigation<br>• Crime reduction initiatives<br>• Other law enforcement policies and techniques | • Helping to identify best practice<br>• Areas for improvement<br>• Post hoc debrief of incidents and investigations as an aid to professional development |
| **2. Crime pattern analysis** | • Crime series identification<br>• Crime trend identification<br>• Hot spot analysis<br>• General profile analysis | Management decisions about prioritization within the "tactical menu" of :<br>• Hot spots<br>• Crime series identifications<br>• Crime and disorder preventive and diversion initiatives<br>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.<br>• Key players<br>• Networks<br>• Criminal assets<br>• Associated trends in criminality<br>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:<br>• The aggregation of standard market profiles maintained locally enables the building of a higher-level view<br>• 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<br>• Impact on criminality or apparently associated criminality<br>• Deeper analysis of social factors which might underlie changes or trends in offenders or offending behaviour<br>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<br>• Illuminates where future pressures are likely to arise and informs partners<br>• 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:<br>• How victims are selected<br>• Technical expertise employed by offenders<br>• Weakness in systems or procedures which are exploited by offenders<br>• Incorporates results from other types of analysis | Highlighting needs for changes in:<br>• Legislation or other form of regulation<br>• Resourcing to meet new threats<br>• Operational planning in ascertaining key points for disruption<br>• Immediate crime prevention/reduction opportunities<br>• Raising knowledge standards through training and briefing products |
| **6. Network analysis** | • Key attributes and functions of individuals within the network<br>• Associations within/outside of the network<br>• Network strengths and weaknesses<br>• Analysis of financial and communications data<br>• Inferences about criminal behaviour in association with target profiles | *Strategically:*<br>• Indicating to management the seriousness of of linked criminality for strategic considerations<br>*Tactically and operationally:*<br>• Informs target operations<br>• Suggests effective lines of enquiry and opportunities for disruption<br>• 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:<br>• Individual potential victims<br>• The public at large<br>• Law enforcement agencies | The compilation of risk assessments as a prelude to prioritizing 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:<br>• Associations<br>• Lifestyle<br>• Operational modality<br>• Financial data<br>• Strengths and vulnerabilities<br>• Techniques which have worked or failed against the target in the past<br>• Can cover any form of offending, not limited to purely "criminal" activity | Support target operations by:<br>• Informing target selection<br>• Identifying needs for intelligence<br>• Indicating how sources and resources may be deployed against the target |
| **9. Operational intelligence assessment (research)** | The real time evaluation of and research into:<br>• Incoming information on associations<br>• Other phenomena around suspects in a current operation<br>• 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

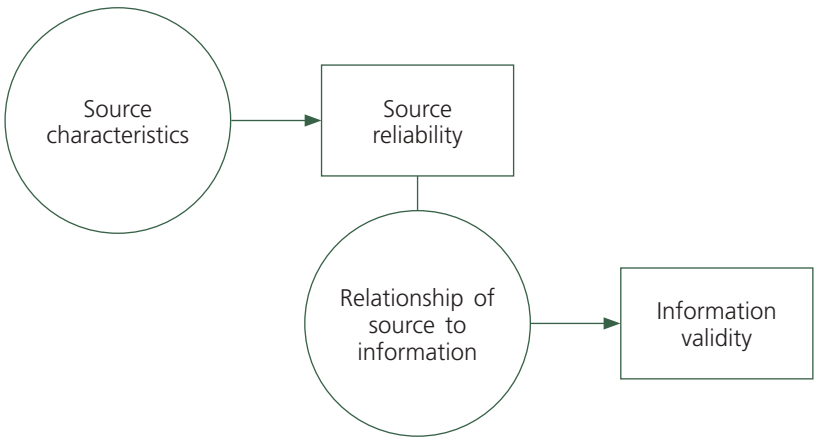
## EVALUATION OF SOURCES AND INFORMATION

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.

**Figure 4-1. The evaluation process**




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

**Table 4-4. Data validity**

| | |
|---|---|
| **1 CONFIRMED** | • Confirmed by other independent sources<br>• Logical in itself<br>• Agrees with other information on the subject |
| **2 PROBABLY TRUE** | • Not confirmed independently<br>• Logical in itself<br>• Agrees with other information on the subject |
| **3 POSSIBLY TRUE** | • Not confirmed<br>• Logical in itself<br>• Agrees somewhat with other information on the subject |
| **4 DOUBTFULLY TRUE** | • Not confirmed<br>• Not illogical<br>• Not believed at time of receipt although possible |
| **5 IMPROBABLE** | • Confirmation available of the contrary<br>• Illogical in itself<br>• 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

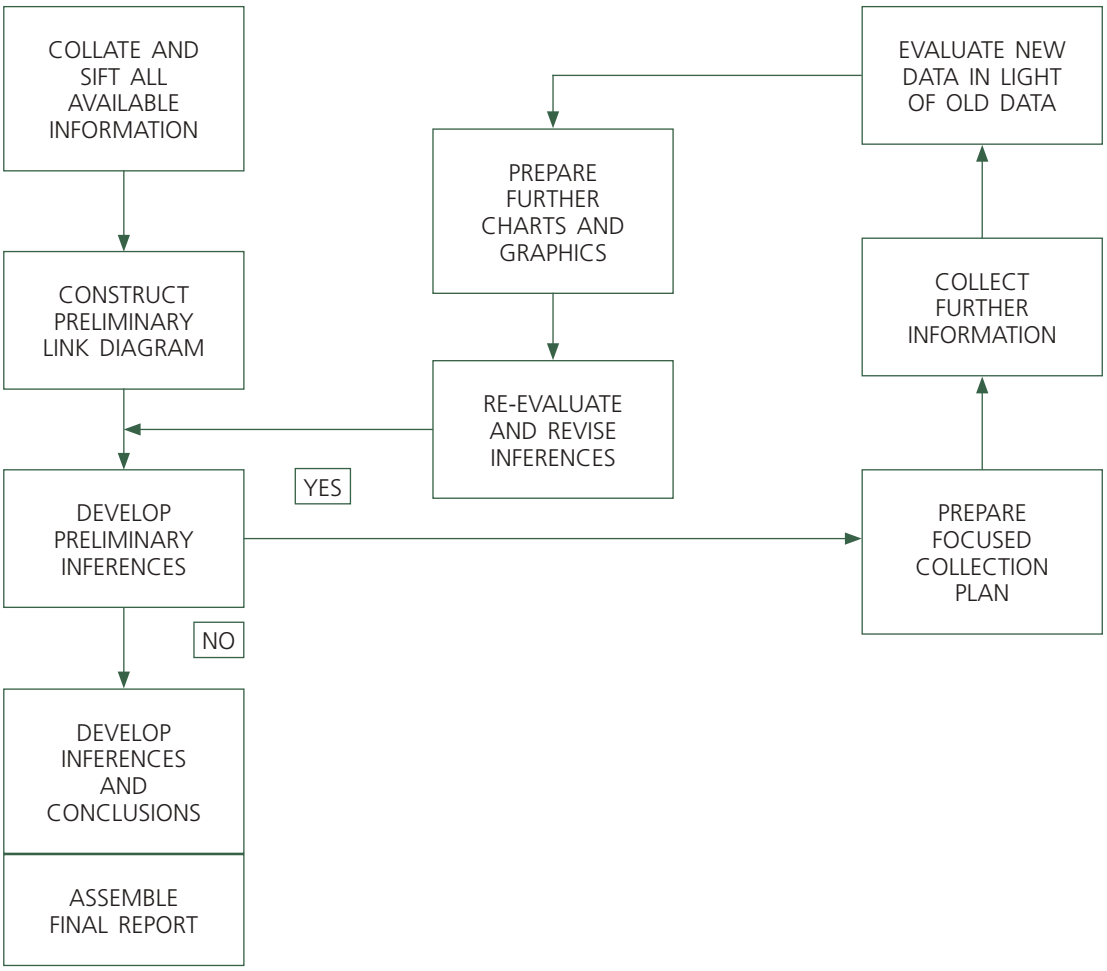
Once intelligence is integrated into an analytical product, it follows that if the product contains any intelligence graded at 'secret', then the whole document would have this protective marking. Similarly if any item was graded with a handling code of 4—dissemination within originating agency only—then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

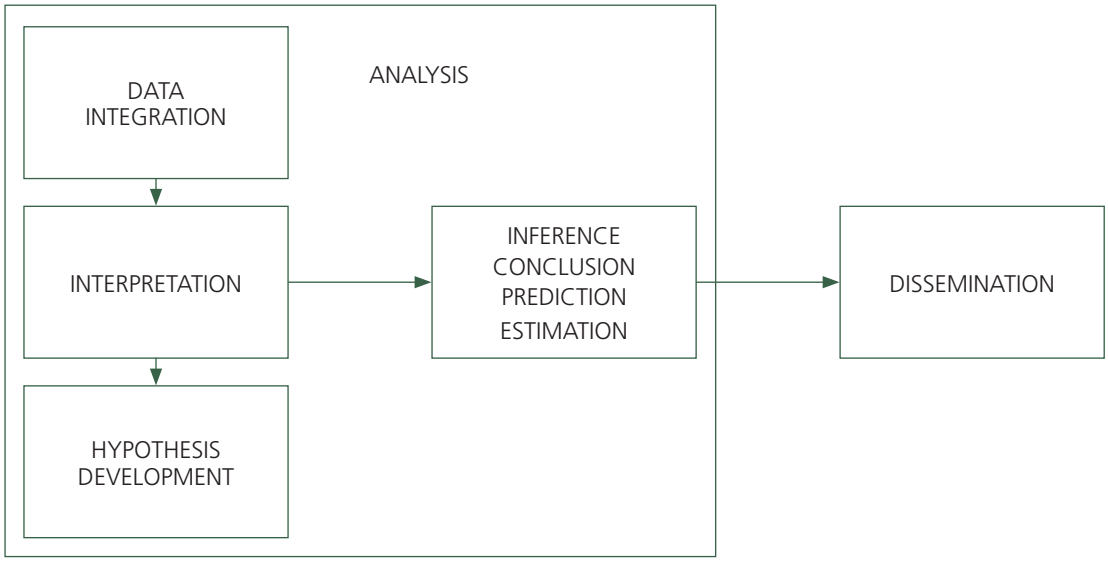
DATA INTEGRATION: COMBINING DATA IN PREPARATION TO DRAWING INFERENCES

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. Basis analysis techniques: link analysis

## INTRODUCTION

Much raw data in an investigation is collated into complex and detailed written reports. Other data pertinent to the analysis of the criminal enterprise or suspected criminal activity is frequently voluminous, and varied in form.

The basic problem for intelligence analysts is putting information together in an organized way so the difficult task of extracting meaning from the assembled information is made easier.

Link analysis puts information about the relationships among entities—individuals, organizations, locations, and so on—into a graphic format and context that will clarify relationships and aid in inference development. Link analysis can be applied to relationships among those entities, which might have been identified in a given analysis.

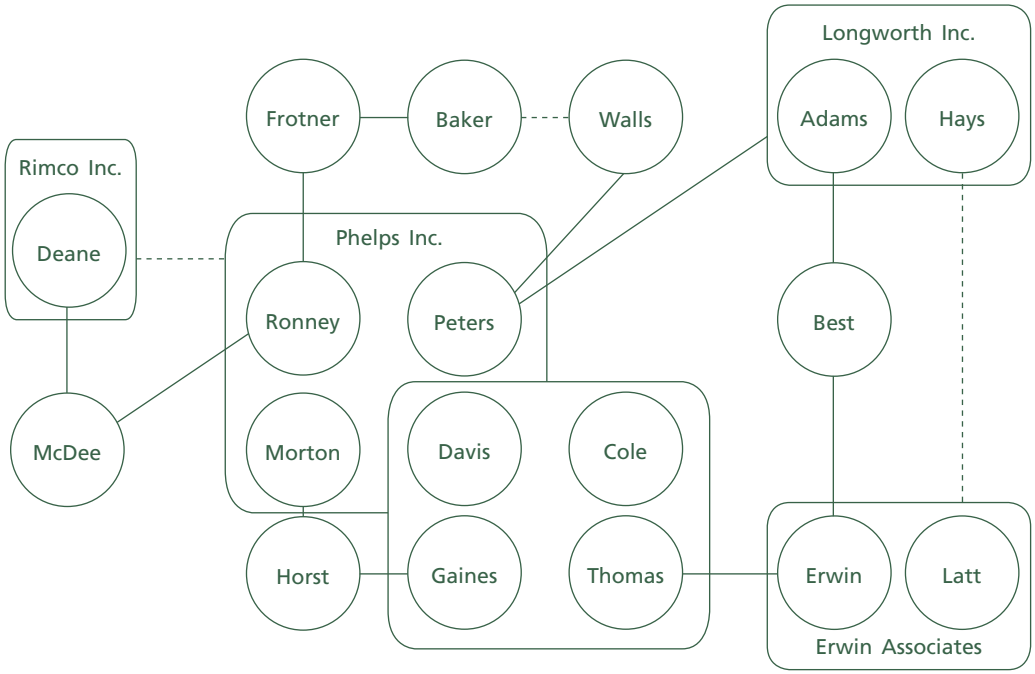
Link analysis is a seven-step process. The product of the process is a link chart such as the example shown in figure 6-1.

The seven steps of link analysis are:

1. Assemble all raw data
2. Determine focus of the chart
3. Construct an association matrix
4. Code the associations in the matrix
5. Determine the number of links for each entity
6. Draw a preliminary chart
7. Clarify and re-plot the chart

Please note that the following detailed methodology describes the application of link analysis by manual means. The use of computer applications greatly simplifies the mechanics of this process but the still requires the same analytical thought process to be followed.

**Figure 6-1. Example link diagram**




*1. Assemble all raw data*
Assemble all relevant files, field reports, informant reports, records, etc.

*2. Determine the focus of the chart*
Identify the entities that will be the focus of your chart. Read through your data and underline or highlight these entities, which may include names of people and/or Organizations, auto license numbers, addresses, etc.

*3. Construct an association matrix*
An association matrix (figure 6-2) is an essential, interim step in constructing a link chart. It is used to identify associations between entities but is not used for presentation purposes. Regardless of which charts are going to be constructed, an association matrix should always be constructed first.

**Figure 6-2. Example association matrix**
**The basis of the association is mileage between cities**

The distance between London and Rio de Janeiro can be found at intersection of the London column and the Rio de Janeiro row, which in this case shows 5,750 miles. This is the association between the two cities

The entity names, which are the subject of the chart construction, are entered on the diagonal axis of the matrix.

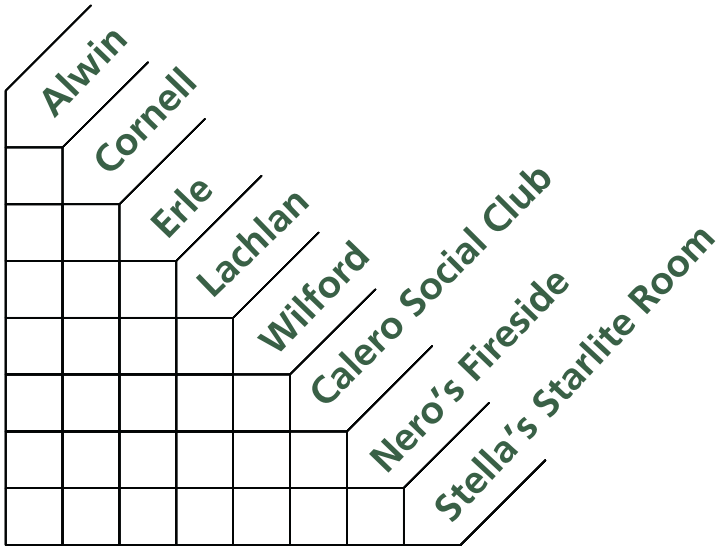
Individuals should be listed in alphabetical order.

Organizations should be listed in alphabetical order, after the individuals.

When Vehicle Registration Marks or addresses etc. are the entities being used, they should be arranged in alphanumeric order after the organizations. This action will assist when checking the matrix.

Inserting an asterisk character (*) prior to the name of the entity may facilitate the counting of the associations.

**Figure 6-3. Association matrix using names of individuals and organizations**




For the matrix shown in figure 6-3 the basis of the association will be evidence of a confirmed or possible linkage between individuals, an individual and an organization, or organizations.

*4. Code the associations in the matrix*

Association codes are used to indicate the basis for or nature of each relationship shown in the matrix. Suggested association codes and their possible meanings are shown in figure 6-4.

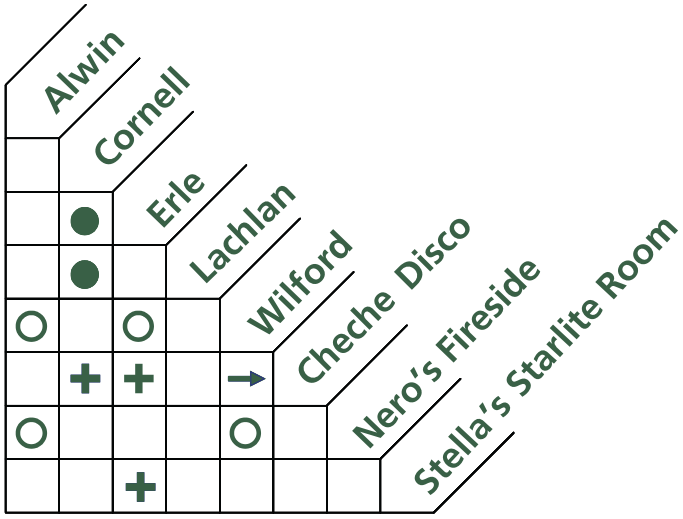
**Figure 6-4. Suggested association codes**

| Association codes | |
|---|---|
| **Code** | **Meaning** |
| ● | Confirmed association between two entities |
| ○ | Suspected association between two entities |
| + | Confirmed member of the organization—officer, manager, employee, club member |
| — | Suspected membership in the organization |
| ➔ | Confirmed investment with no other participation—shareholder, limited partner (direction from owner to owned) |
| ▸ | Suspected investment with no other participation (direction from owner to owned) |

Confirmed links are where the information has been evaluated as A1, A2, B1, or B2.

Unconfirmed links are where the information has been evaluated any other way.

**Figure 6-5. Completed association matrix**



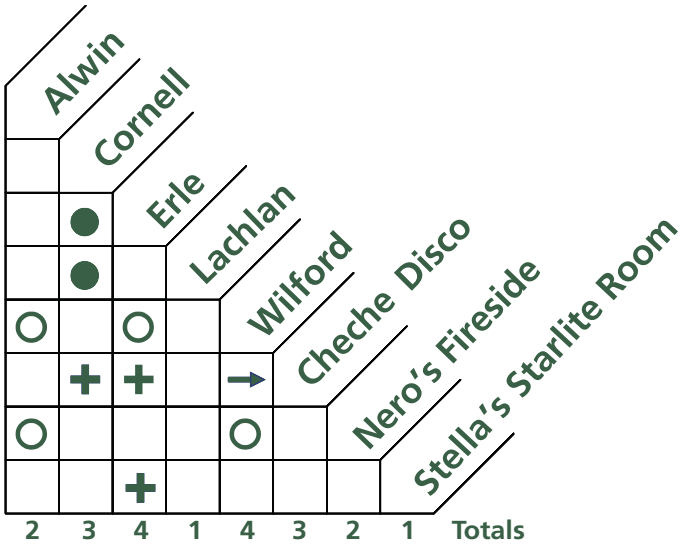

The entries are interpreted as follows:

- Cornell and Erle, a confirmed association
- Cornell and Lachlan, a confirmed association
- Alwin and Wilford, an unconfirmed association
- Erle and Wilford, an unconfirmed association
- Alwin, an unconfirmed association with Nero's Fireside
- Cornell, a confirmed participant in Cheche Disco
- Erle, a confirmed participant in Cheche Disco
- Wilford, an unconfirmed association with Nero's Fireside
- Erle, a confirmed participant in Stella's Starlite Room
- Wilford, confirmed stockholder in Cheche Disco, not an officer

*5. Determine the number of links for each entity*

A useful way to start your chart is to count the number of links associated with each entity in the matrix. Be sure to count across and down for each entity. Figure 6-6 illustrates the procedure.

**Figure 6-6. Sum of links for each entity**




*6. Draw a preliminary chart*

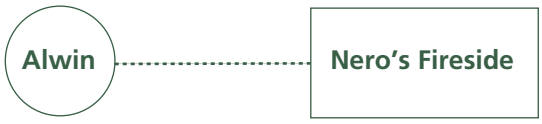
Draw a chart that shows graphically all of the information contained in the association matrix. This can be done by choosing and using corresponding symbols. The preliminary charts shown in figures 6-7 and 8-8 use circles to represent individuals and rectangles to represent organizations.

**Figure 6-7. Confirmed link**


Confirmed links are shown with solid lines and suspected links with dotted lines. Ownership may be noted with a percentage label on a solid line.

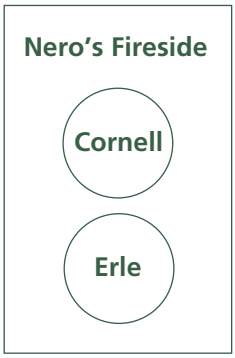
There is a confirmed link between Cornell and Lachlan, based on information.

**Figure 6-8. Unconfirmed link**




There is an unconfirmed link between Alwin and Nero's Fireside based upon information.

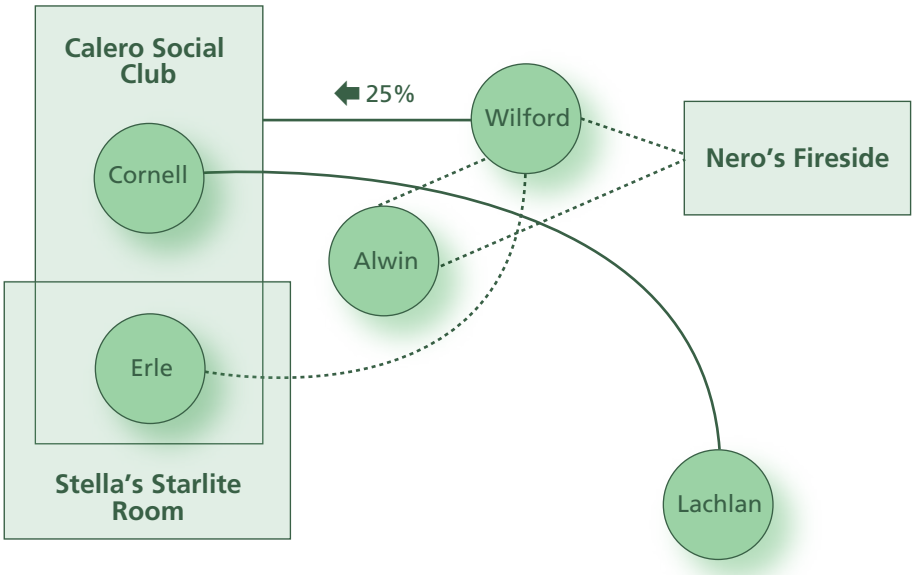
**Figure 6-9. Entities within an organization**




Cornell and Erle are concerned in the organization of the Calero Social Club example: Secretary and Manager.

There may be an implied link between the two individuals due to their roles within the organization. A solid line between the two would indicate a definite association between them. In the example shown in figure 6-9, there is no information available to support the link. However, based upon your analysis you may feel there is cause to show a hypothesized link line.

**Figure 6-10. Preliminary link chart**




*7. Clarify and re-plot the chart*

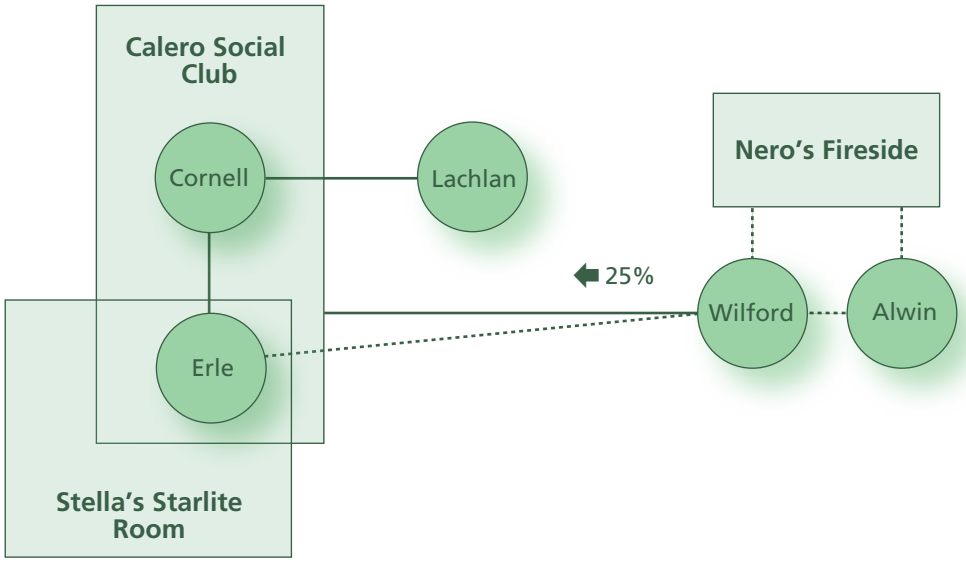
The lengthy and/or crossed lines that result when locating entity symbols may confuse the relationships shown or make interpretation difficult. Redrawing the chart can help clarify the relationships among entities.

Completion of this step resulted in the final chart shown overleaf. All charts should be timed, dated and sequence numbered. This will assist in discriminating between older and more recent charts and reveal to the viewer when the chart was constructed—a factor particularly relevant with regard to disclosure issues.

A key should be added to the chart.

Completion of this step resulted in the final chart as shown in figure 6-11.

**Figure 6-11. Re-plotted chart of figure 6-10**




## LAYOUT OF CHARTS

Chart layout can be enhanced by the imagination of an analyst and therefore can vary considerably in form.

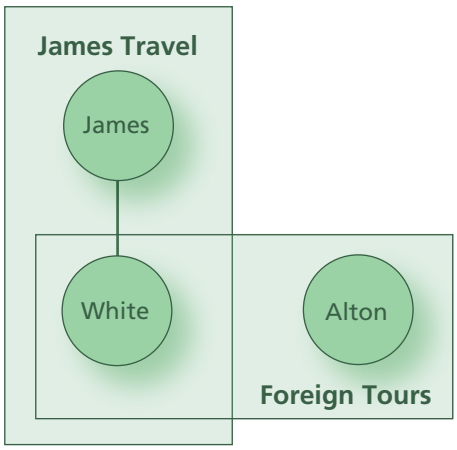
However, the fundamental principle is that charts must simplify information, in other words the "picture paints a thousand words". Therefore the chart should be clear, uncomplicated, uncluttered and concise. A number of ideas are available and only experience will show whether a chart satisfies all of these criteria.

Invariably the chart you create today will not be as good as the one completed tomorrow.

## CHART LAYOUT EXAMPLES

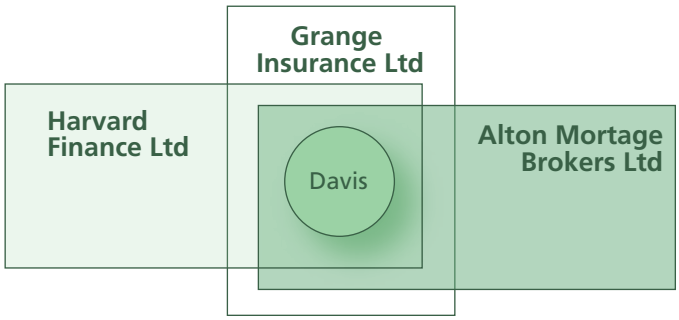
An individual involved in two companies with one other official involved in each of them:

**Figure 6-12. Layout example 1**



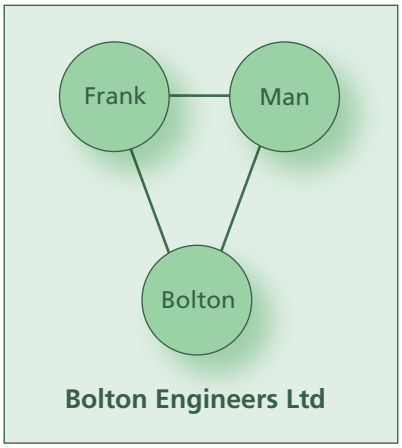
An individual involved in three companies, no other official involved:

**Figure 6-13. Layout example 2**



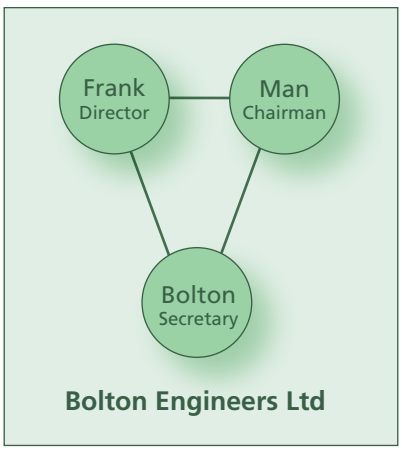

Three individuals in one company with links shown (official position not depicted):

**Figure 6-14. Layout example 3**



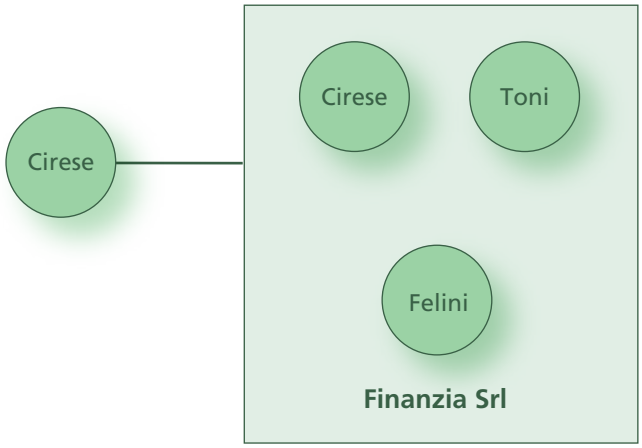

Three individuals involved in the same company, links inferred and official position shown:

**Figure 6-15. Layout example 4**



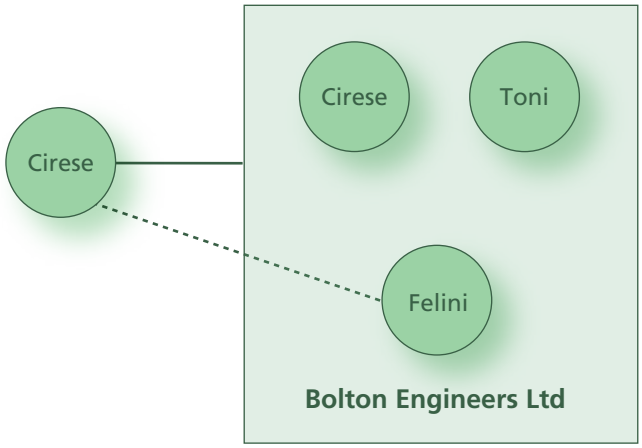
Individual linked to a company but not to the individuals shown as officers of the company:

**Figure 6-16. Layout example 5**



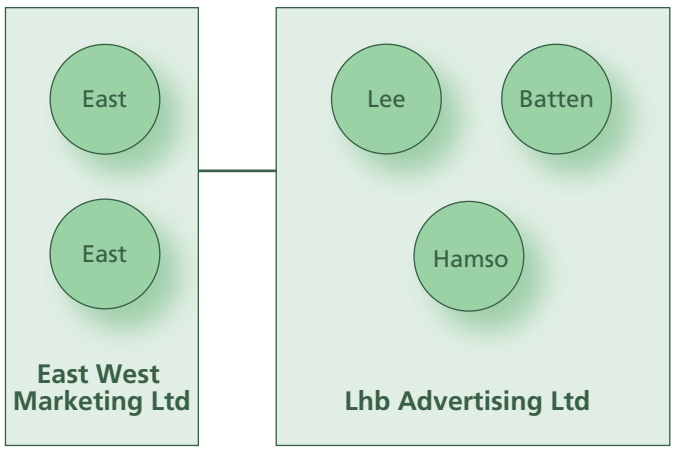

Individual outside a company but with a link to the company and a suspected link to an official of the company:

**Figure 6-17. Layout example 6**




Association between two companies but no known links between the individual officials of the companies:

**Figure 6-18. Layout example 7**

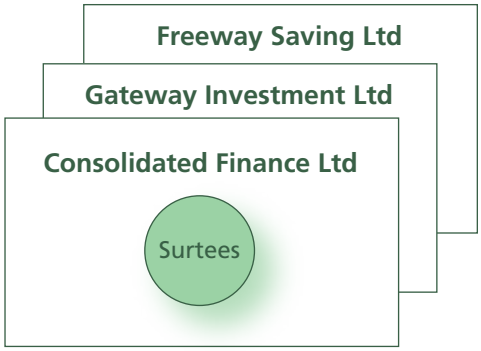


An individual associated to an unknown person:

**Figure 6-19. Layout example 8**

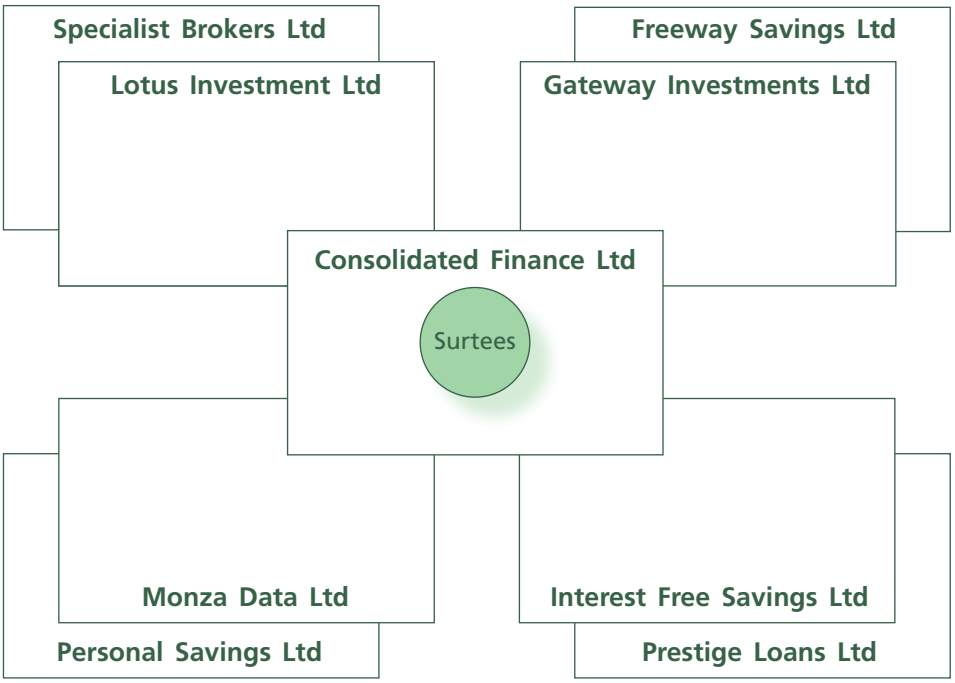

An individual who is an official of a number of companies, which are subsidiaries of each other:

**Figure 6-20. Layout example 9**




A company which has many subsidiary companies:

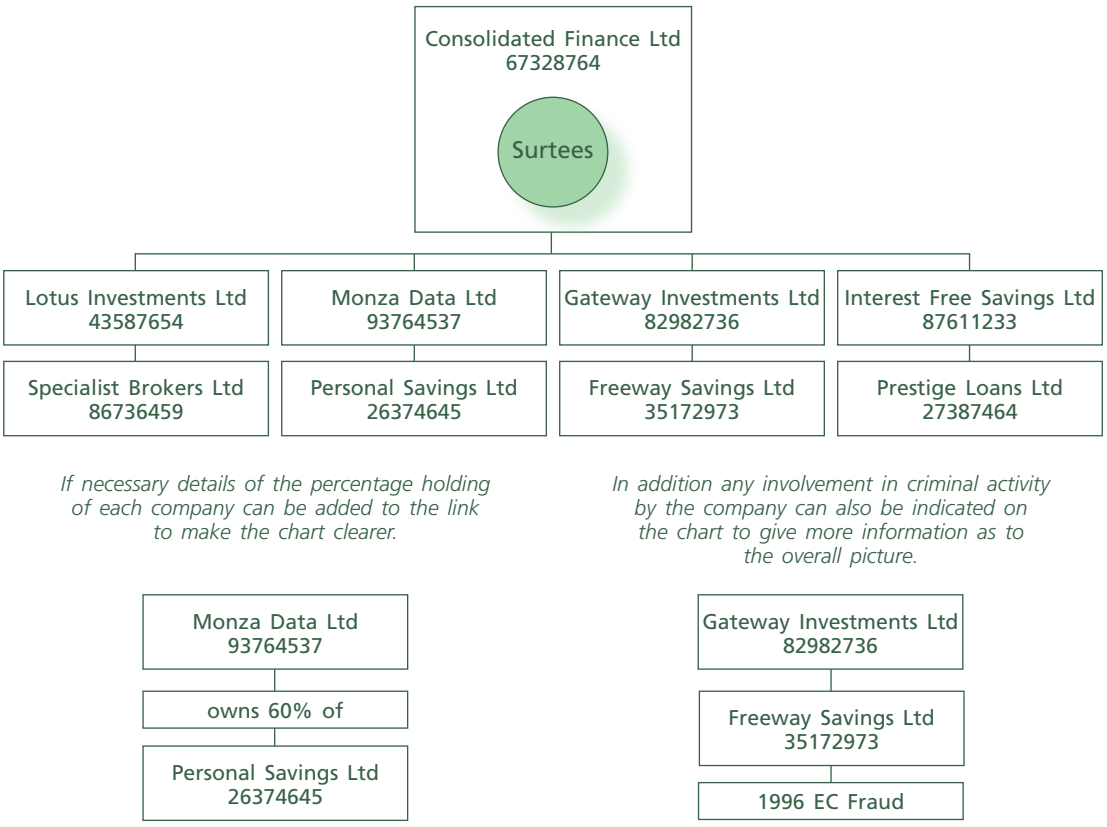
**Figure 6-21. Layout example 10**



This type of chart can also be depicted in the same way as a family tree. Quite often when information is sought on companies there is an indication in commercial databases such as the Dun & Bradstreet Worldbase as to parent company and ultimate owner. Company names and reference numbers and executive names can be searched to find other linked companies. In financial investigations these are particularly useful.

A charted example of this type of information is as follows:

**Figure 6-22. Layout example 11**




Producing a link chart is but a pre-requisite of association analysis. A chart is not in itself an analytical product, it is an analytical tool. Link analysis should not just look at connections, but also at the strengths and relevancies of relationships.

THE IMPORTANT FEATURES OF A NETWORK ARE CONTAINED IN FOUR CONCEPTS: ENTITY, RELATIONSHIP, DIRECTIONALITY, STRENGTH

- *Entities*, are the items under investigation which could include people, businesses, organizations, means of transport, locations, events, objects etc.
- *Relationships* can be familial or based on give and take such as reciprocity (exchange and compromise), suitability (the right person to do the job), bonding (past associations), control (criminal hierarchy or threat), predominance, superiority, subordination and succession.

- *Directionality* relates to the flow of information, favours and authority and enables understanding of the internal mechanics of a network.
- *Strength* is a subjective judgement based on interactions included in the relationships and evaluation of the data provided.

Association analysis as a process would involve information on a variety of linkages from a rich database.

A chart is a working product from which hypotheses could be gleaned regarding the status of associations among the members of the organization or network. Features of a thinking association analysis include looking at relationships and links, their strengths and purposes, what those links mean to the organization and to those investigating an organization.

Often an association chart shows only a "freeze-frame" snapshot of the group. It may be more appropriate to show the evolution of the group over time.

**Linkage issues in association analysis**

1. Who is central in this organization?
2. Which names in the database appear to be aliases?
3. The removal or incapacitation of which three individuals would sever a supply network?
4. What role(s) does a specific individual appear to be playing within a criminal organization?
5. Which communication links are most worth monitoring?
6. What patterns of interaction can be seen and how do these patterns allow us to understand and predict behaviour?
7. What is the nature of information exchanged between individuals in the group?
8. What group pressures or unwritten rules govern the activities of its members?
9. How often are the interactions?
10. Who is the initiator of the interactions?
11. Who forms a bridge or liaison between distinct organizations?
12. Who are the people who can take over the roles of the key personalities if they are removed?
13. What do the organization's financial links tell us about its operations?
14. What business links does it have?
15. What links to other criminal activities does it have?
16. What are the links to geographical locations, 'the territory'?

17. What is the hierarchy of the organization?
18. How is the criminal activity organized?
19. Does the group organization make it vulnerable to infiltration?
20. Could the organization be prosecuted under racketeering or continuing criminal enterprise statutes?
21. Have the links changed over time?
22. What previous bonding elements are known?
23. Are the links changing in strength or centrality?
24. Are certain members connected to some other members to the exclusion of the others?
25. Are there criteria for membership in the organization?
26. What is the organization's propensity towards use of violence?
27. Are there any links between the criminal group and a regulatory or government structure?
28. What is known of the management philosophy of the group's leader?
29. Can this model of linkages be applied to other criminal organizations?
30. Have there been other groups with similar structures before in this or other jurisdictions?
31. Does this group's structure enable us to predict the structure of future similar crime groups?

*Association Analysis Format Model*

This should consist of the following:

- An executive summary of the findings of the analysis.
- An overview of the group with the answers to those questions pertinent from the previous list of linkage issues.
- A link chart or series of charts, depicting the group.
- Biographical summaries on each investigation target and potential target.
- Conclusions about the group.
- Recommendations for further tactical or strategic action, including a list of questions to be answered
- and the possible sources of information (highlight intelligence gaps).

Applying the Process-Oriented Approach to association analysis, the standard seven-step process described at the beginning of this chapter can be expanded in the following way:

1. Collect data
2. Organize/collate data
3. Extract association material
4. Prepare association matrix
5. Prepare link chart
6. Produce biographical summaries of entities in the chart
7. Summarize chart
8. Apply questions/issues as appropriate to organization or network
9. Establish what necessary information is present and what is absent
10. Draw interim hypothesis(es)
11. Develop a list of unanswered questions and recommendations for collecting that information and for further investigative or prosecution steps to be taken
12. Present findings and a written report to management

# 7. Basic analysis techniques: event charting

An event chart is an appropriate tool for developing meaning from a related set of events. An event chart shows a sequence of events so that the times of occurrence and the relationships among the events become clear. The event chart should be developed early in the analysis of a complex case. The event chart consists of the following components:

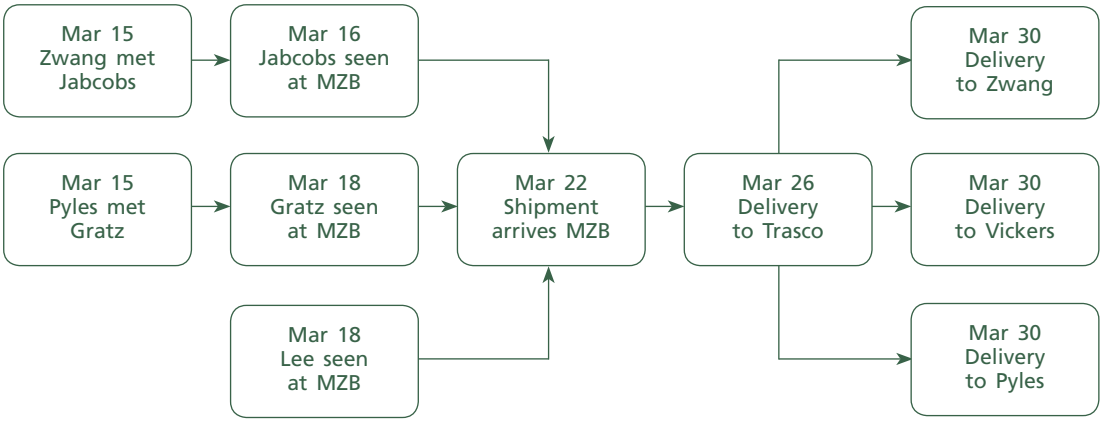
- Brief descriptions of events are contained in symbols such as circles or rectangles. Ensure that in any one chart a symbol represents the same thing whenever it is used. Keep the descriptions of events short—no longer than three or four words.
- Connecting lines are used to indicate relationships among events—the time sequence of events in which one event leads to another.
- An arrow on each line indicates the sequencing of the events—the flow of events through time.
- The date and/or time associated with each event is tied in some way to the description of the event—within the event symbol, close to the symbol, or linked to the symbol.

Since events are often not reported in sequence, take careful note of dates and times. These components can be combined into an event chart in a variety of ways, limited only by the objective of the analysis and the creativity of the analyst. The governing factors in constructing an event chart are *(a)* to provide a clear and accurate presentation of the information and *(b)* to keep the chart as simple and to the point as possible.

The final chart is a powerful tool for the analyst to visualize the importance of events in a criminal activity. Anything that might detract from this visualisation should not be contained in the chart.

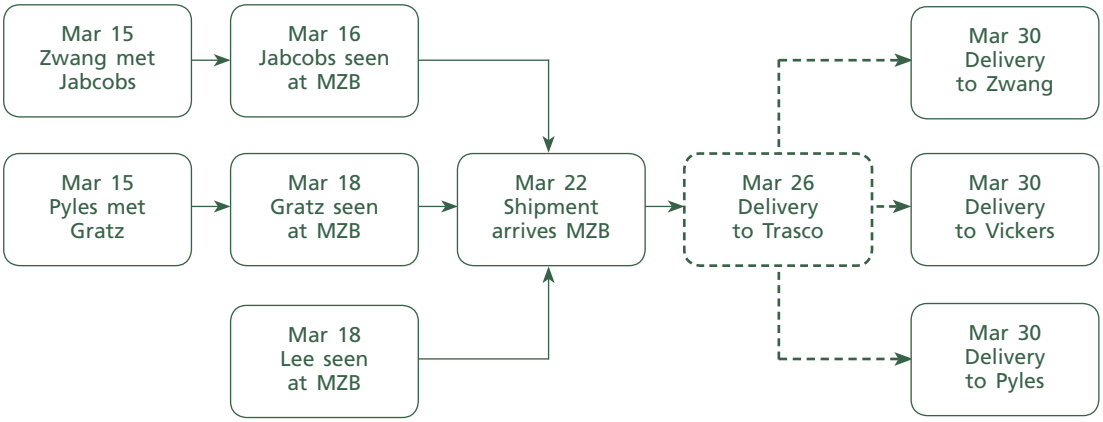
The most commonly used type of event chart is the one shown in figure 7-1. In this chart, all information except the connecting lines and arrows is contained within the event symbol (the date and the description of the event).

**Figure 7-1. Example of an event chart**



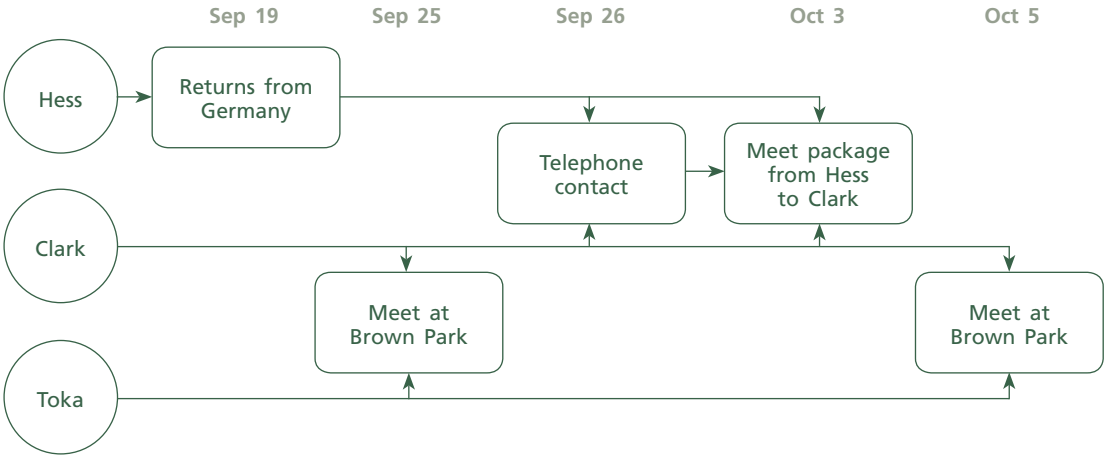

An event chart can show both verified and hypothesized information. For example, under other circumstances, we may suspect that a delivery was made to Trasco on March 26. However, we have not yet confirmed that it was. A hypothesized event is shown in the chart in figure 7-2.

**Figure 7-2. Example of an event chart with a hypothesized event**




If it is important to reveal the pattern of events surrounding several entities—individuals or organizations—an event matrix chart might be the more appropriate. An example of an event matrix chart is shown in figure 7-3.

**Figure 7-3. Example of an event matrix chart**



The term matrix is applied because the chart (figure 7-3) lists individuals along one side of the matrix (the left-hand side in the example) and time along the other side (along the top in the example). In this format, significant events are plotted at the intersections between times and individuals. Arrows go from an individual only to the events in which that individual is involved. If more than one individual is involved in an event, show the symbol between the individual's lines.

In general in event matrix charts, the horizontal scale is time and the vertical one divided into themes which can be persons, telephones, vehicles etc. or any combination of such entities. Event matrix charts can be extremely large and complex and are best generated using bespoke computer software packages.

# 8. Basic analysis techniques: flow analysis

The majority of criminal organizations carry out their activities in order to obtain some form of commodity, such as money, drugs, and goods in order to generate wealth.

All these commodities need to flow through an organization and if this flow is understood then knowledge of how the organization works can be obtained, thus making for more efficient law enforcement action. For instance, by understanding the flow of money through an organization you can identify the roles of individuals in a complex money laundering enquiry, often identifying the key figures in the organization.

If this is linked to a drug enquiry then these people are often not involved with the drugs themselves and separate charts can be created to show the movement of drugs or flow of money through the organization. In many cases the flow of the commodity indicates the hierarchical make up of the organization which in turn leads to an understanding of the power base of the organization. Flow charts can also be produced to show intangible activities such as political influence or supervisory control.

As with all charts they are the imagination of the analyst, however the one underlying important factor to remember is that the connecting line will have an arrowhead, either at one end or both, to depict the flow. An example of a flow chart is shown in figure 8-1; note there is no indication as yet to the nature of the commodity, only chartist flow.

**Figure 8-1. Example of a flow chart involving individuals and organizations**

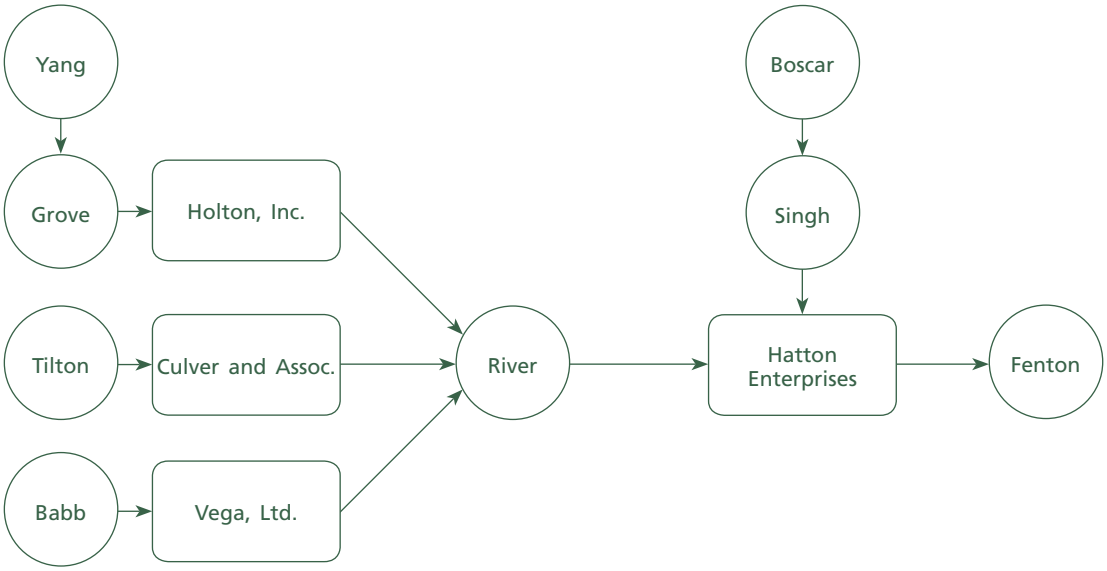


**Figure 8-2. Futher flow chart involving organizations and individuals**

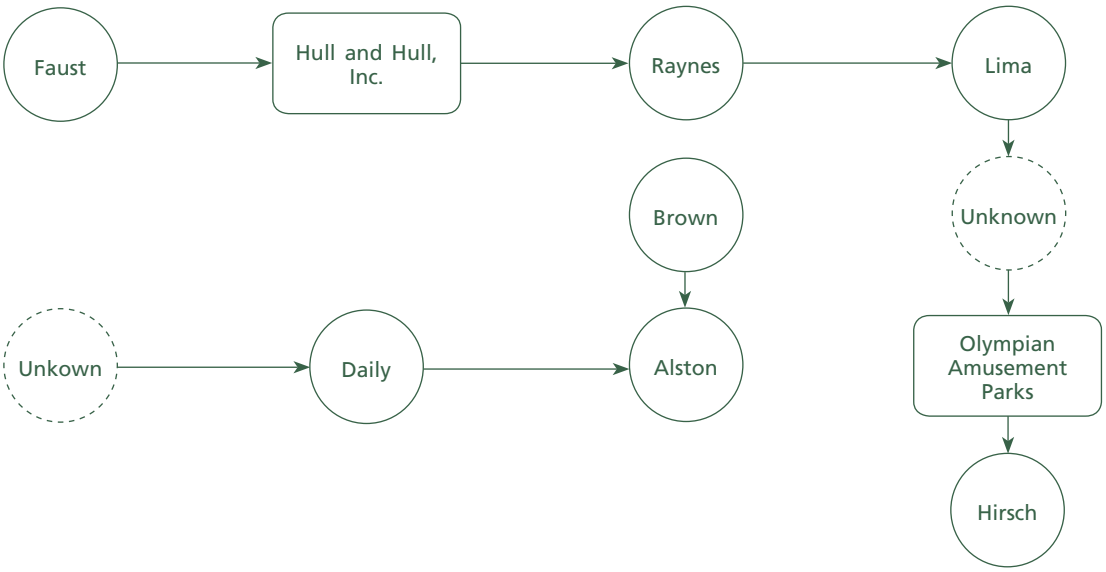



Figure 8-2 includes two individuals whose identity is unknown. The chart shows the paths by which the commodity flows to Hirsch.

Flow chart analysis can be applied for a variety of purposes. It is often used to complement and corroborate the results of association analysis. The most common subcategories are:

- Commodity flow analysis
- Activity flow analysis
- Event 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, the 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/her behalf.

A commodity flow chart will normally include a reference to the commodity or/and any numerical value which describes a particular transaction, e.g. money units or weight on the label of the directional arrow that represents the "flow". Dates are also shown, when possible, to indicate the time span of the activity.

Commodity flow analysis aims to answer questions, such as:

- Who ends up with the largest amount of the commodity in question?
- Are there locations and individuals shown, to which (whom) the commodity is siphoned?
- If a criminal hierarchy is involved, what does the flow of the commodity indicate to us about the relationships within that group?

A commodity flow chart often reflects or exposes the structure of a criminal organization. It can provide insight into who are the apparent and more hidden operators and beneficiaries of the criminal activity under investigation. It can help to hypothesise about the nature of the group and the extent of its activity. Obvious uses for commodity flow charts include applications to stolen property, bribery, drug distribution, money laundering.

A commodity flow matrix is often used for manual generation of commodity flow charts. It is prepared in a similar manner to a telephone record matrix (see chapter 9). The data inserted

reflects the goods or currency moving among the people and/or businesses involved. The names of the sources from which the commodity originates are arranged in a logical order across the top of the matrix or down the left side. They are then followed by a logic arrangement of the names of the receivers of the commodity. The bottom and right side are left free for "from" and "to" totals. This design of the matrix allows the analyst to keep track of the flow of a particular commodity from origin to destination.

There are two approaches to the construction of a flow chart.

*Approach 1:*

- Construct a link chart first;
- Identify the links that are associated with the flow of the commodity of interest;
- Construct a flow chart using those links.

**Figure 8-3. Construct link diagram**

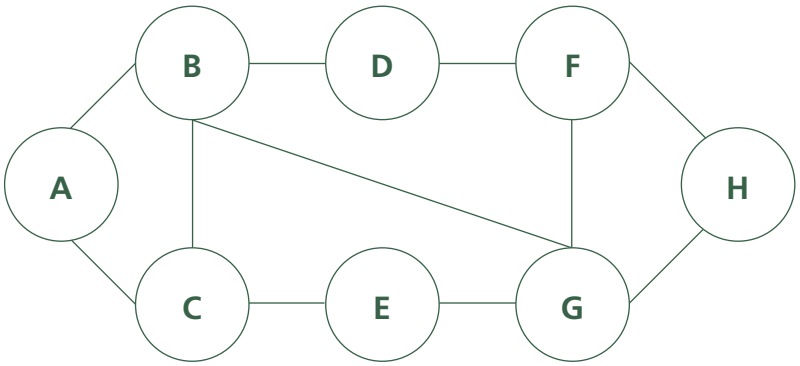



**Figure 8-4. Identify flows links**

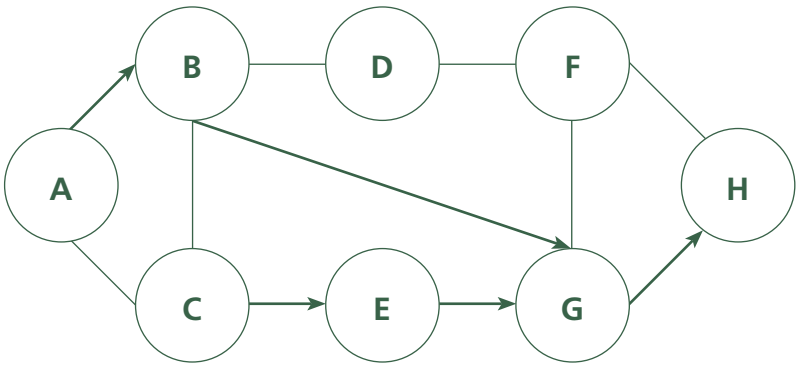
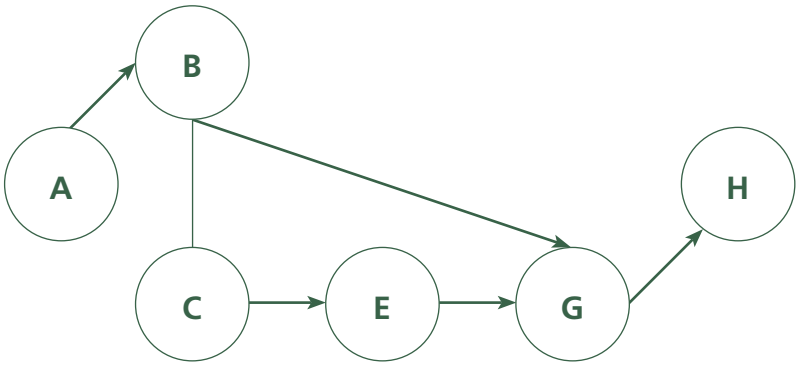



**Figure 8-5. Extract flow chart**



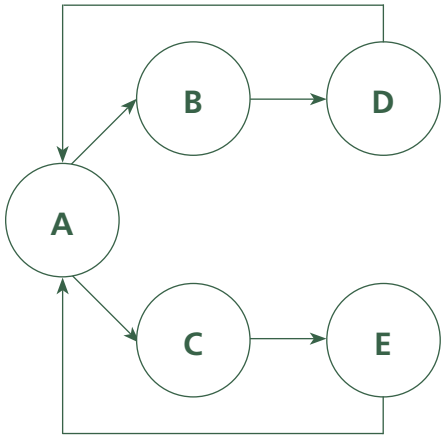
*Approach 2:*

- Assemble all raw information
- Determine the commodity which is being targeted
- Construct a square association matrix
- Enter link codes in the matrix
- Determine the number of links
- Draw the chart; clarify and re-draw it as necessary

**Figure 8-6. Square matrix with flow link codes entered**

| From | To | | | | | Totals |
|---|---|---|---|---|---|---|
| | A | B | C | D | E | |
| A | | • | • | | | 2 |
| B | | | | • | • | 1 |
| C | • | | | | | 1 |
| D | • | | | | | 1 |
| E | • | | | | | 1 |

**Figure 8-7. Flow chart constructed from information contained in the matrix**

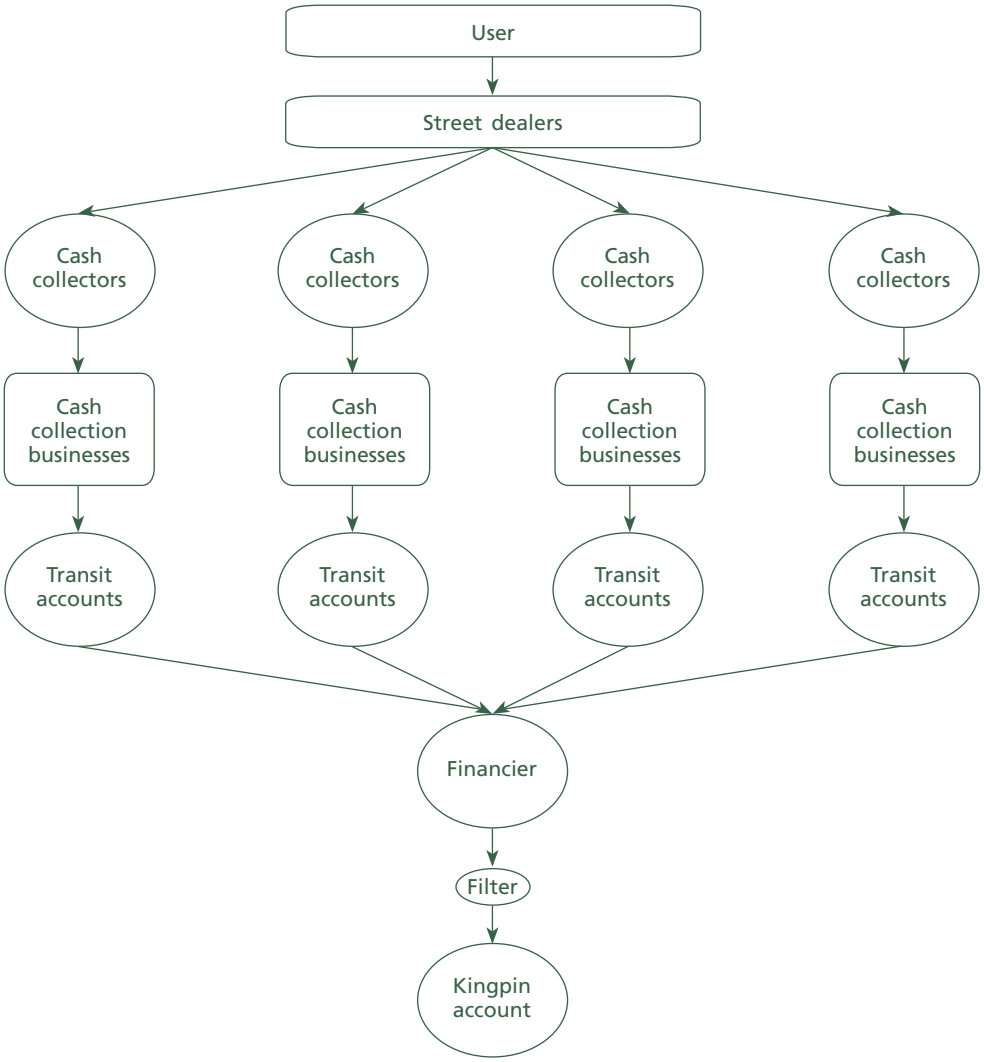



*Activity flow analysis* is used to provide a generic view of a set of criminal actions, or operational modalities, to determine what the key actions were and provide an overview of a crime. An activity flow chart shows general steps needed to complete a particular process. It differs from the event flow chart in that the latter is more specific and uses exact occurrences and dates, while an activity flow chart provides an overview of occurrences and generally does not use dates.

Activity flow charts are made by gathering information on the events which occurred in a process or series of similar processes, and generalizing them to depict a hypothetical, rather than a specific, process.

Activity flow charts can be used to explain complex processes, such as money laundering or securities manipulation. They can also be used in place of event flow charts to avoid disclosure to non-vetted audiences of specific investigation-sensitive information. Activity flow analysis can also be used to create a comparison between crimes or crime operations to see if there is a similarity or a connection between them.

**Figure 8-8. Example activity flow chart**
**Hypothical flow of money in a drug trafficking organization**




*Event flow analysis* is the compilation and analysis of data relating to events as they have occurred over time to allow the analyst to draw conclusions and/or make recommendations. They are used most frequently in relation to specific criminal violations, where the events leading up to and away from the violation need to be viewed in context.

Event flow analysis is a chronology of what occurred within the framework of a criminal activity. That is, only the events which impacted on or were part of the criminal activity should be noted. To complete an event flow analysis, one must review all case documents for events that occurred. These events are placed in a manual ledger or a computerised data base. The system of collation must permit extraction of the data by date and, if necessary, by hour. Once put in proper order, the events are reviewed to determine their importance for inclusion in the chronology.

The event chronology made be visualized in an event chart or in a chronological table, showing the date/time of the event in one column and a brief description of the event in the other. Chronological tables can be automatically generated from random data by commercially available spreadsheet programmes.

Event flow analysis can result in the determination of operating modalities if the events that occurred in a series of crimes are compared for similar attributes.

Event flow charts can be either simple or matrix.

**Figure 8-9. Simple event flow chart**

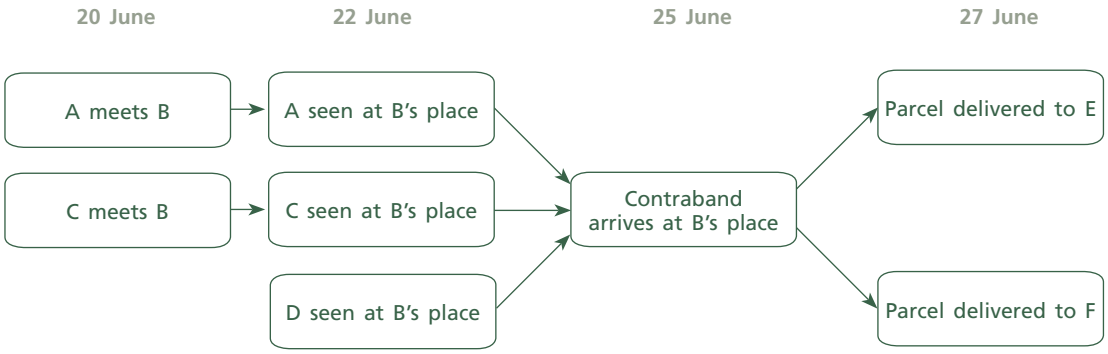
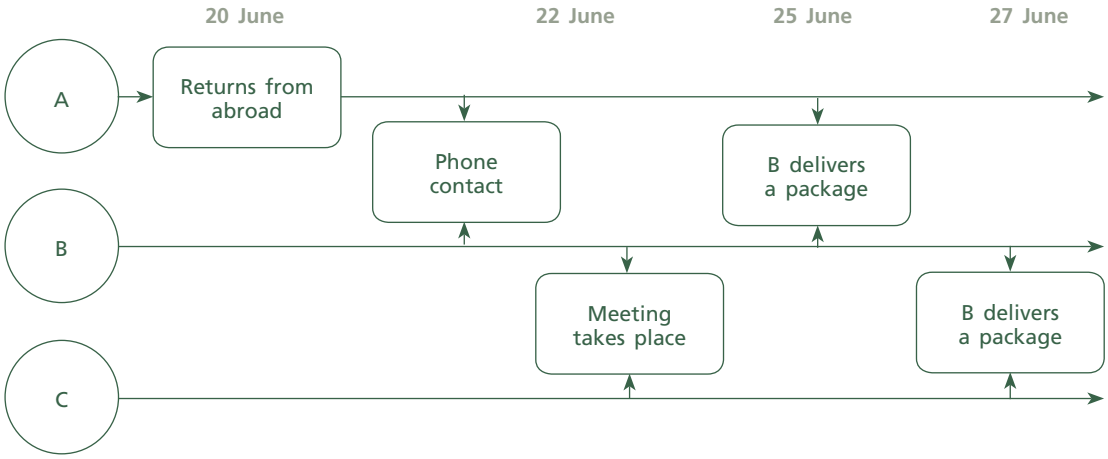



**Figure 8-9. Matrix event flow chart**




Matrix event flow charts, similarly to matrix event charts in general, are often extremely large and complex and are best generated using bespoke computer software packages.

# 9. Basic analysis techniques: telephone analysis

Telephone analysis represents one of the most widespread techniques that can produce illustrative and useful results. It can be subdivided into quantitative or statistical analysis and association analysis. Quantitative analysis aims to establish patterns in data on the basis of numeric parameters of a phone call—day, time, duration. Association analysis uses the results of the statistical analysis and link diagrams to produce hypotheses about the purpose and content of the calls, i.e. relationships and purpose of contacts of the targeted individuals.

The key to interpreting telephone data is in recognizing that it is simply a form of directional data, and thus is ideally suited to being charted using conventional flow charting techniques of the types already covered in this chapter.

Data routinely collected by the telephone companies as part of their normal business with customers can be accessed with comparative ease and minimum expenditure of resources. Perhaps the most important feature of this type of information is that it is freely (and thus in general truthfully) given by the customer, and can be retrieved from the telephone companies without direct contact with the customer. However, it is now a process of which criminals are now routinely aware and try to circumnavigate.

It should be emphasised at this point that what is being discussed is not telephone tapping. No information whatsoever as to the identity of the person actually making or receiving a call or as to the content of the call is retrieved by this technique.

What is generated, however, is information regarding traffic between specific telephones/ telephone lines.

Each of these types of connection (between normal telephones, mobile telephones, pagers, fax machines, computers, in fact any means of communication connection type) represents a potentially valuable source of information, however, the sheer number and variety of these "information sources" can be problematical to the investigator. Firstly, the detail of information the analyst can access varies between sources. Incompatibility of data and the simple practical difficulties of retrieval from different sources restrict to some extent the use to which the information can be put, particularly where time is a factor. Wherever possible, data should be obtained in structured electronic format and not in paper from.

Secondly, the computerization by the suppliers of their customer databases creates further procedural problems in terms of data protection.

Despite these factors, as will be seen, the benefits of using telephone information far outweigh the disadvantages, particularly when the results of telephone analysis are combined with analysed information from other sources.

What can telephone analysis do for the analyst and the investigator?

- The identification of telephone numbers dialled by a suspects telephone, which may open other lines of enquiry
- The identification of patterns and common numbers that are called
- The frequency of calls
- Potentially, the identification of associates
- Location of caller (mobile phones)
- Be very resource effective

You should be aware as analysts that if called upon to conduct telephone analysis certain authorities and procedures may exist for obtaining such data, this is likely to differ from country to country. In addition, each company will provide the data in differing formats. We recommend that you familiarize yourself with your own country's procedures, and points of contacts once you have completed the course. In general, the analyst can expect to obtain information on a particular telephone/subscriber in specific areas as follows:

- Subscriber's name/address;
- Subscriber's connection number(s);
- Subscriber's account details;
- Payment details (bank/branch/account references);
- Contemporaneous record of connections made (over a particular time period) with details of:
  - Other numbers called;
  - Time, date, duration etc. of each call;
  - Mast locations of mobile phone calls.

Clearly the majority of this information relates to the links between entities (subscriber numbers) rather than the people involved. In order to better describe this information, therefore, a square association matrix and slightly modified form of flow charting is used. Minor additions to the basic flow chart techniques and symbols are used so that the chart is able to illustrate extra information about each link far more clearly than would be the case with just a normal flow chart, specifically so that a single link line can visualize flow and volume information in both directions. Despite these modifications, a telephone toll analysis chart is still merely a flow chart suitably amended to show the information forming each link in greater detail.

To enable the analyst to begin to describe and analyse telephone information, in most cases at least the following detail would be required:

- The number initiating the call;
- The number receiving the call;
- The frequency of traffic in either direction.

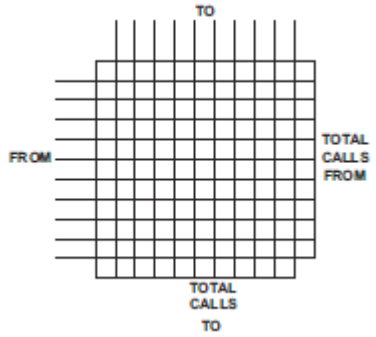
In order that the analyst can take into account the direction of each link between subscribers, a square matrix is used in place of the normal triangular matrix.

The telephone numbers of the calls initiated (made by the subscriber) will be listed in the vertical (from) axis on the left side of the square.

The telephone numbers of the calls received (by the subscriber) will be listed on the horizontal (to) axis on the top side of the square.

To accomplish this, the association matrix is modified slightly, taking on the form of a square. The vertical axis on the left side of the square will indicate initiation of a call. The horizontal axis on the top side of the square will indicate receipt of a call.

**Figure 9-1. Empty matrix**




The telephone link diagram can be constructed by following seven steps:

*1. Determine all numbers (always use dialling codes)*

Determine all of the telephone numbers involved in the traffic—the numbers of the originating calls and the numbers of the calls received.

*2. Arrange subscribers (in numerical order)*

Arrange all numbers in ascending order, including the area code. If there is more than one with the same area code, then arrange the numbers by area code first, then order within each area code. If numbers from different countries are included than care must be taken to ensure that all international codes are added to the data available.

*3. Enter subscribers (Vertical)*

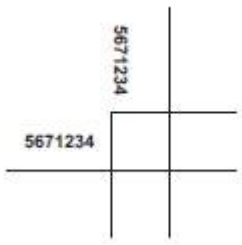
Enter all listings on the vertical axis at the left side of the square, beginning with the lowest area number at the top. Label the grouping "from", at the far left edge of the matrix.

*4. Enter subscribers (Horizontal)*

Enter all listings, in the same order, on the horizontal axis at the top of the square. Label the grouping "to," at the top edge of the matrix.

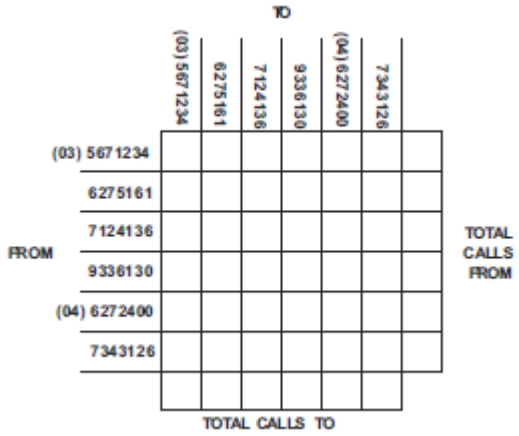
Caution: Make certain that you start the listing along the horizontal axis at the left of the square so that the first number is the same as the first number on the vertical axis.

**Figure 9-2. Matrix with one number**



Note how in figure 9-2 each number occupies the same position on both the horizontal and vertical axes. The completed matrix will look like that shown in figure 9-5.

**Figure 9-3. Matrix with all numbers**



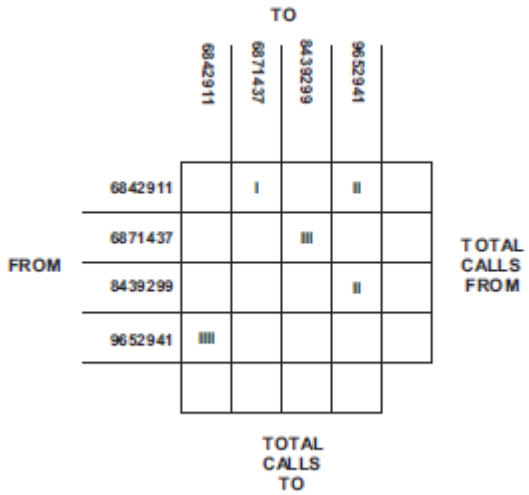

*5. Enter frequency of calls*

Note each call made from one number to another by making a small tally mark in the cell of the matrix, which is common to both listings.

**Figure 9-4. Example call frequency table**

| | Calling Number | | Number Called | |
|---|---|---|---|---|
| Example | 9652941 | calls | 6842911 | Four times |
| | 6871437 | calls | 8439299 | Three times |
| | 6842911 | calls | 9652941 | Two times |
| | 6842911 | calls | 6871437 | One time |
| | 84939299 | calls | 9652941 | Two times |

**Figure 9-5. Completed association matrix for the listed calls**



*6. Add the number of occupied squares for each number*

Count how many numbers have been called by each number (along the row) and how many numbers have called each number (in the column). The result represents the number of links, which must be connected to that number in the finished chart. As a starting point for the chart, the numbers with the largest numbers of links should be placed centrally on the chart.

*7. Develop a link chart*

Develop a link chart from the information contained in the association matrix. As in links among individuals and organizations, use lines to connect symbols representing the different telephone numbers.

In the telephone chart, however, add an arrow to indicate the direction of the call. For example, since calls went both from 01924-770792 to 0113-2928333 and from 0113-2928333 to 01924-770792, arrows would be shown below:

**Figure 9-6. Arrows showing the directions of calls**

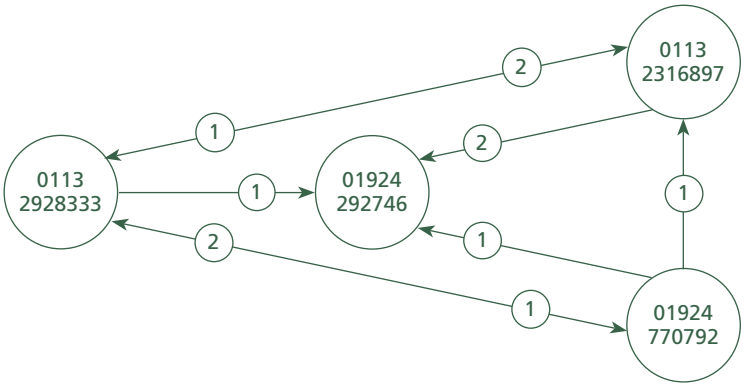

To show the frequency (total number) of calls, place a small circle on the line just before the arrow and insert the number of calls made in the direction of the arrow. This shows that 01924-770792 called 0113-2928333 twice and received one call from 0113-2928333.

**Figure 9-7. Showing both directions and frequency on the link chart**


**Figure 9-8. Alternative display method**


Transforming the information contained in the association matrix above into a link chart results in the chart figure 9-9 following:

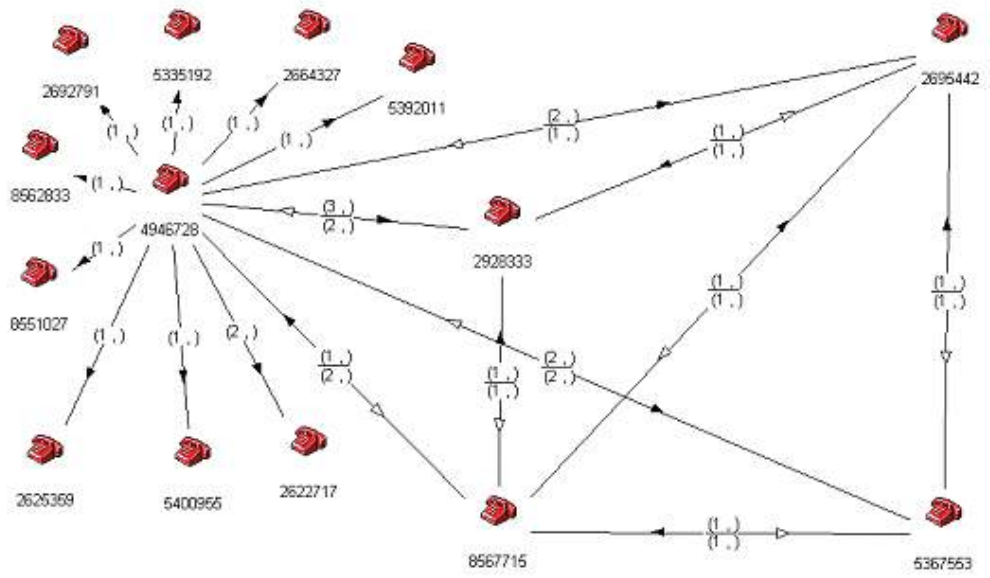
**Figure 9-9. Flow chart of example association matrix**



*Computer generated charts*

Generation of telephone analysis charts by hand is only possible for the most simple of datasets. Analytical software applications are now commonplace in the field of criminal intelligence for this and other techniques. Whilst the use of computers and related software is outside of the remit of this particular manual the techniques used are the same. A computer generated telephone analysis chart has been included to give some idea of what would be produced.

**Figure 9-10. Computer generated telephone analysis chart**




It should also be noted that telephone analysis in general has become a much more complex process in recent years. Often even the type of telephone analysis chart shown in figure 9-10 is likely to be too simplistic in relation to the volumes of data available and the counter measures frequently adopted by criminals to this type of law enforcement technique.

It is a common practice now for criminals using mobile phones to use pre-paid cards and switch handsets (IMEI numbers) and SIM cards (IMSI numbers) in order to disguise as far as possible the identity of the caller. It has become more important to look at the pattern of phone calls using automated systems to infer links between users and give indications of where an as yet unknown means of communication might be in use. This can be further complicated by the use of call centres, gateway numbers, etc. Another technique of use in connecting a phone to a particular user is to look at the locations and times at which communications were made.

# 10. Inference development

## INTRODUCTION

Data description and integration techniques, like link analysis, are not an end in themselves. As already discussed, they are simply tools of the analyst; steps in the process of deriving meaning from the information being analysed.

The common requirement of the everyday work of the analyst is the need, by collecting and then breaking down information, to extract meaning and develop a theory, or theories, about what is or might be "going on". This is the essence of the analytical work.

What needs to be recognized is that any single set of information will inevitably have many alternative explanations, theories and hypotheses about its meaning. Some of these will be obvious and/or highly probable, whilst some may appear far-fetched and extremely unlikely. They still need to be identified and evaluated as options by the analyst.

A useful way of visualizing these hypotheses is as types of models. Models are useful in that they can be used as prototypes, which allow us to examine aspects of a much larger, more complex situation. Car manufacturers, for example, try out their ideas for new/better vehicles or features by creating models which they can then test more quickly, cheaply, and effectively than if they build the full vehicle. By creating hypotheses about criminal information, we are able to "test-drive" our ideas, our theories, in just the same way that a carmaker test-drives a new vehicle. This allows us to find out how our theories operate, how they perform, which ones might work and which won't, and where there is more than one, which performs best.

This in turn helps us provide our clients with quality, tested intelligence options, so that they can make informed choices and decisions in an objective manner, with less resource costs and a greater chance of success.

Here are some examples of "models" we regularly use:

- Prototype cars, aeroplanes, machines
- Mathematical models, equations
- Statistics/graphs
- Analysis charts
- Premises/hypotheses/inferences
- Offender profiles
- Suspect/intelligence packages
- Action plans/mission statements/operational orders/business plans
- Tactical/strategic visions/plans/reports
- Organizational/political policy

## Premises

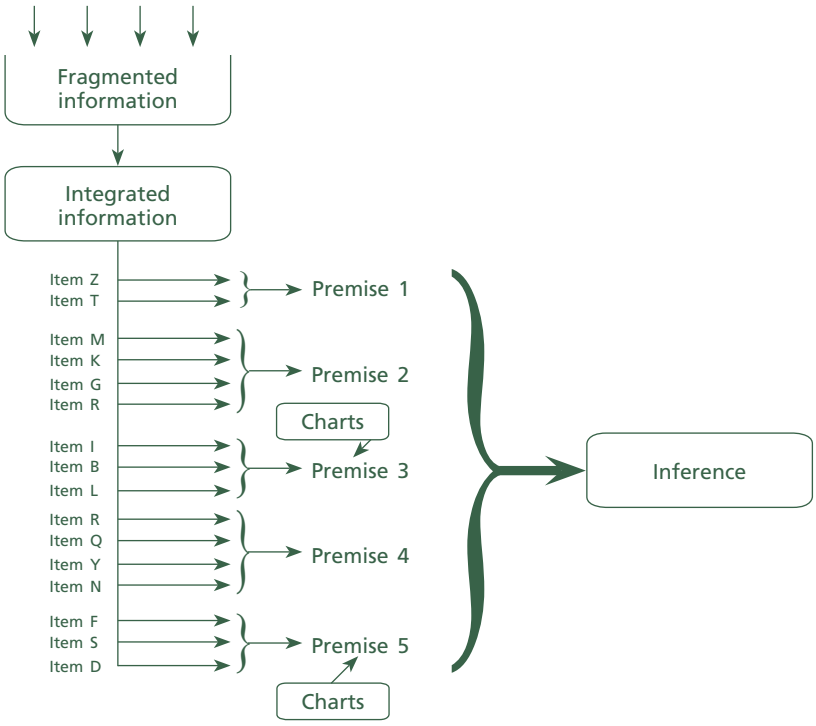
The dictionary definition of premise is: "A previous statement serving as a basis or an argument".

Similarly 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, as they are the first stage of extracting meaning from volume information, of identifying what the information might be telling us.

When information flows into an organization it is often fragmented and therefore needs to be channelled for analysis purposes into an integrated form from which a number of premises can be developed. As a result an inference or a number of inferences can be produced.

An item of data may support one or more premises. Often charts are also produced to give greater weight to a specific premise.

**Figure 10-1. Sample**




A premise might contain just one piece of information, or many. For example, a typical premise might be that thefts of motor vehicles might have risen in the Sandford area, where "in car" CD players are stolen. This might have come from just one crime report or hundreds; in either case, the premise, i.e. the identification of the problem, is the same. The only difference that the number (or quality) of pieces of information might make is to the value or significance placed on that premise. This is the role of probability assessment that will be covered later.

It is vital at this stage to understand two points. Firstly, that the premises are the closest link to the described information, and as such are the most objective and accurate representation of that data. Secondly, 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. This is a valid part of the process of arriving at a final inference, and evidences how the analysis has considered and evaluated a range of options, rather than just one.

A typical premise is illustrated below and constructed from four pieces of information:

1. Information: Smith has no job
2. Information: Smith owns a house valued at £400,000
3. Information: Smith owns three high value sports cars
4. Information: Smith enjoys a luxurious life style

*Premise:* Smith has unidentified income
Premises and inferences are developed within a logical framework. The elements of this framework are an argument and logic.

*Argument:* A list of statements or facts each of which reflects a key point of information or proposition. These statements are called premises, and when linked together, lead to the inference.

*Logic:* The way the premises and inferences are linked together to build the inference.

### Inference

In any criminal investigation the objective of analysis is to find an explanation of what the information means. This explanation is known as an inference. An inference is a statement, which succinctly describes what we think is going on. More formally, an inference is the product of logical thought.

The analyst's ultimate goal is to develop inferences about the nature and scope of the criminal activity being investigated, and about the specific individuals and organizations involved. However, it should be recognized that an inference can be of limited value without some estimate of its probable truth.

The way we react to an inference will differ depending on how confident we are as to its truth. For example, an inference in which we have a relatively low level of confidence might serve only to direct the collection of additional information. A high level of confidence, on the other hand, may lead to specific actions targeted against the principals of the criminal activity.

The very nature of criminal investigation is such that the information available in any criminal enquiry is almost always incomplete, and changes constantly as the enquiry progresses. It follows that inferences are made in the face of uncertainty, and so the best result the analyst can hope for is an inference which is as close as possible to the truth.

## TYPES OF INFERENCE

There are four types of inference:[1]

*Hypothesis:* A tentative explanation; a theory that requires additional information for confirmation or denial.

*Prediction:* An inference about something that will/may happen in the future.

[1] All types of inference require testing.

*Estimation:* An inference made about the whole from a sample, typically quantitative in nature, example: amount of money, time required, size of operation, and so on.

*Conclusion:* An explanation that is well supported; a hypothesis, prediction or estimation that either:
- Appears likely to be confirmed
- Appears a priority for confirmation
- Is a representative summary of the consequences arising from some or all of the constituent hypotheses, predictions and/or estimations.

The initial inference is most likely to be a hypothesis or estimation, which may lead to directed data collection.

If it is possible to arrive at a conclusion straight away, then the problem probably required little or no analysis in the first place. Further data collection or sampling going back round the intelligence process one or more times, allows you to refine the quality of your inference. However, at some point you must arrive at a final inference to disseminate, analysis without dissemination is pointless.

The final step in the inference development process is the use of probability values to assess the degree of certainty about the truth of the inference. This should be carried out by the analyst with particular care. The percentage value of probability cannot be just plucked out of the thin air in accordance with the analyst's "gut feeling".[2]

Probability is derived as a ratio between "number of times the event will occur" and "number of opportunities for the event to occur".

There are three sources of probability estimates:

- *Relative frequency of past events*—where over a given period the number of times an event has occurred in the past is used as a guide to the likelihood of future events occurring.
- *Theoretical estimation*—where some definite formula, however derived, is used as a basis for prediction.
- *Subjective estimation*—where the prediction relies solely upon the personal opinion or judgement, usually as a privilege of experience, expertise or position.

Types of probability values:

- *Simple*—the probability of occurrence of a single event
- *Joint*—the probability of two events occurring at the same time
- *Conditional*—the probability of a second event, given that a first event has occurred

This latter concept is used to assess inferences developed through the inductive logic process. Premises were the building blocks that led us to the inference. They are also, then, the building blocks on which the probability estimate should be based. An accurate assessment can be achieved by developing it systematically through sequential adding of premises. Addition of each new

[2] Extreme care should be taken in assigning probability, especially under evidential constraints.

premise logically increases the probability that the inference is correct. For example, with only one premise assumed true the inference may have a 10 per cent chance of being correct. With two premises assumed true, the probability may rise to 15-25 per cent, and so on.

Criminal investigations profit from hypotheses while these present ideas and insights that point into directions into which investigation could be expanded. Hypotheses represent working ideas for the investigative team and need to be the product of inductive logic. It is creative thinking that produces results that are of value to investigative teams, not merely the bookkeeping of results coming out of investigations.

In strategic intelligence, hypotheses and inferences concentrate upon issues related to intentions, possibilities, limitations and vulnerabilities of criminal adversaries to allow for planning and preparing effective long-term action. The main difference with hypotheses and inferences in operational analysis is that they deal with specific case-related issues that can be put to immediate operational use.

Hypotheses can be accepted, modified or rejected only through collection of additional information. The collection of information to test hypotheses is most effectively done when some prior thought has been given to the development of indicators. Indicators are clues that point to specific events corroborating or rejecting earlier assumptions.

The development and testing of hypotheses, in the context and with the benefit of all the research done during the analysis process, should finally result in the drafting of conclusions or recommendations. They are a vital element of an analytical product in so far as they communicate the essence of the work and the insights resulting from it to parties with operational or managerial responsibilities.

## FALLACIES RESULTING FROM INCORRECT LOGIC

In taking a logical approach to inference development, the analyst has to avoid logical errors or fallacies, which can result in false inferences. The most common fallacies fall into one of two general classes.

Fallacies of omission: some important premise, consideration or aspect of an argument is omitted:

- *Oversimplification*—an inference that fails to account adequately for all relevant conditions or possibilities.
- *Inadequate sampling*—a fallacy produced by drawing inferences (estimates) from too little information or from information that is not representative.
- *Mistaken cause*—an unwarranted cause and effect relationship established between events or conditions that happen to exist at the same time or to precede one another—correlation does not necessarily mean the presence of cause and effect.
- *False dilemma*—a fallacy in which only the extreme alternatives are considered.

False assumptions:

- *Begging the question*—instead of responding to the question or problem, the question is rephrased or the problem is substituted.
- *Hypothesis contrary to fact*—a fallacy that occurs when someone states decisively what would have happened had the circumstances been different, providing a hypothesis that can not be verified.

- *Misused analogies*—when reasoning from an analogy, one assumes that the object or event in the real world is similar to the object or event in an analogy. Analogies are inappropriate as evidence or proof in analytical work.

A further responsibility of an analyst is to assess the risks involved in the carrying out of a specific procedure or line of enquiry. Risk analysis is becoming increasingly significant, when there is a need to balance resource cost of an operational action against a crime problem, which this action is intended to address.

A good inference should typically include, "who" the key individuals are, "what" they are involved in, "where" they are operating, "why" they are doing it, "how" they are doing it, and if possible "when" they are likely to strike again.

An example of an Inference is shown below:

Stephen James is the head of a criminal operation involving the exchange of soft drugs and counterfeit currency for stolen property. Counterfeiting, drug importation, and obtaining goods by deception are the principal ways used by James and his associates to gain financially. They have been operating in the Sandford area for the past two years.

## Logic

For our purposes there are two types of logic, deductive and inductive.

*Deductive logic:* Deductive logic is based purely on facts. It never goes beyond the facts. Premises are based on the facts and the inference does not go beyond the premises. Thus, if the facts on which the premises are based are true, it follows that the inference must also be true. The argument proceeds from the general condition to specific circumstances.

Example of deductive logic:

Premise: Handling stolen goods is an offence punishable on conviction.
Premise: Sam Sharpe was convicted of handling stolen goods.
Inference: Sam Sharpe is subject to punishment for handling stolen goods.

*Inductive logic:* Inductive logic also examines the facts, but by contrast with deductive logic, it goes beyond those facts, the analyst using reasoning to work from the parts to the whole or from the specifics to the general.

Again, in contrast with deductive logic, because inductive logic goes beyond the facts, there is no absolute guarantee that the inference is true even if the premises are true. As criminal investigators we are interested in those cases in which, if the premises are true, the inference is probably true.

Example of inductive logic:

Premise: Mike Lee and Chris Wilson were cellmates in prison and now live together.

Premise: Mike Lee was recently arrested and convicted for supply of controlled drugs from their home.

Inference: Chris Wilson is involved in the supply of controlled drugs.

# 11. Presentation of results

## LOGICAL BRIEFINGS AND WRITTEN REPORTS

### Oral briefings

An oral briefing is most effective when used to present an overview of an analysis that will be the basis for immediate action—such as when results need to be disseminated in a critical fast-moving situation. Audiences are themselves influenced by style, effective presentation can greatly affect the receipt of an analytical product.

> Definition: A short oral presentation of the key elements of a situation or an analysis to a specific audience.

A principal advantage of an oral briefing is that it provides for face-to-face interaction between the users and producers of the analysis. Analysis products can be complex; an effective oral presentation provides the opportunity to deliver the conclusions in a clear logical sequence bit by bit. It is critical, therefore, that briefings reflect the logical reasoning that has gone into the analysis performed in order to produce them.

### Oral briefings have three main advantages:

- Time saving—a maximum amount of information can be communicated in the shortest time.
- Direct contact—an oral briefing provides direct contact between the analyst and the client. This creates an opportunity for dynamic questioning of the data sources, assessment of data reliability, inferences and their probability, etc. Both the client and the analyst can use this opportunity to ensure that the project is progressing in the right direction and is producing actionable results. By having direct contact, the user can more accurately assess the significance of the analysis results as they relate to other information on the topic.
- Dynamism—an oral briefing can be revised at the very last moment to include up-to-the-minute information. It can communicate developments in a project in almost real time. The briefing can, in effect, be a description of the situation up until immediately before the briefing.

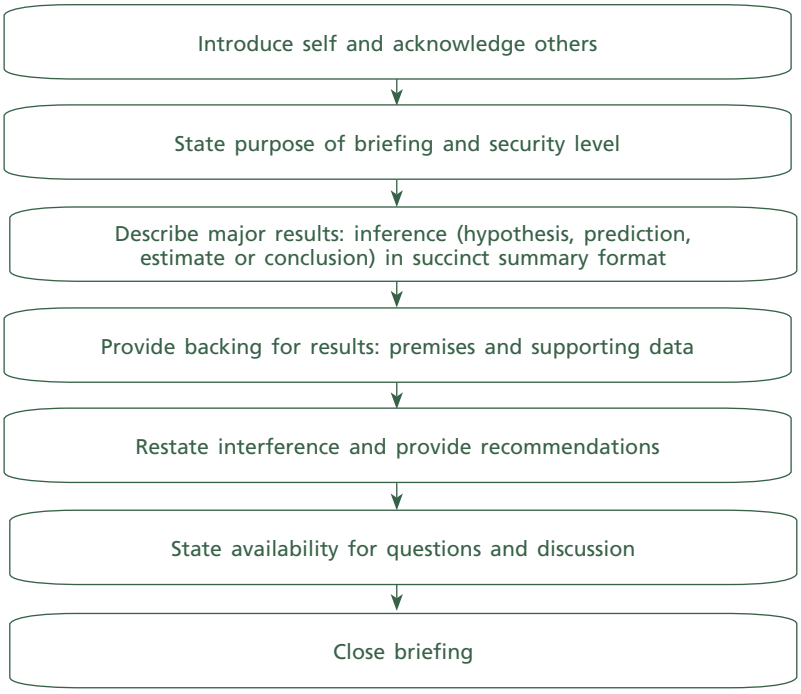
  Oral briefings do tend to include a good measure of improvisation and on-the-spot thinking. However, preparation is still required, as in order to produce the desired impact a briefing has to follow a pre-designed script.

To start with, it is always essential to analyse the audience—what will the information delivered during the briefing be used for? What is the level of audience's knowledge, and where do their interests primarily lie?

## Briefing structure

Careful preparation and logical presentation are essential to the effectiveness of an oral briefing. The logical reasoning that went into your analysis should be evident in the briefing. Figure 11-1 indicates a structural sequencing for the briefing that will provide a means of reflecting that logical reasoning.

**Figure 11-1. Sequence of a briefing presentation**




# CRITICAL STEPS IN PREPARING THE BRIEFING

## Analyse the audience

Know the needs of your audience. For example, will it be used for further dissemination, for making decisions, for developing a data collection plan, or for some other purpose?

Bear in mind the roles and responsibilities of the people in the audience and adjust your style and content to suit. (In other words, consider the difference of presenting to a group of officers conducting a fingertip search to a Senior Investigating Officer (SIO)) Determining the knowledge and background the audience already has of the situation to be covered in the briefing is essential to avoid presenting too much unnecessary data or not enough detail.

Consider the security issues, in particular your duties under legislation, in other words, do the audience need to know or are they allowed to know the information.

Ask yourself "is this the best method of delivery for the content, the audience, the environment and finally, you?".

## Outline your briefing

Your inference and the premises from which you developed the inference in the analytical process provide an excellent basis for your briefing outline. They ensure logical continuity between your analysis and your presentation.

Outline should contain four major sections:

- Introduction
- Statement of the inference
- Supportive premises and data
- Recommendations

*Introduction:* The introduction should be concise and state the purpose of the briefing. Identify yourself. Any sensitivity related to the information in the briefing should be stated at this point. Acknowledgements, as required, are also made at this point.

*Statement of the inference:* Your audience wants to know the results of your analysis at the outset. State your inference clearly, without details and particulars of the analysis at this point.

*Supportive premises and data:* Your premises provide the basis for this section of your briefing. To be most effective, you need to use appropriate charts—those which were developed during the analytical process and which were most beneficial in arriving at the premises.

*Restate the inference:* To remind your audience of the big picture and focus them before you make your recommendations.

*Recommendations:* Provide your audience with recommendations regarding additional data collection requirements and other options for actions where suitable. This would be done as far as you can give your own knowledge and experience. If you have a preferred option(s) state this with your reasons. Allow time for questions.

## "Dry-run" your briefing

Make a preliminary presentation to one or two people competent to point out weaknesses in the content, the logical sequence, suitability of briefing aids, your use of the aids, your approach and delivery, and your timing. If possible check your venue example: How does the TV and video work? Where are the plugs and light switches?

## Briefing aids

Briefing aids are just that; they will not stand on their own. They are valuable tools in ensuring a clear, concise, and logically presented briefing. Their purpose is to reinforce the spoken word. They commonly consist of visual presentations that support the spoken word, such as transparencies used with an overhead projector, flip charts or computer-based presentation software.

| Type | Suitable for | Points for attention |
|---|---|---|
| Flipchart | SHORT MESSAGES<br>Groups of up to 30 | Advance preparation needed<br>Use pencil-ruled lines, black or blue thick pens. |
| Flipcharts/ Whiteboards | DISCUSSIONS | Keep it simple. |
| Overhead | EXPLANATIONS | Laser-printed slides give best quality. |
| Projector (OHP) slides | Groups of up to 50<br>Most needs | Copies from printed work may need enlarging.<br>Colour slides do not show up well if there is a lot of daylight in the room. |
| Video | PERSUADING<br>Groups of up to 30 unless cinema-style equipment available. | Short clips only (8-10 minutes).<br>Pictures must be moving. Must be cued in accurately.<br>Beware: counter numbers work differently on different VCRs. |
| Computer-based presentation software | PRESENTATION<br>Groups of up to 100-150<br>Most things | By far the most professional if used with a remote control. Lighting must be dimmed during use. |
| Handouts | ADDITIONAL MATERIAL<br>Not included in Presentation<br>CONFIRMATION<br>CONSOLIDATION | Must be typed or printed and not too long. May amplify but must not conflict with the message you have given verbally and with other visual aids.<br>Physically check the spelling, the accuracy and the relevance of the content and that you have sufficient copies for your audience |

Note: With any type of visual aid, remember that for the duration of their display, they become the centre of attention. Use them if they will help. Don't let them be your presentation—a particular danger if you use computer driven slides.

Although the saying is "a picture paints a thousand words", visual aids are worth nothing if they are not relevant or detract from the presentation. Visual aids should complement your presentation, not be a substitute for it.

Homemade visual aids can be a minefield of distractions but make a great impact if they are good. The recognized ground rules when making them up are listed post.

## Overhead transparencies

- Remember the 6,7,8 rule: Write a maximum of 6 words per line, with 7 lines per transparency using letters at least 8mm high.
- Use a consistent format and layout, either centred or justified to the left.
- Use permanent pens for handwritten transparencies. A drop of water or perspiration can ruin hours of work with water-based ones.
- Use overlays to build up complicated diagrams.

- Don't put more than one idea onto a transparency.
- Don't present data as "raw figures"—use pie charts, line graphs, bar graphs to demonstrates relationships.
- Don't use pages from books or other documents.
- Don't draw or write to the edge, leave it at least 10mm margin.

## Flipcharts

- Print, using large letters, with different colours.
- Draw diagrams or layouts in fine pencil first—your audience won't see them.
- Keep the written word to 8 words per line, or 8 lines per page.
- Write bullet points only, not full sentences.

## Computer and digital projector

Available software, such as Microsoft PowerPoint, provides an efficient and effective way of both developing and presenting oral briefings. Applications such as PowerPoint provide a complete presentation package containing word processing, outlining, and drawing presentation tools. Presentations can be made from 35mm slides, overhead transparencies, or directly from a computer with an electronic projector.

## Examples of briefing aid use

The size of the print in the examples that follow should be considered as a minimum for hand printed transparencies.

When developing your inference, always use direct, positive terms. Avoid words like "may", "could be", "possibly", etc. The degree of certainty is reflected in the probability value.

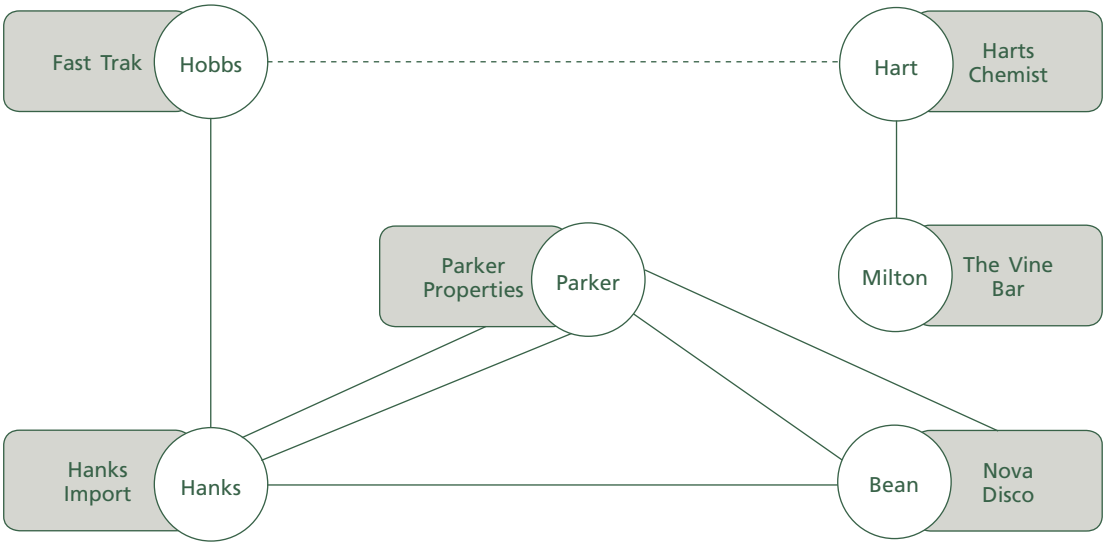
Example of a visual aid for the presentation of an inference

- For financial gain a major cocaine importation and distribution organization is operating in this area.
- Legitimate businesses and associates within them are being used to facilitate the operation.
- Paul Parker is the head of that organization
- There is a 70 per cent probability that this hypothesis is correct

Example of a visual aid for the presentation of premises

- There has been a marked increase in the amount of cocaine available in this area
- Several new companies have been established in the importation and distribution of goods from South America
- Paul Parker is linked to individuals within these businesses
- Paul Parker is linked to businesses specializing in this field
- Those members all have convictions relating to drugs

**Figure 11-2. Visual aid showing the linkages among Paul Parker and the commercial organizations involved**




Example of a visual aid for the presentation of recommendations

1. Liaise with Customs to establish whether or not they are looking at the operation already and with a view to mutual cooperation

2. Identify any other businesses to which Paul Parker may be linked

3. Establish whether or not the companies involved are also importing/distributing drugs for any other individuals

4. Identify key officers in the operation

## WRITTEN REPORTS

Written reports are likely to make up a large part of the dissemination of intelligence. A written report is a presentation of the key elements of a situation or analysis to a specific audience. The audience can range from patrolling officers who only need the smallest bulletin through senior officers requiring more in depth reports to colleagues who may need everything. It is most effective when used to present an overview of an analysis that may be the basis for a future action plan—such as when time is not a crucial factor affecting a potential operation.

It is important to remember that a written report creates little opportunity for direct feedback/questioning.

When it is read it must convey its own worth and make its own points. You do not get as much chance to re-explain as with an oral presentation. This means that written reports must be professionally presented as soon as they are picked up they start to affect the reader. A smart, colour, clear briefing sheet is more likely to be effective rather that a long scruffy textual sheet.

Reports should be proof read both for accuracy and clarity of points, if possible get someone else to do this for you. This will increase the credibility of the report and help to ensure the correct message is delivered.

Circumstances may dictate that a report has to be formulated quickly and under adverse conditions, however, the author should try wherever possible to be in possession of a good dictionary, thesaurus and writing materials.

Using a word processor will aid the efficiency of the report writer as documents can be created, saved and manipulated with relative ease.

There are several advantages and disadvantages to submitting a written report rather than giving an oral briefing.

| Advantages | Disadvantages |
|---|---|
| The report can be tailored to suit a particular recipient's needs, thereby omitting information that is irrelevant and/or unimportant to that person's requirements. | The report writer needs to know the audience in order to streamline the content of a report; otherwise they will have to include as much detail as is known to them at that time. |
| The contents of the report can be re-read at leisure and key points highlighted by the recipient for future use. | Once a report has been written it becomes a historical document, a snap shot of the situation pertaining to the information to hand at that moment in time. |
| The content of the report can be referred back to. Example: when exchanging ideas or further information. | Due to the distance between the writer and the reader, there is an unavoidable delay in exchanges between them. |
| Easy for further dissemination | Its distribution is less easy to control. |

The structure provided by inductive logic for the analysis and for the oral briefing can also serve you well in the preparation of a written report of the analysis. The charts produced by an analyst should ideally not be considered alone. They are produced to assist in understanding the criminal activity taking place and should therefore act as an illustration of the points to be made in a report and a briefing. Consider the following five main rules:

**Five main rules for writing intelligence reports**

- Be clear and concise. Inaccurate statements or errors in calculations will undermine the impact of the reports
- Write in the third person to make the record impersonal
- Avoid the use of professional jargon
- Maintain a logical flow of thoughts, ideas and arguments
- Ensure correct spelling and grammar. Spelling mistakes distract the reader, and in the case of names and identities can lead to confusion.

The report should contain the most important findings, conclusions and recommendations. Like an oral presentation the written report needs to convey the results of the analysis in plain simple language and identify the points which need to be emphasized. The content should be clear, concise, well typed and spaced avoiding lengthy blocks of print.

A very useful structure for writing intelligence reports is the inverted pyramid. To use it, imagine that each paragraph in the report is a pyramid standing upside down on its tip. The most

important idea should be at the widest part of the pyramid—in the topic sentence—and all other ideas in that paragraph support this lead idea. In fact, the sentences that follow the topic sentence should be placed in decreasing order of importance.

Similarly, the entire intelligence report can be approached as an inverted pyramid. The most important information should be at the beginning of the piece, not at the end. If this first section is compelling enough, the reader will continue reading. In preparing a written report, keep in mind that the reader wants to learn the "big idea" first—the big idea is your inference. Some writers withhold the big idea until the end of the report, like waiting to the end of a story to spring the "punch line". The reverse should be the case in an analytical report. Give the punch line first and follow with the story—the details that support the inference.

If you remember to apply this principle throughout the report—to the organization of the report, sections in the report, and paragraphs within each section—the report will also be easier to write as well as easier to read.

In accordance with this approach, the executive summary can be constructed by assembling in sequence the topic sentences of the first three-four paragraphs. While some re-writing may be required to avoid repetition and achieve dynamic reading, this way of structuring the summary paragraph is often effective.

The structure of each topic sentence is also important for keeping the reader's attention. It should have two components—"what?"—the fact, and "so what?"—the implications of this fact. This way the reader learns both what is happening and why it is important.

After finishing the draft, the following technique may be used to test the result. Does the title alone convey both the "what?" and "so what?" of the whole document? Then apply the same technique to the topic sentence of the executive summary. Finally, the opening sentence of each paragraph should also meet this requirement.

A side-benefit of the inverted pyramid model is that it helps to keep the intelligence report short. This technique forces the writer to concentrate on only those facts that are of direct relevance to the subject. It also helps to determine which facts are essential, and which "nice to know".

Finally, good writing often means good re-writing. Reportedly, Mark Twain once apologised to a friend for sending a long letter, because he did not have the time to write a short one.

## The three most common writing mistakes

- *The big build-up*—the author builds the case slowly, saving the conclusions for the end. The theory, presumably, is that this way, the conclusions will appear more dramatic. Unfortunately, most readers will stop reading before they get to the end.

- *The time line*—somewhat similar to the above mistake, this approach aims to tell a story in chronological order and therefore saves the most important—and relevant—elements until the end. Typically, however, the reader is most interested in recent events and loses patience.

- *The hard work*—this approach is also known as "look how much I know on the subject". Typically, intelligence analysts collect a huge amount of information, and often can't bear to leave any of it out. The result is a long and mostly unfocused product.

Content of a written report:

*1. Cover with title*

As well as the title, the cover page is likely to include the analyst's name, unit and date that the report was written. Choose a suitable heading which should immediately attract attention. Also if the document is restricted this should be indicated.

*2. Contents page*

This will be necessary in most cases particularly where the whole document has a large number of charts, appendices, etc.

*3. Foreword/methodology*

The foreword should be brief and contain details of the type of analysis carried out, the methods used, the purpose of the analysis, the team for whom the analysis has been done and if relevant, details of the periods covered by the analysis. In addition, this should include a key of any methods used to highlight portions of text and a key of any symbols used to represent entities and links in intelligence charts.

*4. The summary or overview*

An expansion of the inference statement becomes the report executive summary or overview. The summary should again be brief and include an overview of the results based upon the hypotheses and conclusions, the premises and recommendations.

*5. The main report*

The premises and the information from which they were derived become the major sections of the report. Once again this should be kept brief and should describe logically the structure of the analysis starting with the inference stating the outcome of all the premises used. The premises are then described and supported by the known relevant intelligence and small charts such as link charts and financial profiles which become figures in the major sections of the report. It is recommended that the attention of the reader is drawn to inferences and analysts comments (such as the highlighting of intelligence gaps) by methods such as boxing them using a different background colour to the text in each case. Photographs may also be included in this section although care should taken that too many pictures may hinder future e-mail dissemination of the report.

*6. The conclusions/recommendations*

The final section of the report can include a repeat of the inference/selected inferences as conclusions and provide a listing and rational for the recommendations which should be soundly based on the outcome of the analysis.

*7. The intelligence gaps*

In some intelligence reports it is extremely useful to list the intelligence gaps together in one section, grouped according to the agency/country which can act to fill the gap concerned. This enables the parties concerned to view what is their responsibility to act upon and for the users of the report to initiate and check progress regarding this process.

*8. Appendices and index*

This final section is for the inclusion of any larger or additional charts that show graphically the contents of the report.

If seeking some form of action or response, consider whether the request is viable and realistic. Unreasonable or impossible requests result in a loss of credibility with a damaging effect on future publications. An indication as to how questions should be asked or statements clarified should be included in the report. This may entail providing a contact point where the reader may reach the author.

Before any report is submitted, the author should read it to ensure that it makes sense, the spelling is correct (particularly of names and locations), the report is legible and the content is accurate example: dates of birth.

This in itself will add credibility and prevent problems further along the investigative process, particularly if the report is to be presented at court.

This model is intended as a guide to help the analyst construct a document that achieves the objective in other words, conveying the results of the analysis in the clearest, briefest and most logical way possible.

The structure and delivery of any presentation whether written or oral must be such so as to create maximum impact. This calls for imagination and originality on the part of its constructor. Analysts will develop these abilities with practice and experience.

# Annex I. Sample: criminal information and intelligence guidelines

## I. Criminal information and intelligence guidelines

These guidelines provide the (agency name) with accepted standards for its database on criminal activities. This database is created to fulfil the (agency's) mission to (agency's intelligence mission stated; such as "to collect, evaluate, collate, analyse and disseminate information on individuals and groups who are suspected of being involved in criminal activity and provide this information to the Chief Executive Officer for crime prevention and decision-making purposes").

These standards are designed to bring about an equitable balance between the civil rights and liberties of the citizens of the (jurisdiction) and the need of law enforcement to collect criminal information and disseminate criminal intelligence on the conduct of persons and groups who may be engaged in criminal activity.

## II. Criminal information and intelligence defined

For the purposes of the (agency name), the Criminal Information and Intelligence Database shall consist of stored information on the activities and associations of:

*A. Individuals who:*

1. are reasonably suspected of being or of having been involved in the actual or attempted planning, organizing, financing, or commission of criminal acts; or

*B. Organizations, businesses and groups that:*

1. are reasonably suspected of being or having been involved in the actual or attempted planning, organizing, financing, or commission of criminal acts; or
2. are reasonably suspected of being or of having been operated, controlled, financed, or infiltrated by known or suspected criminals.

## III. File content

Only information with a link to criminals and criminal acts which meets the (agency's) criteria for file input will be stored in the Criminal Information and Intelligence Database (CIID).

Specifically excluded material includes information on the political, religious, or social views, associations, or activities of any individual or any group, association, corporation, business, partnership, or other organization unless such information directly relates to criminal conduct involving the individual, group, corporation or association.

The CIID will also not contain any information which has been obtained in violation of any applicable federal, State, or local law or ordinance.

## IV. File criteria

All information retained in the Criminal Information and Intelligence Databank (CIID) shall meet file criteria prescribed by (agency name). Generally, information shall be retained in accord with generally accepted criminal intelligence file standards.

*A. General file criteria*

1. Information that relates to an individual, organization, business or group which is reasonably suspected of being or of having been involved in the actual or attempted planning, organizing, financing, or committing of one or more criminal acts will be included in the CIID:3

a. homicide
b. loansharking
c. gambling
d. narcotics distribution
e. extortion
f. arson
g. hijacking
h. receiving stolen property
i. conspiracy
j. money laundering
k. racketeering
l. theft by deception
m. fraud
n. counterfeiting
o. identity theft
p. bombing
q. terrorism

2. In addition to falling within the confines of one or more of the above criminal activities, the subject/entity to be given permanent status must be identifiable/distinguished by a name and unique identifying characteristic (e.g., date of birth, criminal identification number, social security number, alien registration number, driver's licence number, address). Identification at the time of file input is necessary to distinguish the subject/entity from existing file entries and those that may be entered at a later time.

Note: The exception to this rule involves modus operandi (MO) files. MO files describe a unique method of operation for a specific type of criminal scenario and may not be immediately linked to an identifiable suspect. MO files may be retained indefinitely while additional identifiers are sought. It should also be noted that due to the common use of multiple and false identifiers by those engaged in criminal and terrorist activities, the identifiers held for the individual may or may not be accurate.

[3] If the database is being designed to focus on a narrow type of criminal activity, then the criminal acts noted would reflect that focus. For example, if the focus of the database were counter-terrorism, then the crimes shown might be: arson; threats to public officials and private citizens; manufacture, use, or possession of explosive devices for purposes of intimidation or political motivation; destruction of public or private property; releasing harmful biological substances to the public; unauthorized detonation of nuclear weapons; inciting or encouraging others to participate in terrorist activities; soliciting or receiving funds to be used in support of terrorist activities; assaults on operators or assistance on public conveyances; theft of conveyances or materials to be used as terrorist weapons; any criminal acts perpetrated by individuals or groups related to terrorism.

*B. Temporary file criteria*

Information that does not meet the criteria for permanent storage but may be pertinent to an investigation involving one of the categories previously listed should be given temporary status. Temporary information shall not be retained for longer than one year unless a compelling reason arises to move the information to permanent status. (An example of a compelling reason is if several pieces of information indicate that a crime has been committed, but more than a year is needed to identify a suspect.) During this period, efforts should be made to identify the subject/entity or validate the information so that its final status may be determined. If the information is still classified as temporary at the end of the one-year period, the information should be purged. An individual, organization, business or group may be given temporary status in the following cases:

1. Subject/entity is unidentifiable—subject/entity (although suspected of being engaged in criminal activities) has no known physical descriptors, identification numbers, or distinguishing characteristics available.

2. Involvement is questionable—involvement in criminal activities is suspected by a subject/entity which has either:

   a. Possible criminal associations—individual organization, business or group (not currently reported to be criminally active) associates with a known criminals and appears to be jointly involved in illegal activities.

   b. Historic associations—individual, organization, business, or group (not currently reported to be criminally active) that has a history of association with persons later known to be involved in criminal activity and the circumstances currently being reported indicate they may become actively involved in criminal activity.

## V. Information evaluation

Information to be retained in the Criminal Information and Intelligence Database will be evaluated and designated for reliability and content validity prior to its filing. Data received in an intelligence unit may consist of unverified allegations or information. Evaluating the source of the information and its content indicates to future users the information's worth and usefulness. Circulating information that may not have been evaluated, where the source reliability is poor or the content validity is doubtful, is detrimental to the agency's operations and contrary to individual's rights to privacy. This evaluation should be systematically performed as outlined earlier in section 4 concerning Evaluation of source and data.

## VI. Information classification

Information retained in the Criminal Information and Intelligence Database is classified in order to protect sources, investigations and the individual's right to privacy. Classification also indicates the internal approval which is required prior to the release of the information to persons outside the agency.

The classification of information and intelligence is subject to continual change. The passage of time, the conclusion of investigations, and other factors may affect the security classification assigned to particular documents. Documents within the intelligence files should be reviewed on an ongoing basis to ascertain whether a higher or lesser degree of document security is required to ensure that information is released only when and if appropriate.

*A. Sensitive classification level:*

1. Information pertaining to significant criminal activity currently under investigation
2. Informant identification information
3. Intelligence reports which require strict dissemination and release criteria

*B. Confidential*

1. Criminal intelligence reports not designated as sensitive

2. Information obtained through intelligence section channels that is not classified as sensitive and is for law enforcement use only.

*C. Restricted*

1. Reports that, at an earlier date, were classified sensitive or confidential and the need for high-level security no longer exists

2. Non-confidential information prepared for/by law enforcement agencies.

*D. Unclassified*

1. Civic-related information to which, in its original form, the general public has access (i.e. public records)

2. Media information (i.e. public reports, newspapers and magazines)

## VII. Information source documentation

In all cases, source identification should be available and should be noted along with the data itself. The true identity of the source should be used unless there is a need to protect the source. In those cases when identifying the source by name is not practical for security reasons, a code number may be used. A confidential listing of coded sources of information should be retained by the intelligence unit supervisor perhaps as part of a confidential sources register or database.

## VIII. Information quality control

Information to be stored in the Criminal Information and Intelligence Database shall undergo a thorough review for compliance with file guidelines and agency policy prior to being filed. The intelligence unit supervisor is responsible for seeing that all information entered into the CIID conforms to the agency's file criteria and has been properly evaluated and classified.

## IX. Information and intelligence dissemination

*A. Open public records exemption*

All documents, materials and information pertaining to criminal intelligence created, compiled, obtained or maintained by the (agency name) shall be deemed to be confidential, non-public and not subject to the Freedom of Information Act (FOIA) or other public information regulations or laws.

*B. Criteria*

Information from the CIID can only be released to an individual who has demonstrated both a need to know and a right to know. "Right to know" is defined as the requestor having an official capacity and statutory authority to receive the information being sought. "Need to know" is defined as the information requested is pertinent and necessary to the requestor in initiating, furthering, or completing an investigation.

*C. Third party data restrictions*

No "original document" which has been obtained from an outside agency may be released to a third agency without the permission of the originating agency.

*D. Information dissemination by classification of data*

Information in the following classifications may be disseminated with the approval of the following personnel:

| Security Level | Dissemination criteria | Release Authority |
|---|---|---|
| Sensitive | Restricted to law enforcement personnel having a specific need to know and right to know | (Management Name) |
| Confidential | Same as for sensitive | Intelligence Section Supervisor |
| Restricted | Same as for sensitive | Intelligence Section Supervisor |
| Unclassified | Not restricted | Intelligence Section Supervisor |

*E. Dissemination to avoid imminent danger*

Nothing in these dissemination restrictions shall limit the dissemination of an intelligence assessment to a government official or to any other individual, when necessary, to avoid imminent danger to life or property.

*F. Dissemination control*

To eliminate unauthorized use and abuse of the system, the (agency name) shall use a dissemination control form that is maintained with each stored document. This audit control shall record the:

1. Date of the request;
2. Name of the agency;
3. Individual requesting the information;
4. Need-to-know;
5. Information provided;
6. Name of the employee handling the request.

## X. File review and purge

Information in the CIID will be reviewed periodically for reclassification or purge in order to ensure that the file is current, accurate, and relevant to the needs and mission of (agency name); safeguard the individual's right to privacy as guaranteed under federal and state laws; and ensure that the security classification level remains appropriate.

*A. Purge criteria*

Information will be reviewed and/or purged using the following considerations:

1. Utility—has it been used in the past two years?
2. Timeliness and appropriateness—is the investigation still ongoing?
3. Accuracy and completeness—is the information still valid?

*B. Review and purge time schedule*

1. Permanent data—permanent data shall be reviewed and/or purged every five years
2. Temporary data—temporary data shall be reviewed and/or purged every year.

*C. Manner of destruction*

1. Material purged from the CIID shall be destroyed. Disposal is used for all records or papers that identify a person by name.

## XI. File security

*A. Physical security*

The CIID shall be located in a secured area with file access restricted to authorized personnel.

*B. Programmatic security*

The CIID must store information in the system in such a manner that it cannot be modified, destroyed, accessed, or purged without authorization. Sanctions will be adopted for unauthorized access, utilization, or disclosure of information contained in the system. The best means to achieve this will likely be through the establishment of an audit trail and periodic audit and inspection examinations.

**Authorization**

These Guidelines shall take effect immediately.

_____

Agency Head

Agency Name Date:

# Annex II. Making recommendations

Having gone through the intelligence process at least once and probably a number of times to arrive at the final inference the analyst will have an in depth knowledge of the investigation or project. A knowledge level, which may not even be matched by the customers of the analysis (investigators/managers). The final outcome of any analysis should be to point the way forward.

To address the "What do we do now", or even the "What don't we do" question. It is not the role of the analyst to make resourcing decisions but to inform them. Making recommendations is a legitimate part of the process, but the extent and details of the recommendations may vary according to whom the analysis is for, and the type of inference provided. Recommendations will broadly be divided into the following areas:

*Further information gathering/directed data collection (filling intelligence gaps)*—Specific information required to test inferences. These recommendations provide the focus for a return to the first stage of the intelligence process ensuring that resources are not wasted collecting non-relevant information. Analysts may wish to consider how such information might be obtained and suggest possible alternatives; however caution is required to avoid obvious statements, which may undermine the value of analysis.

*Target selection*—As a result of analysis of a criminal network the analyst may recommend individuals for target status whose incapacitation would do most to disrupt the network as a whole. This is particularly appropriate when preparing market or criminal business profiles.

*Preventative measures*—In a law enforcement environment it is all too easy to fixate on arresting and prosecuting offenders. There are however, other methods and ways, which can be harnessed to prevent the crime from occurring in the first place. This is an area where the analysts' objectivity and lateral thought may arrive at new solutions to old problems. Such recommendations may be appropriate in crime pattern analysis, problem profiles and strategic reports.

*Predictions/risks*—By their very nature these are types of recommendations, which may be controversial. The ability to state clearly the supporting factors on which you base such recommendations is vital; as such recommendations could potentially be the subject for disclosure and therefore open to legal scrutiny. Risk analysis is an emerging issue brought into sharp focus by the advent of human rights legislation.

*Policy/process*—Strategic analysis projects in particular may highlight weaknesses in existing policies, process or resource levels which can be the subject of recommendations. Ideally any such critiques should include an alternative solution, which addresses the problem.

This is by no means an exhaustive list and these and other types of recommendations can be included in the full range of analytical products as appropriate. Some analysis may only require one type of recommendation, others several. Analysts will naturally be guided in this area by the direction given in the initial tasking. If you feel there are more important recommendations to be made, which do not form part of the original brief these might be presented verbally or as a separate appendix to the main report. In either case it is advisable to discuss them with the customer prior to any broader publication.

The analyst's ability to make recommendations will develop with their experience in a particular organization. Part of that experience should include building knowledge of the organization's capability to gather information, such as, computer access, surveillance, links to other agencies, financial investigations, etc. Such knowledge will ensure that recommendations are both practical and feasible, thus making them more likely to be accepted and adopted.

Recommendations are where the analyst translates the knowledge gained during the analysis phase into ideas and solutions, which can progress an enquiry or project. They are the fundamental and final part of the intelligence process prior to dissemination. The intelligence disseminated is the product by which the analysis will be judged. Therefore, every care should be taken in the preparation and the delivery of recommendations.

# Annex III. Criminal intelligence database

## I. Criminal Intelligence Database description

*A. Purpose*

The (agency name) Criminal Intelligence Database (CID) was created to meet the mandate of (cite laws or policies that cause you to have an intelligence database).

This database provides the (agency) with the ability to determine linkages among criminal individuals and activities in (jurisdiction) and outside of (jurisdiction) if the activity or individual has linkages to (jurisdiction). It also provides the (agency) with the necessary data to coordinate law enforcement efforts across the (jurisdiction). The central collection of information allows the immediate analysis of this data, providing alerts and cautions to State, local and federal law enforcement. It further allows (jurisdiction) to participate in information-sharing networks.

The (agency name) systems policies are based on 28 C.F.R. 23,* which provides standards for multijurisdictional information sharing within law enforcement.

*B. Definitions*

1. "User" is a law enforcement agency participating in the CID system.
2. "Access officer" is an individual who has met the criteria for being an access officer in the CID system.
3. "Agency" is the (agency name).

## II. Access to the Criminal Intelligence Database

*A. Criteria for Access*

Law enforcement agencies designated by the (agency) will be able to access the CID.

Their access will be contingent on:

1. The signing of a Memorandum of Understanding between the User and the (agency).
2. Successful completion of training in intelligence and the system guidelines by at least one user staff member.
3. The assignment of at least one person as intelligence coordinator for the user.
4. Ongoing compliance with the approved Information and Intelligence Guidelines and these procedures.

## III. Protocols for access

*A. User access process*

1. Potential users qualified for access will be notified by the (agency).

*See http://28cfr23.org

2. These potential users will be sent a packet including:
   a. A memorandum of understanding,
   b. A copy of the Information and Intelligence Guidelines, and
   c. A copy of the Criminal Intelligence Database protocols

3. Potential users wishing to be granted access will return the Memorandum of Understanding along with a memo stating who their primary contact person will be.

*B. Access termination provisions*

1. Criteria for user termination
   a. Any breach of security in the CID system caused by an employee of the user, or
   b. Any breach of security in the CID system caused by inadequate security of the user, or
   c. Any violation by the user of federal, state, or local laws or regulations governing the conduct of criminal investigations or the handling of criminal information.

2. Process of termination
   a. The (agency head), or a designee, is informed of infraction by CID system supervisor
   b. If necessary, the (agency head), or a designee, may order the system supervisor to temporarily suspend any access to the system pending the determination of more final action. This is done when continued access could harm the integrity of the system.
   c. System supervisor causes all pertinent information on the infraction to be gathered.
   d. (Agency head), or a designee, reviews information and invites User alleged to have committed the infraction to a meeting to present the user's response to the charges.
   e. Once the user's side is heard, the (agency head), or a designee, determines if access should be permanently terminated.
   f. The user must return all manuals, logs, updates, and data received through or for the CID system to the system supervisor.

*C. Access officers*

3. Criteria for access officers
   a. Only those individuals employed by law enforcement agencies are qualified for appointment as access officers.
   b. Only those individuals with a need to know the information and a right to know the data in the performance of their law enforcement duties may have access.
   c. Only those individuals who have completed the required CID training may have access.

4. Training for access
   a. Upon notifying the user of its acceptance into the system, the User will identify access officer(s).
   b. The access officers will be contacted by the CID system supervisor to schedule their training.
   c. The access officers then participate in CID training.
   d. The system supervisor gives a password, user manuals and other necessary material to each access officer at the training.

5. Access termination provisions
   a. Incidents requiring personal termination of access
      i. Termination of an access officer's employment with agency
      ii. Transfer of an access officer to another function within the user agency
      iii. Personal breach of security of the system
      iv. Violation of user agreement

   b. Process for termination
      i. Voluntary

- User agency notifies CID system supervisor of the transfer or termination of the access officer.
- CID supervisor deletes the password which allowed that officer to have access
- Officer returns all CID related material to (agency name).

ii. Involuntary

- A personal breach of security is uncovered by the user or CID which involves an access officer.
- The access officer's access is immediately terminated by the system supervisor.
- Charges may be brought against the officer.
- An investigation into termination procedures for the user agency may ensue.
- The access officer returns all CID materials to (agency name).

*D. Access by (agency name) staff*

1. CID analysts—will access all programmes, equipment and data necessary to fulfil their duties as system employees. This access is for the purpose of assisting inquirers, and analysing trends, patterns and commonalities for specifically assigned analytical products or projects.

2. (Agency name) investigators—may become access officers in a manner similar to the employees of user agencies. As such, they will have entry and inquiry access to the main index and inquiry files.

3. All (agency name) staff members are required to keep information received from the system in strictest confidence and are not to use their access to obtain data for persons who would otherwise not have access to that data.

4. Any breach in the security of the system caused by an employee may be cause for immediate dismissal.

*E. Access restrictions*

1. Entries and inquiries—access officers may make entries to and inquiries of the database.

2. Sensitivity levels:
   a. Sensitive information. This information is the most sensitive data in the CID and will not be disseminated except under very restricted circumstances.
   b. Confidential information. This data is less restricted than sensitive data. It will not be provided to inquirers, nor will they be told that a user submitted the data. The submitting user will, instead, be contacted and told who has inquired on the subject. The submitting user may then, at its discretion, contact the inquiring user and share the data.
   c. Restricted sensitivity information will be given to inquirers along with submitting user's name for follow-up if additional information is needed.
   d. Unclassified information which has been taken from public records or the media will be disseminated to inquirers without restriction.

*F. Access notifications and verifications*

1. The CID system supervisor will cause monthly logs of entries and inquiries to be generated.

2. All inquiries upon a subject in a file will result in the original submitting User to be notified of the inquiry.

3. Multiple entries on a single subject of a non-restricted classification will cause all entering users to be notified of the other entries.

4. Multiple entries on a single subject which include a restricted classification entry will only cause notification to appropriate users of general (not restricted) entries.

5. The CID system supervisor will cause a computerised log to be kept showing all incidences of matches between inquiries and entries. This log, when compared to the log of all records inquired upon, will show the "hit rate" of the system.

## IV. Physical security

*A. At the (agency name)*

1. Location of CID—The CID computer will be located in a secure environment within the Intelligence Centre at the (agency name). This is part of a secure, patrolled building.

2. The Intelligence Centre is a secure section within the building to which access is limited to authorized CID staff and others with a demonstrable need to be on site.

*B. At user locations*

1. Access to CID files is restricted only to access officers.

2. Users must have the terminal which accesses CID in a secure location which is not in a public area.

## V. Main index

*A. Entry criteria*

1. An entry on a subject may be made only if the subject is reasonably suspected of being involved in terrorist or criminal activity within the past three (3) years.

   a. Terrorist activity is defined as the financing, support, participation, transportation, or furtherance of any activity deemed by federal or state law to be an act of terrorism. Such acts may include:

      i. Threats to public officials and private citizens
      ii. Arson
      iii. Manufacture, use, or possession of explosive devices for purposes of intimidation or political motivation
      iv. Destruction of public or private property
      v. Releasing harmful biological substances
      vi. Unauthorized detonation of nuclear weapons
      vii. Inciting or encouraging others to participate in terrorist activities
      viii. Soliciting or receiving funds to be used in support of terrorist activities
      ix. Assaults on operators or assistants on public conveyances
      x. Theft of conveyances or materials to be used as terrorist weapons
      xi. Any criminal acts perpetrated by individuals or groups related to terrorism

   b. Criminal activity is defined as any act which is enumerated in federal or State law as being criminal.

   c. Reasonable suspicion is present when information exists which establishes sufficient facts to give a trained law enforcement or criminal investigative agency officer, investigator, or analyst a basis to believe that there is a reasonable possibility that an individual or organization is involved in a definable terrorist or criminal activity or enterprise.

2. Entries are made on individuals, organizations, businesses or groups who are reasonably suspected of having been involved in the actual or attempted planning, organizing, financing, or commission of terrorist acts or are suspected of being or having been involved in criminal activities relating to terrorist acts.

3. No information shall be entered about the political, religious, or social views, associations, or activities of any individual or any group, association, corporation, business, partnership, or other organization unless such information directly relates to terrorist or criminal conduct or activity and there is reasonable suspicion that the subject of the information is or may be involved in terrorist or criminal conduct.

4. No information will be included which has been obtained in violation of any applicable federal, State, or local law or ordinance.

*B. Permanent status criteria*

1. A subject/entity to be given permanent status must be identifiable—distinguished by a name and unique identifying characteristic (e.g., date of birth, criminal identification number, social security number, alien registration number, driver's licence number, address).

2. Modus operandi files which describe a unique method of operation for a specific type of criminal scenario may be included in permanent status regardless of the lack of immediate link to an identifiable suspect.

3. All entries to the index must be reviewed for compliance with policies and criteria prior to being entered into the CID; this review will be completed by an (agency name) analyst or investigator.

4. All entries will be held in an interim file until such a review is completed; at which time they will be entered into the CID.

*C. Inquiries*

1. An inquiry may be made only if the subject is reasonably suspected of being involved in terrorist or criminal activity.

2. An inquiry on a subject may only be made if the inquirer is involved in an investigation, prosecution or analysis involving the subject. A case or project number should be provided to substantiate this claim.

*D. Temporary status criteria*

1. A subject/entity upon which an inquiry has been made may be given temporary file status.

2. When a subject/entity is unidentifiable in the immediate future, having no known physical descriptors, identification numbers, or distinguishing characteristics available it may be given temporary file status.

3. When the link to terrorist or criminal activities is questionable the subject/entity may be given temporary file status. This may occur through:

a. Possible terrorist associations—individual, organization, business or group (not currently reported to be active) associates with a known terrorist and appears to be jointly involved in illegal activities.

b. Historic associations—individual, organization, business, or group (not currently reported to be active) that has a history of association with persons later known to be involved in terrorist activity and the circumstances currently being reported indicates they may become actively involved in terrorism.

## VI. Dissemination

A. The (agency name) shall disseminate intelligence information only to law enforcement authorities which agree to accepted procedures regarding information receipt, maintenance, security, and dissemination.

B. Dissemination shall only occur, where there is a need to know and a right to know the information in the performance of a law enforcement activity.

C. Notwithstanding paragraph A of this part, the (agency name) may disseminate an assessment of intelligence information to a government official or to any other individual, when necessary, to avoid imminent danger to life or property.

## VII. Update or purge of materials

A. Any information that has been retained in the system but has not been reviewed for a period of time (shown below) must be reviewed and validated before it can be used or disseminated.

B. Entries

1 All entries will be reviewed on specific schedules to allow for update and possible purging of data

due to obsolescence or inaccurateness. The following schedules will be used:

a. Subjects entered which are currently under investigation will be updated or purged every two years.
b. Subjects entered which are recently named for participation in terrorist or criminal activity will be updated or purged every five years.
c. Entries scheduled for update or purge will be flagged by the CID databank. The submitting User will then be required to review the entry, update it or purge it from the files.

C. Inquiries

1. All inquiries will be automatically reviewed by the (agency name) staff 180 days after their submission.
   a. If no further inquiries or other information has surfaced on the subject; the system will automatically purge the inquiry and notify the inquirer of the action.
   b. If further inquiries have come in on the subject, the information will be retained for 180 days beyond the last inquiry.
   c. If the inquiry is on a subject in the CID database, the inquiry remains in the files until that subject is purged.

## VIII. Sanctions

Particular sanctions are available in law and regulations covering the operations of a law enforcement information system.

A. (Applicable laws governing files).

## IX. Monitoring and auditing

A. To ensure system participation and integrity, the (agency name) will monitor and/or audit all Users' participation in the system.

B. Automatic monitoring

1. The CID has an automatic audit trail built into each access of the database.
2. Each action of an access officer will be recorded in a log including what data was accessed, who accessed it and the date and time of access.

C. User location site visits

1. At least once bi-annually, each remote site will be visited to assure that there is adequate security for CID access and information received through the system.
2. Such visits will be completed by (agency name) staff members.

## X. Disaster preparedness

A. The system supervisor shall ensure the establishment of a documented disaster plan containing, at a minimum, the following elements:

1. Designation of an alternate computer site with sufficient capacity to process the CID workload to be used in the event of system failure.
2. Weekly backup of database content with off-site storage of backup.
3. Procedures to be followed to initiate and maintain operations at the alternate site when needed.

B. Disaster response testing

1. The system supervisor shall ensure that testing of all disaster response elements will be undertaken annually to ensure the viability of disaster recovery.

2. A report of this test will be provided to the (agency head), or a designee.

3. Notification—The (agency head), or a designee, will be immediately notified of any actual computer disaster.

## XI. Changes to protocols

A. All protocols in this manual are agreed to and established by the (agency head).

B. Any modification of these protocols must be approved by the (agency head), or a designee. Any routines established based on these protocols may be modified under the responsibility of the CID system supervisor.

# References


1. Criminal Intelligence Analysis (West Yorkshire Police, 1998).
2. 2003 Anacapa Sciences, Inc.
3. B. Fiora, "Writing Intelligence Reports that Get Read" (*Competitive Intelligence Magazine*, vol.5 No. 1 January-February 2002).
4. D. McDowell "Strategic Intelligence" (Istana Enterprises, 1998).
5. Europol Analytical Unit, The Hague 10-21 May 1999.
6. Europol Guidelines on Intelligence.
7. IACP Criminal Intelligence Sharing Summit Participant Materials, section 3.
8. IACP, Criminal Intelligence Sharing: A National Plan for Intelligence-Led Policing at the Local, State and Federal Levels. August, 2002.
9. ICPO-Interpol Guidelines on Criminal Intelligence Analysis (Vers. 3, 2000).
10. Intelligence 2000: Revising the Basic Elements, LEIU and IALEIA, 2000.
11. M. Peterson "Applications in Criminal Intelligence Analysis" (Praeger, 1994).
12. M. Peterson "Joining the Debate: Product vs. Process (*IALEIA Journal*, vol. 11, No. 1).
13. National Criminal Intelligence Service, National Intelligence Model.
14. P. Andrews "Principles of Network Analysis" (Issues of Interest to Law Enforcement: Intelligence—the Ultimate Managerial Tool, Law Enforcement Intelligence Unit, 1982).
15. R. Davis "Social Network Analysis: an Aid to Conspiracy Investigations" (FBI Law Enforcement Bulletin, December 1981).
16. R. Morehouse "The Role of Criminal Intelligence in Law Enforcement" ("Intelligence 2000: Revising the basic Elements, L.E.I.U.—IALEIA, 2000).
17. UNDCP Intelligence Policy and Training Manual (2000).
18. Wantanabe, Frank (undated) "Fifteen Axioms for Intelligence Analysts" (www.cia.gov/csi/studies/97unclass/axioms.html).
19. West Yorkshire Police June 2002 and Anacapa Life Sciences Inc. 1993.
20. White House Task Force, 2000.

# 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

United Nations publication
Printed in Austria

V.10-58435—April 2011—100