UNITED NATIONS OFFICE ON DRUGS AND CRIME

Criminal Intelligence Training

MANUAL FOR MANAGERS

Regional Programme Office
South Eastern Europe

TOWARDS
SECURITY AND JUSTICE
FOR ALL

TABLE OF CONTENTS:

Chapter I

1. AN INTRODUCTION TO INTELLIGENCE

FROM INFORMATION TO INTELLIGENCE

Before we can properly discuss and explore intelligence and analysis in theoretical and practical terms, we need to have some common understanding as to what those 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 principals 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 utilising 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 :-

1) What exactly is the problem; what decision do we have to make and why is it significant or important?

2) 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?

3) What meaning can we extract from the information; what does it tell us about what's going on?

4) Is there only one possible explanation, or are there other alternatives or options. Are some more likely than others?

5) 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?

6) 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 summarised 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 utilising information to support decision making in some formal, structured way is nothing new. In order to obtain advantage over an adversary, 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, organisational 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 can need 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 recognised text on the subject of information gathering and intelligence-based actions is 'The Art of War, The Art of Strategy'. This was written in the 5th Century BC by Sun Tzu, a Chinese mercenary warlord who 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. In addition, many early examples are documented in the Bible, such as when the Lord told Moses to send leaders of the twelve tribes to explore the land of Canaan to gather information to estimate the strength and capability of the enemy. 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.

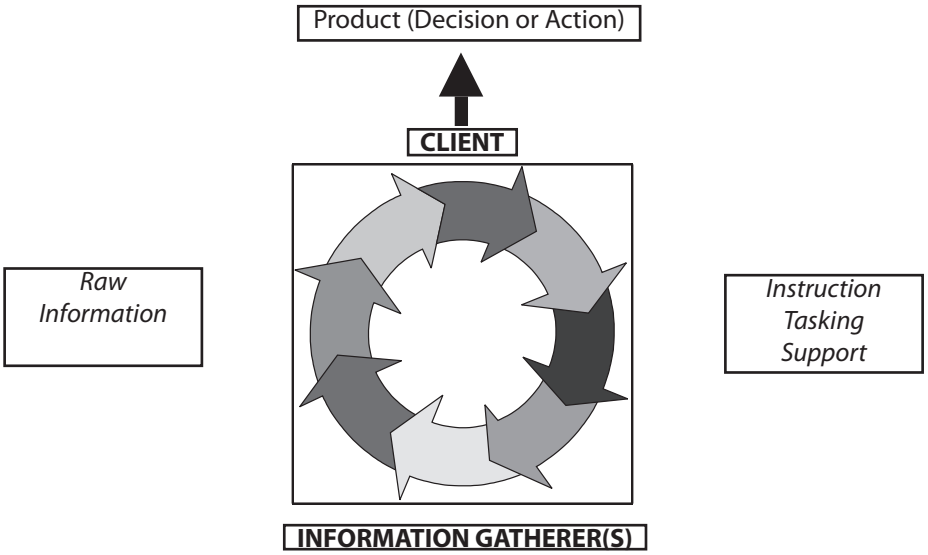

Figure 1-1

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 client/investigator has to deal with. The problem for the client / investigator is that no matter how good the system used to store all this information is, 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 client / 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 the 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] :-

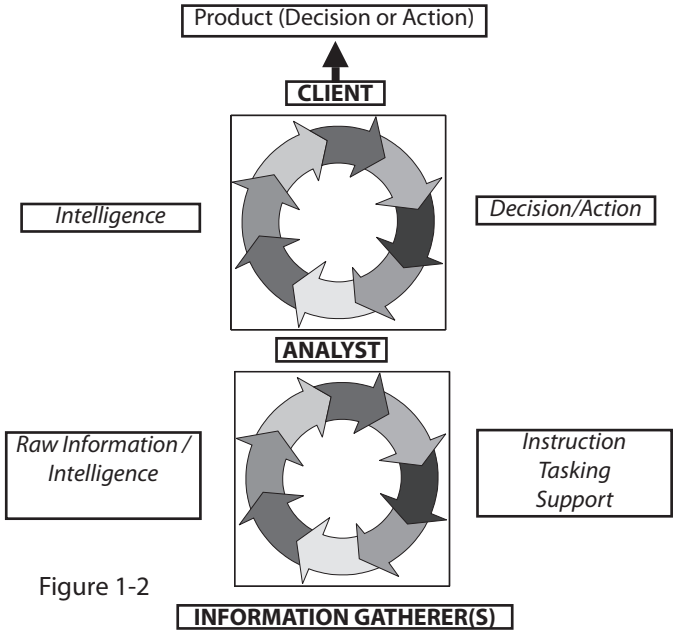

Figure 1-2

[1] The analyst may be supplied 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:

1) To gather information, to understand it and the relevance or relationship of each piece to all of the others.

2) To develop this information objectively to arrive at an understanding of the whole.

3) 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, organisations 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 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 intelligence and information that we have collected concerning them. It provides techniques which structure our natural deductive powers and thought processes, the `natural intuition`, which proficient investigators use subconsciously all the time. It also provides tools, which 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 detective. **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 organised 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 ORGANISED CRIME

The advent of criminal intelligence analysis is directly linked to the transformation of individual crime into organised or group crime. The effective use of intelligence is crucial to a law enforcement's agency 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, 'organised crime' was synonymous with the Cosa Nostra. The picture of organised crime today is quite different. Many of the new criminal groups, with well-developed organisational structures, are established for obtaining power and wealth. These groups include outlaw motorcycle gangs, Russian organised crime, Asian organised crime, African organised 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 organised crime groups and networks is also common place.

Criminal groups continue to be involved in ventures such as gambling, 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 promises to be a challenging new arena for law enforcement.

Criminal organisations 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 will need forward looking, assertive, and comprehensive strategies to counteract the threat of organised crime groups. Criminal intelligence analysis, when tasked and used effectively, can be a major asset in the law enforcement arsenal. Countries with greater experience with criminal intelligence, such as the United Kingdom, have developed national intelligence models in their countries. (Discussed in further detail in section 3 of this manual)

Information technology is very much key to intelligence sharing. Particularly in this age of sophisticated multi-national crime, including terrorism, not sharing intelligence and information in itself could be construed to be a crime.

Chapter II

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 the investigative team with hypothesis and inferences concerning specific elements of illegal operations of any sort. These will include hypothesises and inferences about specific criminal networks, individuals or groups involved in unlawful activities, discussing their methods used, and their capabilities, vulnerabilities, limitations and intentions that could be utilised for effective law enforcement actions.

It is important to note that a good knowledge of operational intelligence is a highly recommended prerequisite to developing a 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 emphasise that National legislations vary in the way intelligence can be used for law enforcement purposes. For this reason intelligence should principally be regarded as an instrumental (primary step) towards evidence gathering. Any request to use this material in court must be in agreement with the provider of the data, and treated on a case by case basis. Once the intelligence process has been well established a greater emphasis can be placed on the role of evidence collection within the criminal investigation with the aim of securing a successful prosecution. Much of this will be based upon collection responding to the hypotheses and inferences originating from the analyst during the intelligence process.

Evidence: data on which to base proof

This part of the investigation responds to reported events and explains what did happen and who was involved. Intelligence analysis is instrumental in 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 unwanted transgression into areas of no relevance. To obtain maximum results the 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 PROCESS

The intelligence process is based around the collection, evaluation, collation, analysis and dissemination of intelligence with emphasis placed upon analysis. All these activities need a substantial degree of advance planning. There is now a much more disciplined approach to the way information and intelligence is handled. Whereas in the past the methods tended to be ad-hoc, now law enforcement agencies have moved towards the collection plan principle of prioritised collection.

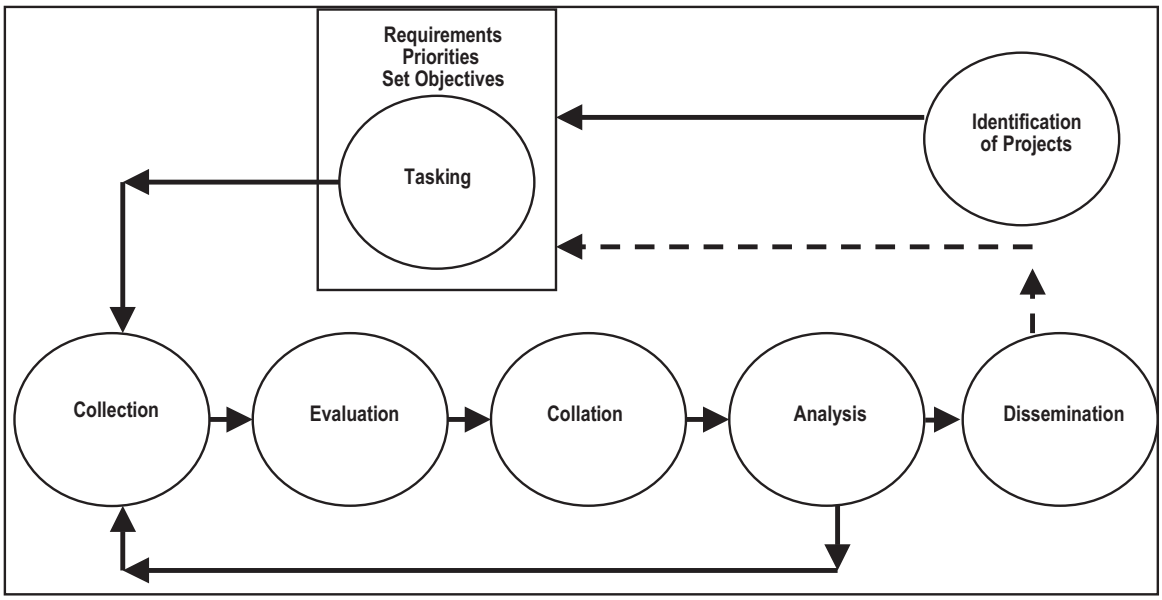

Figure 2-1: The Intelligence Process

THE INTELLIGENCE CYCLE

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

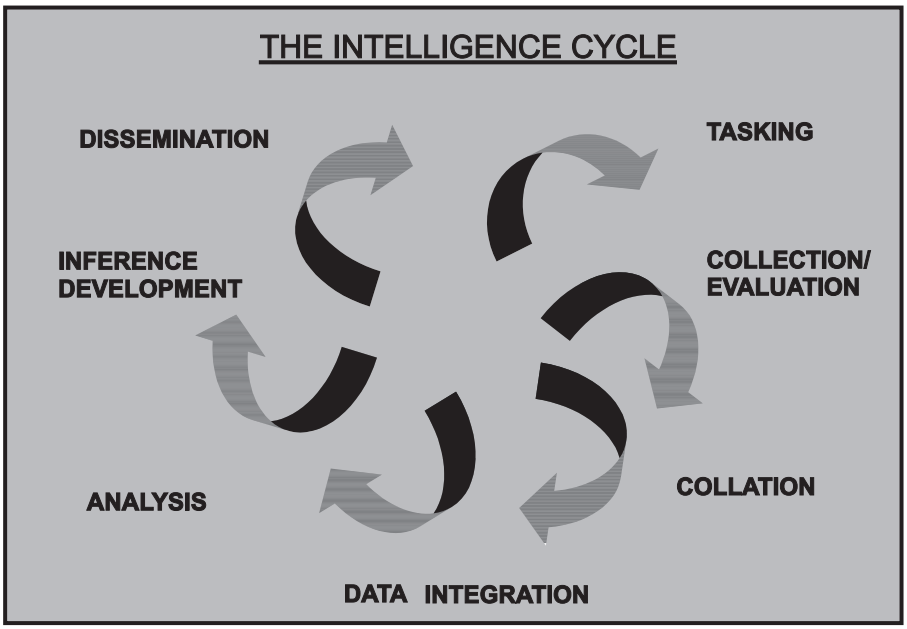

Figure 2-2: The Intelligence Cycle

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 pre-conceived ideas, but 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: 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. It 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 publicly available. One very notable sub-set 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 sensationalised.
- *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 be regarded also 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 to acquire 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 organised crime activities, which very often have a cross-border dimension. Exclusion of information (including Open Source information) purely on the principle 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 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 separate and assessment of the reliability of the source (the provider of the information) and validity and quality (accuracy) of the information.

Evaluation: 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 computerised 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 organisation of the data collected into a format from which it can be retrieved 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 discover it's 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 an 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 organise, summarise 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 jeopardise 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 the 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 like "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 the 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 formalised 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.

Chapter III

3. EXAMPLE NATIONAL INTELLIGENCE MODEL – THE UNITED KINGDOM

The National Intelligence Model (NIM) of the U.K. 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 organised 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.

Product	Aim	Purpose	Content
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 policy makers; To set a control strategy: priorities for intelligence, prevention and enforcement.	• Aim (terms of reference); • Scope (functional / geographic); • Current situation / survey; • Main objectives set / met; • Progress since last assessment; • Major areas of criminality; • Demographic / social problems; • Patterns / trends; • Resource constraints Overview / summary.
2. Tactical Assessment	To identify the shorter-term issues in an area this, with prompt action, can prevent a situation from deteriorating or developing. To monitor progress on current business in the 'tactical menu'.	To assist in the management of current operations and plans, as well as reallocate resources and efforts according to changing needs and problems.	• Current situation – progress on targeting; crime and other series; hot spots; preventive measures. • Options for further action. Advantages / disadvantages. Best courses of action. • Timeframe (short/medium). • Resource implications / changes.
3. Target Profile	To provide a detailed picture of the (potential) offender and his associates for subsequent action.	To assist operational management in selecting targets, guiding investigations, shaping plans and maintaining supervision.	• Personal record; • Criminal record; • Financial profile; • Network / associations report; • Communications report; • Transport report; • Surveillance appraisal; • Intelligence gaps.
4. Problem Profile	To identify established and emerging crime / incident series and crime hot spots.	To assist management in resourcing investigative needs, targeting, hot spot management, and directing crime-reduction initiatives and crime-prevention measures.	• Problem identification; • Background and causes; • Scale of damage; • Level of disorder / offending; • Perpetrators; • Internal / external links; • Social impact; • Resource implications.

Table 3-1: Four Categories of Intelligence Products

Prioritisation 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 in the result 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 Act Guidelines
- ECHR compliant 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
  - The copies of 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 specialised 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 computerised systems that contain:

  - Crime records
  - Open source data
  - Intelligence files
  - Analysis tools
  - Specialised databases (e.g., AFIS, NCIC, CBRS, RISSNET, NADDIS, 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 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 recognised as the backbone of the intelligence doctrine.

The correct balance to be struck between making information as widely available as possible to maximise 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 the national standard intelligence recording form which incorporates 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.

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

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

Product	Description	Purpose
7. Risk Analysis	The analysis of comparative risks posed by individual offenders or organisations to: • Individual potential victims; • The public at large; • Law enforcement agencies.	The compilation of risk assessments as a prelude to prioritising intelligence or enforcement work at both strategic and operational levels leads to completion of risk management plans.
8. Target Profile Analysis	Illuminates criminal capability and threat and includes information about: • Associations; • Lifestyle; • Operational modality; • Financial data; • Strengths and vulnerabilities; • Techniques which have worked or failed against the target in the past • Can cover any form of offending, not limited to purely 'criminal' activity.	Support target operations by: • Informing target selection; • Identifying needs for intelligence; • Indicating how sources and resources may be deployed against the target.
9.Operational Intelligence Assessment (Research)	The real time evaluation of and research into: • Incoming information on associations; • Other phenomena around suspects in a current operation; • May or may not be entirely the responsibility of an analyst.	The prevention of 'mission creep' and the prioritisation of investigative needs arising from incoming intelligence during a current operation, together with identification of resultant priorities for ongoing intelligence work.

Table 3-2: Nine types of Analytical Technique

Chapter IV

4. EVALUATION OF SOURCE AND DATA

EVALUATION OF SOURCES AND INFORMATION

Once information had 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 standardised 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 of the EU. 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.

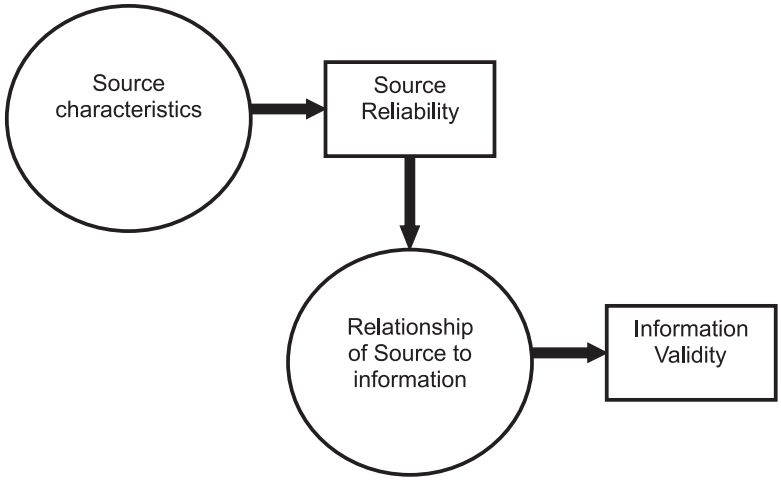

Figure 4-1: The Evaluation Process

Three fundamental principles apply to evaluation:

1. Evaluation 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. Evaluation must be carried out as close to the source as possible.

Evaluation Tables using the 4 x 4 System

Source Evaluation

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

Table 4-1: Source Evaluation; 4 x 4 System

Information evaluation

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

Table 4-2: Information Evaluation; 4 x 4 System

Evaluation Tables using the 6 x 6 System

Source Reliability

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

Table 4-3: Source Reliability; 6 x 6 System

Data Validity

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

Table 4-4: Data Validity; 6 x 6 System

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.

Following evaluation it is advisable to continue with intelligence classification, determining who has the right to know and the need to know. Once intelligence is integrated in the analysis product, it can be difficult to isolate elements of the whole with a higher level of sensitivity, restricting dissemination of these elements to a narrower group. The primary reason for classifying intelligence is the protection of the source, the circumstances or the method by which intelligence has been obtained.

The need for the above makes the issue of grading intelligence complex. It can be further compounded by the fact that any information of a more general nature, which forms part of an analytical product that also contains sensitive classified intelligence, will automatically be assigned higher grading and could become more difficult to access.

Chapter V

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: the careful examination of information to discover it's meaning and essential features

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

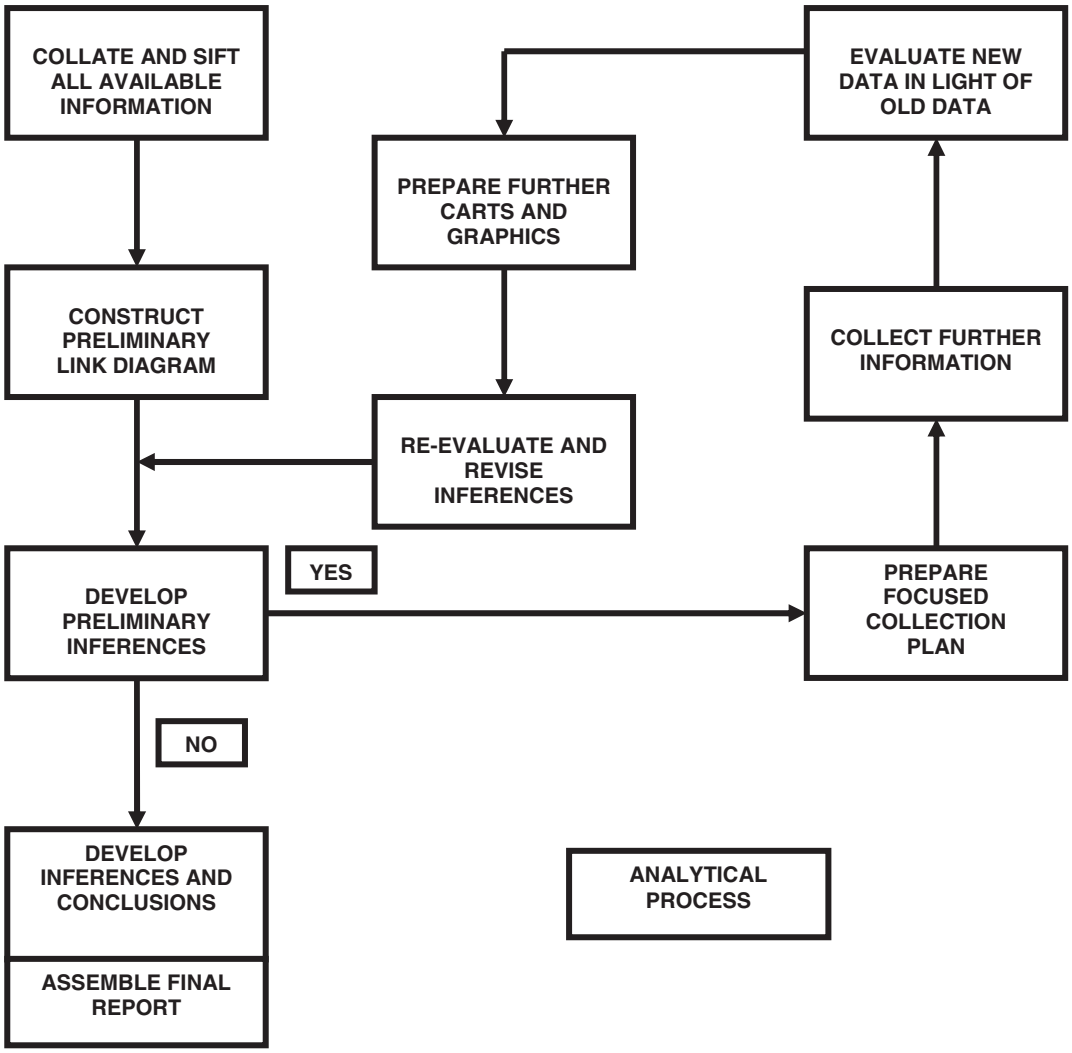

Figure 5-1: The Analytical Process

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 minimise 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 bi-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.

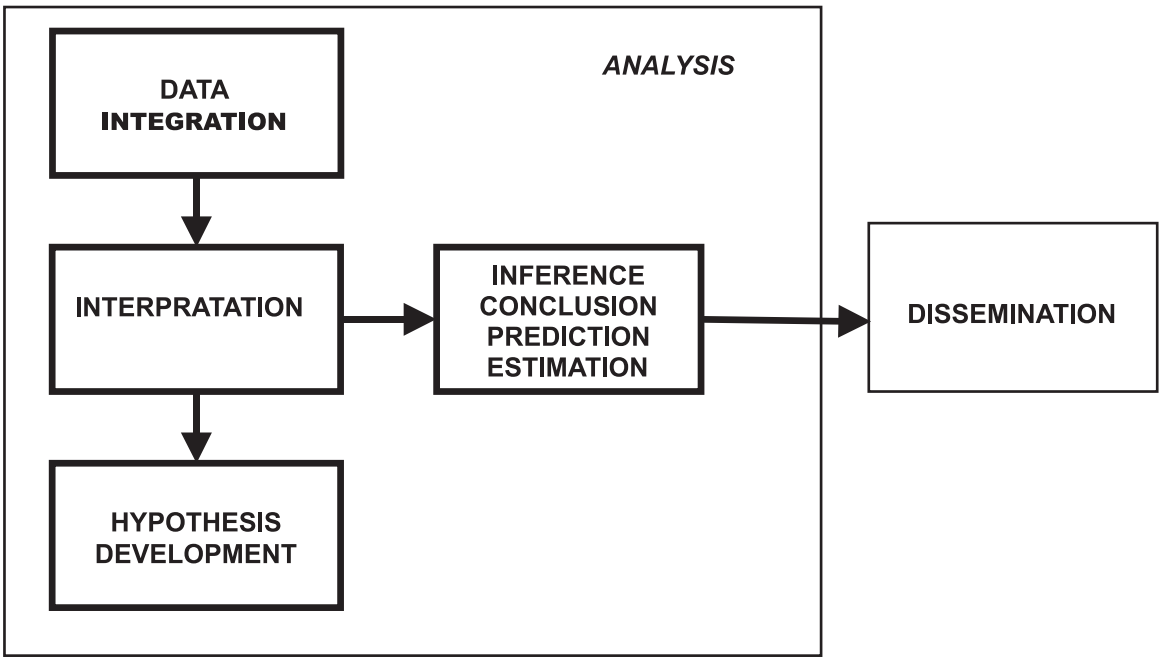

Figure 5-2: The Process of Analysis

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

1. Believe in your own professional judgement

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

2. 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 maximise your value to your agency.

3. 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.

4. 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.

5. 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.

6. 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.

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

Excessive details merely obscure the important facts.

8. 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.

9. 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, not the reason.

10. 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.

11. 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.

12. 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 programmes, compilation, visualisation, 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 organisation for which they are being produced.

Chapter VI

6. TYPES OF ANALYSIS

McDowell as shown in Figure 6-1 following identifies the use of intelligence at three levels, tactical, operational and strategic. In essence it is easiest to begin with tactical intelligence which will lead to a requirement for and can feed operational and strategic intelligence analysis

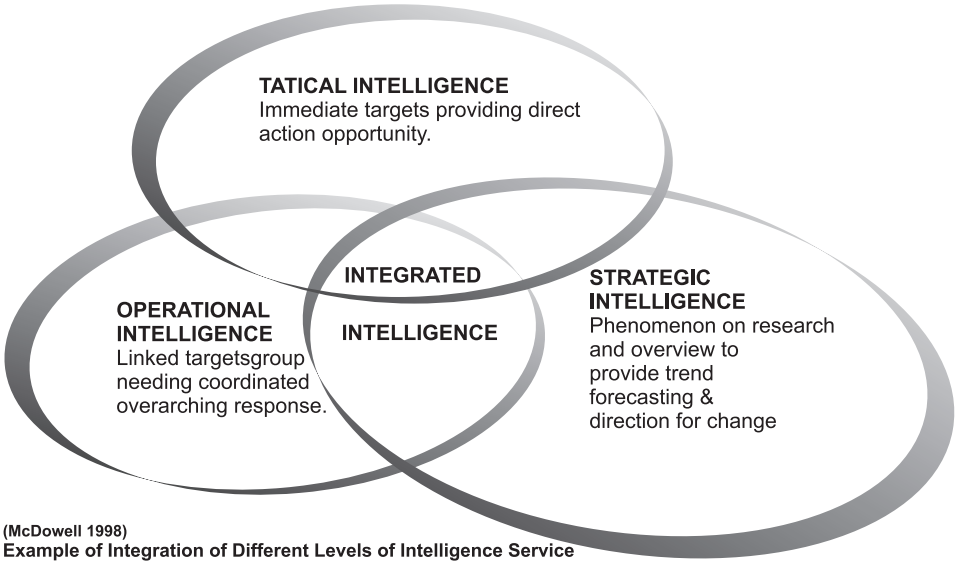

Figure 6-1: Integration of Intelligence Levels

TACTICAL INTELLIGENCE

Tactical intelligence is used to develop methods to counteract immediate criminal threats and is usually directed at a specific crime or criminal entity. It may be in reaction to an incident or used to prevent a crime.

Tactical information is usually factual data collected during case investigations and surveillance operations. The information may act as an investigative lead; or it may simply consist of a list of the subject's associations; provide locations of hang outs, listing of businesses associations, or describe criminal tendencies. This information gives law enforcement authorities a basic understanding of the criminals and their activities.

Tactical intelligence consists of this data in a compiled and analysed form: names, addresses, identifiers, criminal associates, and other identifying information. Tactical intelligence may take on many forms, but it is primarily the collection of facts to form a tile on a targeted subject with a view toward an investigation or prosecution. This tactical intelligence is collected on an ongoing basis and should be readily available as an effective and valuable resource for investigators working on criminal investigations. Finally, tactical intelligence provides the pieces of information that are the building blocks on which intelligence professionals build further analysis.

OPERATIONAL ANALYSIS

Operational analysis in essence consists of:

1. Summarising information received on a given enquiry in proportion to the reliability of the various components.

2. Identifying the silent features such as groups of, or individual criminals; relevant premises, contact points and methods of communication. Such identification may come as a result of a structured approach to information and intelligence gathering as a result of a criminal incident or identification of emerging trends.

3. Researching and interpreting information, carrying out further research, and then disseminating the results of the analysis as quickly as possible.

4. To give clear directions to operational teams in line with the aim of the intelligence led policing.

Enquiries can be of varying duration. During their course the impetus can fluctuate, and differing operational priorities present themselves. Part of the operational task of the analyst is to assist in ensuring a balance whilst at the same time adhering to the original direction of the enquiry, giving due weight and consideration to new development and priorities.

The length of operational analysis is immaterial. The most important factors for analyst are the nature, source and validity of the information dealt with. The results will be an assimilation of the data, which comprises of known facts and rumour, speculation and innuendo. The analytical product will contain further intelligence requirements, specific recommendations and options for further work. Equally essential and incumbent on the analyst, in operational work, is to research and develop information, in addition to answering operational questions, striking the correct balance between the two.

Analysts need to be flexible and creative and the quality of analysis is independent more upon the experience, accuracy and sensitiveness of the analyst themselves, rather than relying on the type of technique used. However a number of data integration techniques are used from the 'Analytical Tool Box' which is constantly evolving, due to the need to target the ever-changing activities of criminals.

Presentation techniques for operational analysis differ from that which is required for strategic analysis. More emphasis is placed on the production of charts, diagrams etc., which will often support oral briefings to operational teams. In this respect the presentation of operational analysis findings is often concise due to the need to produce both timely intelligence and to meet operational demands.

STRATEGIC ANALYSIS

The basic purpose of strategic analysis is to create knowledge to be used by decision makers for long term planning and allocation of resources. A strategic analysis is therefore future oriented. The time horizon depends on the character of the decision that has to be taken. When conducting a strategic analysis one can have different levels of ambition, depending on the task given to the analyst.

The lowest analytical ambition level is **descriptive analysis**, in which data and information is, by the use of scientifically acknowledged methods, systematically organised, analysed and presented. Often the purpose is to find out if there is any general trends in the development of criminality, or a pattern of crime, and occasionally also to see if it is possible to extrapolate trends into the future. Statistics are often used in this type of analysis and it is probably the most common conducted type of crime analysis.

A more difficult level of analysis is the **explanatory**. The base of this kind of analysis is most often a descriptive analysis. However, now the purpose is also to understand the causes of criminality. This is a very difficult task because it most often includes the study of a large amount of variables and an understanding of how they are related to each other. To be able to conduct this type of analysis in a proper way normally demands good knowledge in the use of scientific methodology.

The most difficult analysis is the **predictive** that is to make prognosis of future development. To predict the future in detail is of course impossible, but by using either descriptive or explanatory analytical results, or both types of material, it is possible to reduce uncertainties and at least make so called 'educated guesses'.

A strategic analysis often implies studies of complex relations of a large amount of variables. The approach and method should therefore be carefully considered and chosen. Methods used in, and experience from research within, academic disciplines such as social and political science, economics, criminology and behavioural science are often very useful when conducting various forms of strategic analyses. The outcome of a strategic analysis is often presented in form of a report, but oral briefings or presentations of a produced report are common in some law enforcement organisations.

A strategic analysis project can take many different forms. It could for example be:

- a general threat assessment;
- the production of a situation report or,
- a more specialised study of a certain phenomenon.

Detailed explanations are as follows:

Threat Assessments

The purpose of a threat assessment is to analyse and evaluate the character, scope and impact of criminality. Often they will be long term future oriented and therefore at the most difficult level of analytical ambition. It normally has to include an explanatory analysis, or at least a study, of various contributory factors. When having the ambition to predict the occurrence of certain phenomena it is of course necessary to try to understand what causes them. Therefore, one major part in the production of a threat assessment is almost always the study of relevant political, social, demographic, economic and other variables for the purpose of trying to understand their meaning and correlation.

Ideally threat assessments are used as basis in the planning process within law enforcement organisations. An assessment could be specific, that is concerning one or just a few types of crime, or it could be general about all types of crime that confronts an organisation.

Situation Reports

Another strategic analytical product is the situation report. This type of report is mainly descriptive and only oriented towards the current crime situation, and therefore is not as analytically ambitious or as difficult to conduct as a threat assessment. In a situation report the ambition may not be to evaluate the impact of criminality, rather just to give a description of the current situation. As with threat assessments, situation reports could be specific or general. However, such reports give a picture of the current crime situation, criminals' modus operandi etc. They are often used as an aid to decision making in respect of the allocation of resources, as well as the choice of methods and techniques to combat crime and should always attempt to be as predictive as possible and take into account, where available, trends apparent from previous reports.

Risk Assessments

The aim of a risk assessment is to identify and examine vulnerable areas of society that are, or could be, exploited. By examining weak, and vulnerable areas, for instance within a certain business sector, it will then be possible to give recommendations about a number of diverse issues such potential counter measures. When conducting risk assessments not only the character of the vulnerable sector, but also the nature of potential criminals and their modus operandi has to be taken into account.

When producing any strategic analysis the analyst should always remember that good presentation of the material will ensure the attentiveness of the reader. Therefore the analyst should:

- have sound knowledge of clients requirements;
- have an understanding of subject matter;
- have a clear idea of the structure of the report;
- make informed judgements;
- produce conclusions and recommendations that have practicality and relevance

Report writing is a skill in itself and specific training for the analyst may be required if they work in an environment that has set procedures and formats.

Chapter VII

7. SECURITY AND THE INTELLIGENCE PROCESS

INTRODUCTION

Law enforcement agencies, as a vital part of their function, have a legitimate requirement to collect and store information. A great deal of this information will be of a personal or operational nature; and, as such, privacy and security implications must always be at the forefront of information custodians' minds. Information that is not afforded adequate protection may be misused or alternatively accessed by unauthorised persons resulting in misuse of the information. Misuse of law enforcement information can be damaging to an agency's operations and reputation and can also place individual's lives or reputations in danger. Complacency and lack of due attention to security and control procedures can be a major contributing factor to the misuse of information. Alternatively, misuse may also result from corrupt behaviour on the part of law enforcement officers.

It is of the utmost importance that the opportunities for misuse are kept to an absolute minimum through appropriate safeguards and protective measures, adequate internal controls and suitable supervision. It is equally important that management and staff are aware of and understand the security needs of their organisation; and, in implementing suitable checks and balances, agencies should use an approach that encourages both personal and corporate integrity and develops an ethical climate that discourages the misuse of information.

THE INTELLIGENCE UNIT AND SECURITY

While all staff of an organisation has a duty to ensure security obligations are properly met, an intelligence unit's approach to security will be more extensive with greater emphasis on the protection of the unit's personnel, assets and information. The reasons for this are twofold. Firstly, the intelligence function of a law enforcement agency is, perhaps, one of the most sensitive areas in respect of the collection, storage and use of information. Not only could the misuse or unauthorised release of intelligence information jeopardize an agency's operations, but such release could also be extremely harmful to the individuals concerned - particularly when the intelligence is yet to be confirmed or verified. Secondly, the very nature of an intelligence unit's work and the information it holds significantly increases the risk of the unit and its staff being targeted by organised crime for penetration and corruption.

THE *MUSTS* OF SECURITY

Security is a series of procedures and measures which, when combined, provide protection of people from harm; information from improper disclosure or alteration; and assets from theft or damage. The basic premise on which all successful security systems are based is that no single security measure is, by itself, relied upon (Criminal Justice Commission 1995:1.7). To be effective, a system *must* comprise a number of complementary 'layers' that provide checks and balances and multi-level protection. This is often referred to as the 'defence in depth' approach. In ensuring that intelligence information is being appropriately and securely dealt with, consideration *must* be given to the 'security layers' that can be applied in respect of personnel, physical accommodation and information handling.

The intelligence unit *must* take steps to ensure that all members of the unit are of the highest possible integrity, with no personal circumstances or links to criminality that may see their integrity compromised. The unit *must* ensure it is physically secured at all times and that only authorised personnel can gain access to the intelligence work area. When handling information and files, intelligence personnel *must* also adopt work practices that ensure information is processed in such a way as to prevent unauthorised access to their work. In general terms, the unit *must* take all appropriate measures to restrict knowledge of the unit's activities to as few persons as possible to avoid any compromise of those activities.

Suitable security measures relating to staff and the operational environment will ensure that intelligence material is handled, processed and used in a manner, which is commensurate with its sensitivity and, at no time, is placed at risk of passing into the hands of unauthorised persons. This will be achieved by ensuring that:

- the capture of intelligence material and the methods used are properly controlled;
- the storage of intelligence material is secure;
- the validity of intelligence material is confirmed;
- the integrity of intelligence material is maintained;
- the intelligence material is only available to persons deemed to have a need and right to that material;
- disseminated intelligence material is only used for legitimate law enforcement purposes;
- transmission of intelligence material is via secure means;
- there is overall management control and appropriate accountability for the intelligence system and related procedures.

It is important to understand that, in addition to protecting against any compromise of the intelligence unit's activities, the security system also has an important role in protecting the right to privacy of individuals. A great deal of the information captured for intelligence purposes is drawn from allegations, unverified reports of activities and associations, and other sources where the veracity of the information has not been fully tested. For example, Godfrey and Harris (1971:93) discussed how the surveillance of several individuals arriving at a particular premise allegedly for a criminal enterprise meeting, confirms their presence at the premises, but does not confirm the relationship between the persons seen entering the premises. They went on to highlight how the problem is even more complicated where a public place, such as a restaurant, is involved. Who is engaged in conspiracy, and who is simply a hungry or thirsty member of the public? Similarly, if telephone records show the phone of a criminal target 'A' called the phone of 'B', this does not necessarily mean 'B' is involved in 'A's' criminal activities. Without confirmation of the users of the two phones at the time in question and the details of the conversation at the time, it cannot be verified whether 'A' indeed called 'B' or for what purpose the call was made. 'B' could be later found to be totally innocent of any involvement of knowledge of 'A's' activities.

Information from observations of this kind can seldom be presented in court and, without other corroborating evidence, cannot be verified. It is, however, essential information for intelligence purposes in seeking to develop an understanding of the associations, networks and operational patterns of organised crime.

With this in mind, intelligence unit personnel and their managers must be fully aware of their responsibility to maintain a security system not only for protection of their own operations but also for the protection of individual's rights, by preventing the inadvertent leakage of unsubstantiated information that might be damaging to the person, or persons, to whom the information refers - whether or not that person has a criminal record.

THE *MUST-NOTS* OF SECURITY

While the importance of security in protecting against any compromise of the intelligence unit's activities can never be overstated, it is important that security procedures are not applied to an extent where they impede the flow and use of intelligence products. Godfrey and Harris (1971:93) highlighted this fact in discussing a number of areas for which security policy should not be used to excess. These areas are still relevant today; and, in this respect, when preparing security policy and guidelines, the intelligence unit should note the following.

Security *must not* be used to exclude authorised persons with a legitimate need and right to know from accessing intelligence reports and findings. Intelligence is only of use if it is disseminated to clients who need it. It is of little use if retained purely for the knowledge of intelligence personnel. Once a consumer's need to know is determined, and found appropriate, the intelligence material must be made available. Watson et al, (1990: 405) discuss 'Need to know' and the 'Need to know principle' as general intelligence terms. The concept of 'Need to know' involves not allowing access to information to those who do not need it to perform their job. For example staff in an intelligence unit has no need to know the terms of employment of other staff within an organisation so they are denied access. Staff working in the personnel section of the agency has no need to know details of Intelligence targets so they are not told. It is important to stress that access is by need and not solely by virtue of position, rank or level of security clearance within an agency. Even a person with the highest level of security clearance may be denied access to particular information on a basis that there is no 'need to know'.

The intelligence unit may place security conditions on the intelligence material and security obligations on the recipient in respect of how the material should be handled. However, the purpose of such conditions is to ensure that the material is suitably actioned by the appropriate people with due regard to its sensitivity, not to prevent it from being read.

Security *must not* - under any circumstances - be used to conceal the employment of illegal or unauthorised techniques, such as electronic surveillance, where such is not permitted by law in a particular jurisdiction or if permitted where correct legal procedures have not been followed. Intelligence personnel and intelligence units must operate lawfully at all times and be accountable for their actions through appropriate documentation and audit procedures.

Security *must not* be used to conceal reports from the jurisdiction's political leadership or other representatives who are not members of the law enforcement agency. Nor should security be used to prevent documents from being used for prosecution purposes, even though the sources may be highly sensitive.
Security *must not* be used to conceal or cover up mistakes or corrupt activities by members of the unit or agency.

SUMMARY

This brief introduction highlights how the sensitive nature of intelligence necessitates that security procedures must be an integral part of an intelligence unit's day to day function. A key objective of security is to maintain the integrity of the intelligence unit, its staff and its information. This objective is best achieved by applying a 'defence in depth' approach in respect of the following areas:

- *Personnel Security* to assure the personal integrity of the organisation's staff;
- *Physical Security* to protect the organisation's accommodation and assets;
- *Information Security* to protect information against inadvertent use or unauthorised access.

These areas are discussed in more detail in the following pages in order to give readers a basic insight into the steps that should be taken to maintain the integrity of the intelligence process.

In addition to providing for a secure and successful intelligence function, the adherence to sound security procedures should enhance the morale of the agency as a whole by providing strong resistance to misconduct and corruption. It should also encourage a greater flow of intelligence from within the agency due to the confidence in the security of the intelligence unit.

PERSONNEL SECURITY

"Personnel security is the means or procedures, such as selective investigations, record checks, personal interviews, and supervisory controls, that are designed to provide reasonable assurance that people being considered for access to classified information are loyal and trustworthy" (Watson, et al. 1990:435). The sensitivity of the intelligence area, and the information it handles, requires that personnel engaged

in intelligence work be subject to extensive background checks prior to their employment or transfer to such areas. Personnel security vetting is a process that checks a person's identity and verifies his or her background, character, and financial situation, in order to ascertain with a degree of certainty that the person is trustworthy, discreet and of suitable integrity for employment and access to classified material. This process goes beyond the basic pre-employment checks, as it does not necessarily follow that a person suitable for employment within the general stream of duties in an agency is automatically suitable for access to secure areas and classified material (Commonwealth of Australia 1991:85).

The integrity of a person can only be determined by probing the background of the person, his or her past employment history, associations, and lifestyle. In discussing background investigation, Godfrey and Harris (1971:94) described the process as "not a perfect system by any means;" however, experience has shown that when done thoroughly, background security vetting does provide an effective means of establishing a person's suitability for employment.

All intelligence staff must undergo initial vetting and be security cleared before commencing employment. Security vetting is a voluntary process and the potential staff member must consent to their background being investigated for the purposes of employment. Naturally, if consent is not given, employment will not be considered further as the obtaining of an appropriate security clearance (an administrative determination that an individual is eligible, from a security standpoint, for access to classified information (Watson, et al.1990:505) staff should also be required to report any changes in personal circumstances, and undergo periodic security checks, to confirm continued suitability for intelligence duties.

Initial Security Vetting - The Background Investigation

Initial security vetting of a potential employee is conducted by way of a background investigation that should probe all aspects of the person's professional and personal life. The investigation should seek to detect indications of lack of character or lack of integrity. Godfrey and Harris (1971:94) correctly pointed out that a person who lacks integrity in their personal life - for example, in past dealings with family or associates - should be considered a potential risk to act without integrity in a professional capacity, at some time in the future. Similarly, during a background investigation, inquiries with past employers will assist considerably in judging the person's suitability for intelligence duties.

To assist in conducting the background security investigation, the person under consideration should be requested to complete a security vetting questionnaire - providing both personal and financial information. The questionnaire should require the person to provide full and accurate information in respect of the following:

- personal details, including previous names;
- family details, including spouse and children;
- current and past residential addresses;
- education history, including places of education;
- employment history, including contact details of past supervisors;
- travel movements (if applicable);
- details of any criminal convictions;
- details of any other adverse encounters with the law, including traffic offences;
- financial details, including savings, investments and assets.

The questionnaire should conclude with a certification by the person as to the accuracy and completeness of the information provided. The person completing the questionnaire should also be required to provide certified copies of supporting documentation such as birth certificate, marriage certificate, passport, drivers' license, and education / professional qualification certificates.

Armed with the information from the questionnaire, the officer performing the background security investigation can then conduct independent checks to verify the information provided and explore any particular areas that require further evaluation. When appropriate the investigating officer should seek

additional information by contacting persons previously associated with the person under consideration such as past educators, past employers, family members, neighbours, etc. It is essential that the investigator carefully evaluates all information available on the subject of the investigation and that a balanced and informed assessment is made of the individual's reliability and trustworthiness. (Character Assessment is as the balanced and informed estimation of an individual's reliability and trustworthiness which is derived from comprehensive checks on identity, background, personal values and behaviour.) An assessment of the subject's maturity, responsibility, tolerance, honesty and loyalty in past situations will enable conclusions to be drawn regarding the suitability of the subject.

It is also essential that the investigator verify the legitimacy of any documents provided by the subject. With the ease of access to sophisticated graphic software, it is not difficult today to produce high-quality certificates and other documentation that to all intent and purpose appears genuine. Checks must, therefore, be made with the issuing authorities to confirm that the claims made by the applicant are authenticated.

Any information that casts doubt over the subject's integrity or character must be fully explored to a point where the information is either corroborated or discredited. For example, as Godfrey and Harris (1971:94) discussed, it would be of little value to simply report an allegation that a previous landlady felt the subject was an undesirable tenant because of noisy parties and wild goings-on that caused complaints from neighbours. The investigator would be duty bound to ascertain the character of the landlady and her relationship to the subject. The investigator would also have a duty to check the allegation with the neighbours and to ascertain if other information was available regarding the subject's social activities. If the investigator were simply to report that the allegation could not be substantiated, it would be open to conclude that in the absence of other evidence, there remains a possibility that the criticism reflects accurately on the subject's social life. If, on the other hand, details of the additional information gathered during evaluation are included in the investigator's report, a clearer record is created. If the additional information enables the investigator to draw a firm conclusion, the record not only facilitates the removal of any doubt as to whether the allegation is substantiated or discredited but also ensures that the matter is clarified once and for all.

If the investigator is unable to draw a firm conclusion regarding a particular allegation and doubt remains as to the subject's character or integrity due to the allegation, then the matter should be raised with the subject. As Godfrey and Harris (1971:95) correctly pointed out, such a procedure is delicate and should be undertaken with care and preplanning. A formal but not unfriendly atmosphere is recommended for such confrontations. Often, the subject's responses will provide sufficient additional information to enable the matter to be clarified. If not, the confrontation will provide an opportunity for the investigator to observe the subject's reactions and facial expressions, which may contribute to the investigator's assessment of the matter.

In addition to probing the personal background of a person under consideration for employment in an intelligence role, it is equally important to examine the person's financial standing. Such an examination will determine whether the subject is in any financial difficulty. A poor history of financial responsibility could cast doubts on the subject's reliability and responsibility in other areas of life. On the other hand, financial problems have the potential to place a person at risk of compromise in the form of corruption or blackmail. The subject's financial information should be cross-referenced with other lifestyle and employment information to provide a more complete assessment of earnings and expenditure. Additionally, the recording of an employee's financial information at the commencement of employment provides a base for future comparisons should any allegations be made regarding unexplained wealth or changes in lifestyle.

If, having concluded all aspects of the background security investigation, the investigator is satisfied that the subject's background, character and financial situation reveal nothing adverse; it can be concluded, with a degree of certainty, that the person is trustworthy and of suitable integrity for employment and access to classified material. A security clearance can, therefore, be issued. If, on the other hand, at the conclusion of the background security investigation, any doubt remains as to the character or integrity of the subject, then a security clearance cannot be granted; and the person cannot be considered further for employment in the intelligence unit.

Periodic Security Checks

The fact that a person is cleared for employment at a particular time does not necessarily mean that person will always be suitable for employment. The person's circumstances, values, attitudes and other traits could be changed over time. It is, therefore, important that information impacting on security clearances is kept up to date and procedures are in place for this to happen. On commencing employment, intelligence personnel should be briefed on the security requirements of their position. They should be advised that, during their employment they are required to report any changes in personal or financial circumstances in order that an assessment can be made as to whether the changes impact on their security clearance. They should also be advised that, in addition to any changes they report, they will also be required, from time to time, to undergo periodic security checks to confirm their continued suitability for intelligence duties.

Periodic security checks should involve an updating of the initial background security investigation, focusing in particular on the officer's personal life and financial status. Any significant changes to the officer's previous profile should be investigated. For example, if social activities are found to have changed and there is evidence of increased spending or substantial borrowing, explanations should be sought for the changes. While increased income may have a legitimate source, if no apparent source can be identified the subject officer may fall under suspicion of corrupt activity. Alternatively, increased borrowing could indicate the subject officer may be vulnerable to corrupt approaches.

Periodic security updates should be conducted at regular intervals - say, for example, every two years. Personnel should be advised of these procedures and encouraged to actively participate as part of the unit's anti-corruption strategy. Pride in the integrity of the unit and its personnel should be the over-riding objective.

Notwithstanding the regular security procedures, the unit commander always retains full authority to order a background security investigation of one of the unit's personnel at any time. The commander, after all, is responsible for the overall integrity of the unit. If there is any suspicion regarding the integrity or character of one of the unit's personnel, the commander should act immediately rather than wait for the next periodic security check. Any delay in acting on such suspicions would expose the intelligence unit to an unacceptable risk of serious damage.

Physical Security

Physical security is described by some as having two meanings. The first involving the "physical measures used to protect classified equipment, material and documents from disclosure to unauthorised persons" (Watson, et al 1990:438). The second involving the "physical measures, such as safes, vaults, perimeter barriers, guard systems, alarms and access controls that are deigned to safeguard installations against damage, disruption, or unauthorised entry, information, or material against unauthorised access or theft, and specified personnel against harm" (Watson, et al. 1990:438).

Put simply from a law enforcement intelligence unit perspective, physical security involves the steps taken by an agency to provide physical barriers that prevent unauthorised access to premises and information, and protect personnel from physical harm (Criminal Justice Commission 1995:4.1). This is best achieved by having systems that enable premises to be secure when unattended and for access to be monitored. Persons authorised to access the intelligence unit should wear appropriate ID passes at all times when in the unit, and any other visitors should be escorted. The security system should, where possible, include electronic keys and audit logs of all access. In addition to secure access to the unit, all information and related documents should be stored in secure containers such as safes, strong rooms or secure lockable cabinets.

With appropriate physical security in place, personnel within the intelligence unit should have confidence that they can work freely without fear of compromising their material.

The Physical Environment

The location of the intelligence unit should be given careful consideration in order that the unit may be given the optimum protection. If at all possible, you do not want an area that handles extremely sensitive information to be located on the ground floor of the agency's accommodation. Nor would it be wise to locate such an area close to a main entrance or busy corridors. To reduce the risk of unauthorised persons accessing the intelligence area, it is wiser to locate the unit above the ground floor and in a quieter part of the agency accommodation where there is less passing traffic, so to speak.

The physical work environment of the intelligence unit must be secure at all times, with access restricted to authorised personnel only. This is best achieved by issuing all unit personnel with identification passes, which must be worn in a visible manner at all times while working in the unit and by utilising a single controlled access point, which requires unit personnel to use individual unique security keys to gain entry. (Modern technology provides numerous access security systems, ranging from simple electronically coded keys and proximity cards, to the more sophisticated systems that recognise individual attributes such as voice, fingerprint, and retina.) By using this type of electronic security system, a security audit log can be generated for all access to the unit. Where there is a necessity for visitors to enter the unit for legitimate work-related reasons, there must be a physical method of identifying the visitor and recording their access. A common method of recording visitors is to use a register, which can be completed with the following details:

- date of visit;
- name of visitor;
- agency or organisation the visitor represents;
- name of the officer to be visited;
- time of the visitor's arrival;
- time of the visitor's departure;
- signature of the visitor.

On completion of the register, visitors should be issued with - and instructed to - visibly display temporary visitors passes while within the intelligence unit.

During normal working hours, the responsibility for recording access to the unit by non-unit personnel should rest with a specific staff member. Outside of normal working hours, the unit should be secured to the extent that only unit personnel using their security keys may gain access. Movement detectors and internal surveillance cameras can provide additional levels of protection for the unit when unattended. If such devices are installed, they must be linked to an alarm system, which is monitored on a 24-hour basis; for example, in the agency's main operation control room.

Building regulations and work place safety requirements usually require that offices have more than one exit in case of fire or other emergency. Within a secure intelligence unit such exits should be designed for 'emergency flight from the unit only.' All emergency exits should be alarmed so that, if they are opened at any time, attention is immediately drawn to the fact that the security of the unit may be at risk of being compromised.

Central Registry / File Room

Intelligence files and source documents should be centrally stored in a separately secured dedicated area within the intelligence unit. This provides for a further level of security within the unit and also enables additional controls to be placed on the movement of material. The walls of the central file room must be from slab to slab, rather than floor to ceiling, as many modern ceilings have open cavities for air-conditioning ducts and fire sprinklers, etc. Where possible, the walls and door should be at least fire-resistant, if not fireproof.

Access to the file room should be restricted to a small number of personnel (specifically the registry / file room personnel) and through a single door, which has a similar security access control system to that used for the main entrance to the intelligence unit. All movement of material to and from the file room must be recorded by the registry / file room personnel to ensure a full audit trail is maintained of access to material and to know exactly who has possession of particular material at any given time, should it be required by other personnel.

Storage Containers

When in day-to-day use, it is sometimes impracticable to return all material to the central file repository. In such cases, intelligence personnel must have access to their own secure storage containers. In seeking to protect documentary information, the storage container in which the information is contained is the last line of defence. Storage containers must provide an adequate level of protection commensurate with the sensitivity of the material to be stored.

Clear Desk Policy

An additional security measure to prevent unauthorised knowledge of information is to ensure that all staff practice a 'clear desk policy' when absent from their work place for an extended period of time. This will include securing material in appropriate containers and either logging off computer systems or implementing a password-protected screen saver. This type of security practice is particularly important in work areas that have open plan accommodation and where compartmentalisation is difficult. It is also an important practice, on occasions, where an intelligence officer is seconded to assist another investigation unit that may not be afforded the same level of security as that of the intelligence unit.

Information Security

Watson, et al. (1990:291), defines information security as "the process of safeguarding knowledge against unauthorised disclosure." When handling information and files, intelligence personnel must adopt work practices that ensure information is processed in such a way as to prevent unauthorised access to their work. Information security systems are based on the principles of accountability and protection. "It is axiomatic that, in order to be able to account for information, there must be a record of its existence. Also some items of information are more sensitive than others and, therefore, require a greater level of protection (Criminal Justice Commission 1995:5.1). These principles are recognized by the use of a system that not only records information but also allocates security classifications and restrictions to differing levels of information sensitivity.

Classification Systems

Information should be allocated a security classification dependent on its sensitivity and the level of protection it requires. The criteria for assessing the sensitivity of files or information are, at best, subjective. That is to say, a personal judgment factor enters into most decisions as to whether a file, or particular piece of information, requires special treatment and protective handling. When making such assessments, consideration should be given to the amount of damage that could result - now or in the future - from any unauthorised disclosure, alteration or destruction of the information.

Commonly used classification systems usually employ three distinct categories of classification, for example 'restricted, confidential, secret', 'in-confidence, protected, highly protected'; or alternatively 'confidential, secret, top-secret'. Such classifications are a form of caveat that warns the recipient of his or her responsibility and liability with regard to the security of the information. As a general rule, the level of classification should be kept to a minimum consistent with affording adequate protection to the information. The urge to apply a higher classification when in doubt should be resisted. Over-classifying can result in expensive storage and auditing measures and ultimately bring the system into disrepute.

In addition to utilising a classification system, similar to that described above, the intelligence unit can also introduce a range of subject indicators that provide for additional categorisation of information. A past approach to this type of additional categorisation, discussed by Godfrey and Harris (1971:100) was to use colour tabs, or a combination of tabs, to alert users to certain aspect of the information or document's contents. For example, a particular colour tab could indicate if the information is independently corroborated, a different colour could indicate that the matter involves corruption. Today, the use of technology and various computer software packages enables these categories to be an integral part of the intelligence unit's database. The database records should clearly indicate the various subject matters covered in each document and also indicate any restrictions that are placed on the use of the material. In this way, personnel accessing the database should be able to quickly identify not only the classification level of the material, but also the matters the material relates to and whether there are additional restrictions placed on the material's use.

An additional level of security used by some agencies is to use special security paper in addition to other caveats. Such paper makes each particular hard copy document unique, should there be more that one copy of the document.

Storage of Intelligence Material

Intelligence information should be stored in both hard-copy and electronic format. Hard-copy source documents must be retained in order to verify data recorded electronically. In addition to providing for secure storage of documents, as discussed under the heading of 'Physical Security' , the intelligence unit must also have procedures in place to provide for appropriate backup copies of electronic data. Backup copies of electronic data should be created on a regular basis and stored at a separate secure location. Backup procedures provide a full record of the data at any given time in the past. This can be useful if an allegation is made that data has been tampered with. The existence of a full backup of electronic data also ensures a minimal amount of data is lost should a disaster of some type (for example a total system failure or fire) strike the intelligence unit. Collation methods and appropriate storage procedures for both electronic and hard copy material should be detailed in written procedural instructions. The procedures should provide for appropriate security and specifically nominate who is responsible for such material.

Access to electronically stored data should be subject to strict authorisation, with appropriate procedures in place to ensure security is maintained. Authorised access should only be granted on a need to know basis, and each user uniquely identifiable through secure user ID's and personal passwords. Individual user ID's, coupled with appropriate structuring of data storage procedures, will restrict access to only that data to which that user has a need to access. All access transactions should be logged, and procedures should exist for audits to be conducted in this respect. Such procedures should cover both reactive and proactive auditing. Audits should be documented and available for inspection.

Included within access controls are any facilities that allow extraction / transfer of electronic data (for example, downloading from a central database to other applications such as a PC database or software graphics package). Any such facilities must be subject to strict control procedures, as access to such extracted data must also be maintained for audit purposes.

Although seen by some as inconvenient, where possible the use of floppy disks should be avoided or alternatively strictly controlled. This type of additional security approach will not only help to prevent unauthorised copying of electronic records but will also help to guard against damage by computer viruses[2] that may be imported electronically through the use of disks or direct downloads / electronic transfers of data.
Suitable security precautions against this type of threat should include:

- strict control over who has the ability to change the operating system and applications software
- strict procedures controlling the import of software or documents from external sources
- compulsory use of virus checking software for all imported software and documents before being loaded onto the unit's main system;
- a suitable decontamination plan should damage occur.

[2] *A virus is a code inserted into an apparently harmless piece of software or document that is able to reproduce by copying itself into other software or documents. A virus will inevitably carry a logic bomb, perhaps benign but frequently capable of doing serious damage to the system*

Integrity of Intelligence Material Quality Control

In addition to preventing unauthorised access to intelligence data, it is equally important that procedures are in place to ensure that the integrity of intelligence data is maintained. Relevance, accuracy and reliability are major considerations in respect of integrity. These factors are particularly important in respect of electronic databases, which are accessed and relied upon more frequently than hard-copy material. As such, intelligence databases should be subject to a specified process of quality control, with a dedicated member of the intelligence unit being responsible to checking new data after collation to verify it is free from error and that it has been correctly classified and stored.

Dissemination of Intelligence

The security of intelligence unit and its information systems also extends to the dissemination of intelligence material, either at the unit's own initiative or in answer to requests from other units or agencies. Intelligence information should, under no circumstances, be provided to non-law enforcement agencies. When disseminating to a law enforcement agency, care should also be taken to ensure that the receiving agency has appropriate procedures in place to ensure that the security of the information is maintained at an appropriate level.

It should be clear to all personnel within the intelligence unit who has the authority to authorise the dissemination of intelligence material. This authority will ordinarily rest with the commander / officer in charge and / or one or more of the senior managers of the unit if the unit is large. Procedures should provide for a record to be kept of all such disseminations; highlighting the data disseminated; the reason for dissemination, to whom and by whom it was disseminated, and how the information was disseminated.

Where a request for information is received from outside of the unit, procedures should detail how an individual intelligence officer should receive and respond to the request. The identity of the requesting officer and the reason for the request should be carefully considered in order to verify if the request satisfies the need and right to know principles. Records of all disseminations should be retained and be available for auditing.

In respect of the actual physical transmission of intelligence material, the intelligence unit should have clear procedures regarding how intelligence material - both hard-copy and electronic copy - should be dispatched. Such procedures should provide for appropriate security through the use of suitable packaging such as double enveloping, receipt books and methods of transmission. Extremely sensitive material should only be dispatched via a secure 'safe-hand' system. All records and receipts should be retained and available for inspection.

Responsibility of the Unit Commander

While all staff members have an obligation to maintain security, it should be noted that the intelligence unit commander has a particular responsibility for the effectiveness of an intelligence unit's security system and related policies and practices.

Chapter VIII

8. MANAGEMENT OF THE INTELLIGENCE UNIT

INTRODUCTION

The term 'management' has been defined as the control and direction of organisational resources to achieve defined goals. Traditionally, managers have been tasked with the functions of planning, directing, staffing, training, budgeting, coordinating, reporting, providing public information and obtaining appropriate equipment. All of these functions are familiar to law enforcement managers. This chapter, however, will be focusing on those unique managerial challenges that occur when a law enforcement manager assumes the role of managing a criminal intelligence unit. When that occurs, the manager's role becomes more complex; and there are a number of issues that must be recognised and considered.

CHALLENGES

The primary issue for the new manager involves understanding the proactive concept of criminal intelligence and how the process works. Harris called the management of the police intelligence unit, "Perhaps the most difficult assignment that can be given to a supervisor in a police department". Part of this difficulty is because many law enforcement managers have had little exposure to intelligence, and an assignment as an intelligence unit manager will be their first opportunity to understand and work with the concept. Most law enforcement managers learned policing from the street up and have been trained throughout their careers to deal with problems in a reactive mode. Criminal intelligence requires a new mindset since it is an effort to change the perspective from a reactive approach to a proactive one. In essence, intelligence attempts to learn of criminal activity before it occurs and prepare the agency to deal with specific crime issues when they are small and can be managed with minimal resources. Once a crime problem takes root, it becomes more difficult to manage and requires additional resources.

Simply stated, a properly managed criminal intelligence function can have a tremendous impact on a law enforcement agency and the community it serves. However, the key words in that sentence are 'properly managed'. It is not an easy task to properly manage this multidimensional task. It requires a trained staff that is provided appropriate direction and has the support of the agency, the political body that governs the agency, and the community it serves.

Law enforcement administrators can now benefit from a professionally managed criminal intelligence unit without being overly concerned about the threat of adverse litigation. The potential difficulty in this scenario, however, relates to the fact that much of the public is unaware of the professional standards now in place for criminal intelligence and might still have a negative view of government and the intelligence function. Thus, it falls to the unit manager and the agency's chief executive officer to sell the importance and legitimacy of the criminal intelligence function to community wide audiences, including the agency's governing body. This can be accomplished with an ongoing, educational effort to inform politicians and citizens about criminal intelligence and its value to the safety of the jurisdiction. It needs to be well known that criminal intelligence is a proactive crime prevention effort and a viable part of community oriented policing. The educational effort can be supplemented with periodic reports to the involved city council or county board of supervisors, which reinforces the function's legal capabilities and identifies in general terms the existing criminal threats to the jurisdiction.

CRIMINAL INTELLIGENCE RESPONSIBILITIES

One of the first considerations for an agency is the extent of responsibilities that it intends to accept concerning the criminal intelligence function. Obviously, this is a local decision; but conditions regarding size of the agency and criminal issues within the area should dictate the need, mission and resources of the unit. In 1973, the National Advisory Commission on Criminal Justice Standards and Goals supported the concept that any police agency with at least 75 sworn personnel should employ a full-time criminal intelligence officer (Police Standard 9.11). This guideline may be a starting point for an agency but might not satisfy an agency's need for criminal intelligence. Organised crime and terrorist activity is seldom overt and certainly does not recognise jurisdictional boundaries. Many times, an agency will need to perform a threat assessment to learn the extent of its organised crime presence.

A small agency needs to understand the proactive concept of criminal intelligence and recognise that most law enforcement agencies, regardless of size, are susceptible to organised criminal activity that may extend beyond jurisdictional boundaries. Their personnel should be trained to recognise and report indications of organised crime, and criminal extremist and terrorist activity. This information should then be shared with intelligence-trained personnel from neighbouring agencies, the sheriffs department or appropriate state law enforcement agencies. Often, small pieces of information, which may appear inconsequential by themselves, can be a significant part of a larger picture pertaining to a criminal enterprise. This type of effort by members of smaller agencies would be important steps in allowing for criminal activity to be analysed and evaluated on a larger scale either county wide, regionally or state-wide.

Medium-sized agencies (75 to 250 sworn officers) and large agencies (Over 250 sworn officers) should have a criminal intelligence function. The size of the unit would depend upon local crime conditions and the scope of the unit's mission. Agencies with only one or two officers assigned to the unit may have an issue regarding the availability of sufficient resources for accomplishing all of the functions required by the intelligence process.

A viable option for reducing the intelligence workload for a medium-sized agency is to enter into a networking or mutual aid criminal intelligence agreement. These agreements can be either formal or informal, with any number of surrounding law enforcement jurisdictions. Conceivably, neighbouring agencies have common problems that can be approached with shared resources. This type of agreement allows an agency to assign limited personnel to work with intelligence officers from surrounding jurisdictions on combined investigations. This concept can be expanded to the point where one lead agency within a region maintains the responsibility for keeping the intelligence file while other member agencies provide the investigative personnel. Member agencies would have access to the file for both input and dissemination purposes. The pooling of resources from several agencies is a tremendous asset in the area of training new or inexperienced criminal intelligence officers. Another benefit to this type of arrangement is that individual agencies do not lose all of their criminal intelligence expertise if an officer retires, promotes or transfers from the criminal intelligence position. Instead, there is a pool of expertise to service the combined areas.

Specific responsibilities for criminal intelligence units include the following:

1. Initiate inquiries and conduct information searches to obtain criminal intelligence information relating to specific criminal activities designated by the chief executive officer.
2. Develop and maintain a system for collecting, reviewing, evaluating, storing, collating, retrieving and disseminating information relating to designated criminal activities.
3. Develop analytical capability to provide useful criminal intelligence reports, both strategic and tactical.
4. Maintain the integrity and security of all information entrusted to the unit.
5. Adhere to legal and ethical procedures in obtaining information.
6. Develop methods to evaluate the effectiveness of the unit in accomplishing its law enforcement goals and in safeguarding the privacy of all individuals about whom the unit has information.
7. Establish and maintain liaison with law enforcement agencies at all levels in order to foster a meaningful exchange of information on criminal matters.

ORGANISATIONAL STRUCTURE

The criminal intelligence function is a separate and distinct activity that requires special consideration when positioning it within an agency's organisational structure.

Depending on the size of the unit, the criminal intelligence officer, supervisor or unit manager, needs direct access to the chief executive officer. This direct access is imperative since the unit's primary function is to provide the chief executive officer (CEO) with timely strategic intelligence that will allow for appropriate planning to meet developing criminal trends. Members of the organisation must recognise the need for the intelligence officer to report directly to the CEO. This reporting procedure, which circumvents the normal chain of command, is used to eliminate communication filters and to ensure the confidentiality of criminal intelligence information.

Ideally, the criminal intelligence unit should be located in its own secure office with appropriate equipment. It should not be combined with other investigative units such as narcotics, vice, detectives, or internal affairs. Intelligence differs considerably from investigations, and it is important to understand why these legitimate law enforcement functions must be treated differently.

Basically, criminal intelligence is a proactive effort designed to prevent crime by providing the CEO with knowledge of criminal events that may occur in his or her jurisdiction. If performed properly, this allows the CEO time to make decisions to counter potential criminal activity. Frequently, the criminal intelligence process involves 'soft' information, which cannot be used in court. 'Soft' information can include hearsay information from rumours, suggestions, and beliefs for the building of files. In collecting initial raw data, intelligence officers often go to sources that investigators would seldom consider for their investigative needs. In addition to surveillance observations and materials selected from public databases, intelligence officers may note anonymous comments about people who they believe may be planning a crime or listen to others they feel might be in a position to know. Their specialty is the nurturing of this type of soft data into refined and useful criminal intelligence.

This type of information collection involves careful evaluation and analysis and requires that the needs of law enforcement are balanced against the individual's right to privacy. This right requires that the dissemination of criminal intelligence information be treated carefully and in conjunction with established 'right-to-know' and 'need-to-know' standards. As a result, intelligence files require a high level of security. This level of protection is greater than that required for most other law enforcement files.

On the other hand, the investigation of specific crimes is strictly reactive functions designed to arrest and prosecute the involved suspect or suspects. This effort is directed toward identifying suspects and witnesses, recovering stolen property and contraband, and procuring viable evidence for use in court. Its focus is toward 'hard' or provable information, which is designed for court purposes.

The difference between the two disciplines is significant. Intelligence files need to be kept in a separate location from investigative files and the functions needs to be assigned to different units. This separation will help to ensure that professional standards are maintained in each area of expertise.

AGENCY SUPPORT

Agency support of the intelligence effort is crucial to a successful program. That support must encompass all personnel from the chief executive to the line officers. The necessary support can be obtained once staff understands the objectives of the program, and how they can assist with the effort.

Frequently, the perception of the criminal intelligence unit has been a problem with some agencies. In some instances, the intelligence mission is not clear to those outside the unit. The function, role, objectives, and the mission of the unit need to be shared with others in the organisation. The established guidelines for the release of information from the unit and the modification of the traditional chain of command should be explained to avoid misconceptions that a 'secret squad' exists. Some of the mystery concerning

intelligence is stripped away once the process is explained and the legal aspect of privacy rights and need for confidentiality is recognised. Most informed employees will subsequently accept the manner in which intelligence must operate and will assist in the effort.

UNIT MISSION

Determining the criminal intelligence unit's mission is another important concern. The criminal intelligence function, like other specialised law enforcement assignments, requires appropriate direction and focus. Specific parameters are necessary so that the criminal intelligence effort will not lose its perspective and will retain its ability to consistently deliver a useful product. Mission statements help provide that direction. They should indicate the agency's expectations of its criminal intelligence unit so that unit personnel, as well as the rest of the agency, understand the function.

Mission statements should address three different components:

1. The first portion of the mission statement should describe the criminal intelligence process of collecting, evaluating, collating, analysing and disseminating information related to criminal activities.

2. The second component of the mission statement requires the agency to identify the type or scope of criminal activity that the criminal intelligence unit will be addressing. In crafting this portion of the statement, it is important to determine what crime problems or issues are threatening the concerned jurisdiction. Each community or area has its own unique challenges and the mission statement should reflect those issues. For example, if a jurisdiction's prevailing crime problem involves Criminal Street gangs or 'emerging organised crime groups', then the mission statement should identify those concerns as the unit's focus.

   In determining the focus of the criminal intelligence unit, it is also important to identify an objective that can realistically be accomplished by the personnel and resources assigned to the unit. It is counter productive to the unit to design the mission in such broad terms that the assigned personnel cannot adequately perform the job.

3. The final portion of the mission statement should describe the results that are expected to be obtained by the unit. If the primary function of the criminal intelligence unit is to provide strategic intelligence to the chief executive officer, this portion of the mission statement should indicate that the information provided will allow the CEO to make rational choices regarding unanticipated criminal threats and the deployment of the agency's resources.

The following is a sample mission statement:

"The Department's Criminal Intelligence Unit will collect, evaluate, collate, analyse and disseminate information on individuals and groups who are suspected of being involved in (criminal problems of concern to the jurisdiction) and will provide this information to the Chief Executive Officer for crime prevention and decision making purposes."

TRAINING

State of the art training in criminal intelligence is available and should be made available for members of the agency. In order to maximize the benefits to be derived from a criminal intelligence unit, the department's training commitment should start with the chief executive officer. The CEO needs to understand how the unit operates and what it can produce. Of particular interest for the CEO is how strategic intelligence products can help the agency prevent crime, properly allocate resources and budget for emerging crime problems. The agency's managers and supervisors must also understand the concept of intelligence and how it can help reduce crime. Their support will greatly enhance the coordination of the collection effort.

Line personnel are a significant resource for the intelligence unit. They must understand that they are the eyes and ears of the agency. They are present in the community 24 hours a day, 7 days a week interacting with individuals and observing activities. It is critical that they understand their ability to contribute to the intelligence effort. In return, intelligence personnel should provide them with tactical information that will help keep them safe and assist them in recognizing threats in the community. Patrol personnel also need to understand the legal issue of individual privacy rights and the reason dissemination rules are so stringent. Proper training of line personnel will assist them in understanding the strategic need for the intelligence unit's close relationship to the CEO.

It is important that the city manager or county administrator be advised of the presence and purpose of the criminal intelligence function. These administrators are ultimately responsible to the community for the services of their governments and must be fully aware of the crime prevention aspects of the unit and the legal constraints within which its works.

Training the agency's legal advisor prior to any legal issues arising also has its benefits. It provides an opportunity for the attorneys to understand the unit's policies, procedures, and the legal constraints with which the intelligence unit must operate. Although legal actions against criminal intelligence units have drastically diminished in recent years, the unit's legal advisor needs to be cognisant of the unit's operational guidelines prior to receiving subpoenas or lawsuits.

MANAGING THE PROCESS

Criminal intelligence units require proper direction, appropriate guidelines and consistent oversight. The traditional five-step intelligence process of collection, evaluation, collation, analysis and dissemination will not prove valuable for an agency unless ongoing and effective direction and coordination exists throughout the five step process. The objective of the process is to provide both strategic and tactical products for the agency.

The management, supervision and direction of a criminal intelligence unit will differ according to the size and composition of the unit. In every case, however, the direction of the intelligence effort is critical. Every intelligence project requires a focus. That focus and specific direction has to be of value to the agency. Many agencies have collected volumes of criminal intelligence information that has never been put to use. This obviously filled file cabinets and computer space but failed to provide a useful product for the agency. Properly identifying targets can resolve this issue and provide useful products to help ensure the safety of the community.

Effective direction starts with the CEO providing general guidance and broad objectives. The unit manager will subsequently select the targets or identify the specific goals. Once a specific intelligence project is identified, the methods and procedures for the collection of information must be considered and implemented. This collection plan is often the Achilles heel of the process. If a proper plan is not devised and carried out, then the objective is frequently not obtained.

Criminal intelligence personnel can be deployed in a number of different ways depending upon the project. Intelligence personnel can be assigned by criminal subject, criminal organisation, geographic area, ethnic organised crime type or by criminal activity. This decision usually depends on the type of specific information gathering effort being undertaken.

Once a criminal intelligence project is initiated, the manager needs to meet with his staff to determine what methods and resources will be used to obtain the required information. Data can be gathered through or from surveillance, undercover operatives, data banks, criminal informants and law enforcement or citizen sources. A method that should not be ignored is the use of overt intelligence personnel being assigned to monitor known criminal subjects. Once the habits of these suspects are established, intelligence officers can create appropriate opportunities to interview or converse with the criminal suspects in public places. This type of contact can be very effective. Many times, criminal subjects will willingly converse with police investigators in public. Even those subjects who will not voluntarily speak with known intelligence officers

can be influenced by observing intelligence officers in public locations where the suspect expects to conduct either social or business meetings with criminal associates. The psychological impact of this type of contact in restaurants, bars, hotels and other public places will generally impede the suspect's activity and, undoubtedly, make them concerned that the officers are aware of their criminal intentions.

In addition to specific intelligence projects that are undertaken by the unit, regular sources of information must be cultivated and established by the unit to keep abreast of criminal activities within the jurisdiction. This stream of information would include the review of selected crime and arrest reports, newspaper articles, search warrants, special publications and items from law enforcement contacts or community sources.

All of this raw data must subsequently be reviewed and evaluated for mission relatedness and, if deemed appropriate, considered for file input. "The unit commander must establish an effective filing system. It should be one that minimises clerical work to the greatest extent possible while providing the analyst with an effective tool. A second major requirement for the filing system is that retrieval of information be easy. Finally, the system must be as simple as possible to enhance accuracy of filing so that... there is assurance that all information relative to a particular subject is made available."

"In order to provide guidance, and at the same time ensure the legality of files, the unit commander must develop specific guidelines that determine what material can be entered into the files, how it is to be organised, and finally how information that is no longer deemed essential is to be purged from the files ".

The analysis step has been accurately described as the 'heart' of the intelligence process. Without this part of the process the agency will not be able to extract a viable return from the collected data. This step of the process involves the need for management to ensure there is ongoing communication between the analysts and the data collectors. Their efforts need to be coordinated to ensure that appropriate data is available to the analyst for their respective projects.

The last step in the process involves the dissemination of the intelligence product. The consumers include the CEO, the agency and other law enforcement agencies. The unit manager needs to ensure that dissemination rules of 'need to know', 'right to know' and the third-party rule (no original document that has been obtained from an outside agency is to be released to a third agency) are followed. Additionally, appropriate guidelines need to be in place for release approval and to document the requests and release of information to consumers. "The unit commander must decide how the unit is to disseminate its output. In all cases, the intelligence unit should adopt an affirmative program, disseminating information and output as widely as possible within the constraints of sensitivity of information. An intelligence file that is not used is worthless".

Every intelligence unit should be evaluated on a regular basis. The unit manager should ensure that the unit is meeting its stated objectives. An informal evaluation should ask the following questions:

1. Is the unit staying within its guidelines?
2. Is the unit focused on its defined mission?
3. Is unit training needed?
4. Is the unit meeting its objectives?
5. Is it producing analytical products?
6. Does the unit provide the agency with both tactical and strategic products?
7. Are the unit's products valuable to the agency?

SUPERVISION

One of the keys to proper supervision is ensuring that all members are aware of the unit's objectives and focused on their individual roles. This requires ongoing communication among members of the unit. Frequent meetings are necessary so that a team effort is established in reaching unit objectives.

The unit as a whole needs to know the targets, the ongoing activities of the unit and the information needs being sought. This sharing of information and ideas for obtaining essential data is necessary as tenured intelligence officers tend to have a variety of sources from which to access items of information. Close coordination between the field collectors and the analysts must occur so that an accurate and complete picture of the criminal issue is developed.

Clear and concise unit guidelines are essential for the smooth and efficient operation of an intelligence unit. Assigned personnel need to understand the rules and procedures under which they must operate. The guidelines for unit operations should address issues, such as policy; mission; responsibilities; reporting procedures; file criteria and maintenance; information evaluation and classification; purge procedures; and dissemination. Additional guidelines must exist for the use of informants, unit security and the use of special funds. "The unit commander is also responsible for establishing guidelines that will inform investigators of targets they may cover and under what conditions... the commander then has the follow-on task of insuring that the investigators, in fact, observe the guidelines."

STAFFING

The unit manager should keep in mind that criminal intelligence personnel must possess a wide range of abilities to ensure their success in this assignment. Some of the more obvious include integrity; high intellectual capacity and analytical ability; initiative; and the ability to communicate effectively, both verbally and in writing. Another consideration is the ability to establish rapport with diverse individuals, from law enforcement personnel to the various members of the community. This ability is crucial and will ultimately determine an officer's capability to obtain information from a wide range of sources. Other important characteristics are an officer's judgment and his ability to anticipate what may occur in any given situation. Obviously, there are many individual skills to consider, but the success of the unit ultimately will depend on the talents of the assigned personnel.

The rotation of personnel is a subject that many CEOs feel is important in today's management environment. The argument in favour of a regular rotation of assignments relates primarily to the prevention of corruption in sensitive positions and to providing agency personnel a wider range of knowledge and experience. While rotation may be appropriate for many, if not most, assignments within a law enforcement agency, criminal intelligence is a specialty assignment that should not be rotated on a routine basis. The primary reasons for this perspective include the length of time it takes for an intelligence officer to learn the assignment and be effective, the skill development and training investment required, and the law enforcement contacts and other valuable contacts that have to be established. For these reasons, any rotation of intelligence personnel should be based on an evaluation of the quantity and quality of the intelligence products received from the assigned individual.

LIAISON

An ongoing need exists for the sharing and coordination of criminal information between law enforcement agencies at all levels of government. In many instances, pertinent criminal intelligence data relating to one's own agency is first obtained from adjacent agencies. This sharing of data on a regular basis allows for a more comprehensive review of criminal activities, which impact more than one jurisdiction. Local agencies should be networking on a regional basis and on a regular schedule. Pertinent information should also be shared with state and federal authorities. It is recommended that all intelligence units have membership in the Regional Information Sharing System (RISS) and the Law Enforcement Intelligence Unit (LEIU). Professional investigative associations also offer valuable contacts and training opportunities.

SUMMARY

The 21st century has arrived, and it is appropriate that law enforcement recognise criminal intelligence as the 'Ultimate Management Tool for Law Enforcement'. Crime prevention and suppression is law enforcement's business, and the criminal intelligence function allows police agencies to be proactive in addressing the criminal threats in our communities. As a critical component of Community-Oriented Policing, criminal intelligence needs to be the approach that police agencies embrace to achieve an optimum level of public safety.

10 STEPS TO ESTABLISHING A SUCCESSFUL CRIMINAL INTELLIGENCE PROGRAM

1. Create a proper environment.
    - Obtain the active support of the agency's chief executive officer.
    - Gain the political and budgetary support from the appropriate elected officials.
    - Educate the agency and the community concerning the benefits of having a criminal intelligence function.

2. Establish the criminal intelligence unit as a proactive crime prevention operation, which supports the concept of community oriented policing.

3. Design unit mission statements focused toward specific criminal activities and disseminate it to the entire agency.

4. Select qualified personnel, including at least one trained analyst, to staff the unit.

5. Obtain separate, secure quarters for the unit.

6. Implement and enforce professional guidelines for:
    - Unit operations
    - File procedures
    - Security
    - Special expense funds
    - Informant control

7. Provide training for:
    - The chief executive officer
    - Appropriate elected officials
    - Criminal intelligence managers and supervisors
    - Criminal intelligence officers and analysts
    - The remainder of the agency's personnel
    - Legal advisor

8. Liaison with neighbouring agencies and participate in regional and state criminal intelligence networks. Join The Regional Information Sharing System (RISS) and the Law Enforcement Intelligence Unit (LEIU).

9. Require both strategic and tactical products from the unit and evaluate its operations on a regular schedule.

10. Ensure the chief executive officer meets regularly with the criminal intelligence unit supervisor to provide appropriate direction.

Chapter IX

9. STANDARDS AND GUIDELINES

COMMISSION FOR THE ACCREDITATION OF LAW ENFORCEMENT AGENCIES

THE STANDARDS MANUAL OF THE LAW ENFORCEMENT AGENCY ACCREDITATION

Criminal intelligence

As intelligence relates to law enforcement agencies, it is principally concerned with collecting, processing, and disseminating information relating to specified crimes and criminal activities. These areas of concern vary widely among law enforcement jurisdictions but typically include organised crime, vice, illegal drug trafficking, terrorism, gangs, and civil disorders. Ordinarily, the intelligence function should not perform enforcement activities but should be a source of information for operational units. While some agencies my separate the function, others may assign it to the criminal investigations function as an added responsibility.

The standards in this chapter address the basic concerns of a law enforcement agency in carrying out the intelligence function. The standards do not include the intelligence gathering activities associated with special events, such as visits by dignitaries or sporting events. Nothing in this chapter should be interpreted as permitting the collection of data for political or other purposes unrelated to crime.

Administration

If the agency performs an intelligence function, procedures must be established to ensure the legality and integrity of its operations, to include:

a) procedures for ensuring information collected is limited to criminal conduct and relates to activities that present a threat to the community;
b) descriptions of the types or quality of information that may be included in the system;
c) methods for purging out-of-date or incorrect information;
d) procedures for the utilisation of intelligence personnel and techniques.

Commentary: The intent of this standard is to establish agency accountability for the criminal intelligence function in writing. Proving compliance with this standard may be accomplished through a series of documents or a single, all-inclusive directive.

For this standard, the agency has several options. First, this function may be an extension of the criminal investigation function. In this case, functional responsibility and position accountability can simply be described in the C.I.D. directive (s). On the other hand, the agency may wish to assign this function with its vice, drug and / or organised crime control function(s). In this case the description of functional responsibility may be addressed within those directives. The placement of this function within the organisational structure is optional but carries with it the responsibility for complying with the standards.

Intelligence activities are important in all agencies, regardless of size. Certain essential activities should be accomplished by an intelligence function, to include a procedure that permits the continuous flow of raw data into a central point from all sources; a secure records system in which evaluated data are properly cross-referenced to reflect relationships and to ensure complete and rapid retrieval; a system of analysis capable of developing intelligence from both the records system and other data sources ; and a system for dissemination of information to appropriate components. The intelligence activities should include information gathering, analysis, and dissemination to the appropriate functions / components. Activities undertaken in the intelligence effort should avoid indiscriminate collection or distribution of information.

Training in the safe, effective and legal use of specialised intelligence equipment is required prior to personnel using the equipment. All use should be carefully documented. This equipment may include audio and / or visual monitoring equipment, night vision equipment, and specially designed surveillance vehicles.

If the agency maintains a confidential fund for intelligence activities, control and management of the fund should comply with all applicable standards.

A written directive governs procedures for the safeguarding of intelligence information and the secure storage of intelligence records separate from all other records.

Commentary: Intelligence information should be distributed only to criminal justice agencies and on a need-to-know basis. Intelligence information should be collated and analysed in a secure environment. If a computer is used for intelligence purposes, there should be a secure system that protects against unauthorised attempts to access modify, remove, or destroy stored information.

The highly sensitive nature of intelligence files requires that they be maintained separately from other agency records to prevent compromise and protect the integrity of the system. If the intelligence function is performed by an individual with other responsibilities (CEO, deputy chief or as an activity of a larger function (criminal investigations), the separation and security intentions of this standard should still apply.

INTERNATIONAL ASSOCIATION OF CHIEFS OF POLICE NATIONAL LAW ENFORCEMENT POLICY CENTRE - CRIMINAL INTELLIGENCE

I. Purpose

It is the purpose of this policy to provide law enforcement officers in general, and officers assigned to the intelligence function in particular, with guidelines and principles for the collection, analysis, and distribution of intelligence information.

II. Policy

Information gathering is a fundamental and essential element in the all-encompassing duties of any law enforcement agency. When acquired, information is used to prevent crime, pursue and apprehend offenders and obtain evidence necessary for conviction. It is the policy of this agency to gather information directed toward specific individuals or organisations reasonably suspected of criminal activity, to gather it with due respect for the rights of those involved, and to disseminate it only to authorized individuals as defined. While criminal intelligence may be assigned to specific personnel within the agency, all members of this agency are responsible for reporting information that may help identify criminal conspirators and perpetrators.

III. Definitions

Criminal Intelligence: Information compiled, analysed and / or disseminated in an effort to anticipate, prevent, or monitor criminal activity.
Strategic Intelligence: Information concerning existing patterns or emerging trends of criminal activity designed to assist in criminal apprehension and crime control strategies, for both short-and long-term investigative goals.
Tactical Intelligence: Information regarding a specific criminal event that can be used immediately by operational units to further a criminal investigation, plan tactical operations and provide for officer safety.

IV. Procedures

1. Mission

It is the mission of the intelligence function to gather information from all sources in a manner consistent with the law in support of efforts to provide tactical or strategic information on the existence, identities, and capabilities of criminal suspects and enterprises generally and, in particular, to further crime prevention and enforcement objectives / priorities identified by this agency.

- Information gathering in support of the intelligence function is the responsibility of each member of this agency although specific assignments may be made as deemed necessary by the officer-in-charge (OIC) of the intelligence authority.
- Information that implicates, suggests implication or complicity of any public official in criminal activity or corruption shall be immediately reported to this agency's chief executive officer or another appropriate agency.

2. Organisation

Primary responsibility for the direction of intelligence operations; coordination of personnel; and collection, evaluation, collation, analysis, and dissemination of intelligence information is housed in this agency's intelligence authority under direction of the intelligence OIC.

- The OIC shall report directly to this agency's chief executive officer or his designate in a manner and on a schedule prescribed by the chief.
- To accomplish the goals of the intelligence function and conduct routine operations in an efficient and effective manner, the OIC shall ensure compliance with the police, procedures, mission, and goals of the agency.

3. Professional Standards

The intelligence function is often confronted with the need to balance information-gathering requirements for law enforcement with the rights of individuals. To this end, members of this agency shall adhere to the following:

- Information gathering for intelligence purposes shall be premised on circumstances that provide a reasonable indication that a crime has been committed or is being planned.
- Investigative techniques employed shall be lawful and only so intrusive as to gather sufficient information to prevent the criminal act and / or to identify and prosecute violators.
- The intelligence function shall make every effort to ensure that information added to the criminal intelligence base is relevant to a current or on-going investigation and the product of dependable and trustworthy sources of information. A record shall be kept of the source of all information received and maintained by the intelligence function.
- Information gathered and maintained by this agency for intelligence purposes may be disseminated only to appropriate persons for legitimate law enforcement purposes in accordance with law and procedures established by this agency. A record shall be kept regarding the dissemination of all such information to persons within this or another law enforcement agency.

4. Compiling Intelligence

- Intelligence investigations / files may be opened by the intelligence OIC with sufficient information and justification. This includes but is not limited to the following types of information:

a) subject, victim(s) and complainant as appropriate
b) summary of suspected criminal activity
c) anticipated investigative steps to include proposed use of informants, photographic, or electronic surveillance
d) resource requirements, including personnel, equipment, buy/flash monies, travel costs, etc

e) anticipated results
f) problems, restraints or conflicts of interest:

- Officers shall not retain official intelligence documentation for personal reference or other purposes but shall submit such reports and information directly to the intelligence authority.
- Information gathering using confidential informants as well as electronic, photographic, and related surveillance devices shall be performed in a legally accepted manner and in accordance with procedures established for their use by this agency.
- All information designated for use by the intelligence authority shall be submitted on the designated report form and reviewed by the officer's immediate supervisor prior to submission.

5. Receipt / Evaluation of Information

Upon receipt of information in any form, the OIC shall ensure that the following steps are taken:

- Where possible, information shall be evaluated with respect to reliability of source and validity of content. While evaluation may not be precise, this assessment must be made to the degree possible in order to guide others in using the information. A record shall be kept of the source of all information where known.
- Reports and other investigative material and information received by this agency shall remain the property of the originating agency, but may be retained by this agency. Such reports and other investigative material and information shall be maintained in confidence, and no access shall be given to another agency except with the consent of the originating agency.
- Information having relevance to active cases or that requires immediate attention shall be forwarded to responsible investigative or other personnel as soon as possible.
- Analytic material shall be compiled and provided to authorized sources as soon as possible where meaningful trends, patterns, methods, characteristics or intentions of criminal enterprises or figures emerge.

6. File Status

Intelligence file status will be classified as either 'open' or 'closed', in accordance with the following:

- *Open* intelligence files are those that are actively being worked. In order to remain open, officers working such cases must file intelligence status reports covering case developments at least every 180 days.
- *Closed* intelligence files are those in which investigations have been completed, where all logical leads have been exhausted, or where no legitimate law enforcement interest is served. All closed files must include a final case summary report prepared by or with the authorisation of the lead investigator.

7. Classification/Security of Intelligence

- Intelligence files will be classified in order to protect sources, investigations, and individual's rights to privacy, as well as to provide a structure that will enable this agency to control access to intelligence. These classifications shall be re-evaluated whenever new information is added to an existing intelligence file.

a) *Restricted* intelligence files include those that contain information that could adversely effect an ongoing investigation, create safety hazards for officers, informants or others and / or compromise their identities. Restricted intelligence may only be released by approval of the intelligence OIC or the agency chief executive to authorised law enforcement agencies with a need and a right to know.
b) *Confidential* intelligence is less sensitive than restricted intelligence. It may be released to agency personnel when a need and a right to know have been established by the intelligence OIC or his designee.

c) Unclassified intelligence contains information from the news media, public records, and other sources of a topical nature. Access is limited to officers conducting authorised investigations that necessitate this information.

- All restricted and confidential files shall be secured, and access to all intelligence information shall be controlled and recorded by procedures established by the intelligence OIC.

a) Informant files shall be maintained separately form intelligence files.
b) Intelligence files shall be maintained in accordance with state and federal law.
c) Release of intelligence information in general and electronic surveillance information and photographic intelligence, in particular, to any authorised law enforcement agency shall be made only with the express approval of the intelligence OIC and with the stipulation that such intelligence not be duplicated or otherwise disseminated without the approval of this agency's OIC.
d) All files released under freedom of information provisions or through disclosure shall be carefully reviewed.

8. Auditing and Purging Files

- The OIC is responsible for ensuring that files are maintained in accordance with the goals and objectives of the intelligence authority and include information that is both timely and relevant. To that end, all intelligence files shall be audited and purged on an annual basis as established by the agency OIC through an independent auditor.
- When a file has no further information value and / or meets the criteria of any applicable law, it shall be destroyed. As record of purged files shall be maintained by the intelligence authority.

SUGGESTED CRIMINAL INTELLIGENCE STANDARDS AND GUIDELINES

Every local and state enforcement agency engaged in the collection, retention, and dissemination of intelligence-related information should consider implementing the following standards and guidelines.

1. Standard - Every agency should implement a mission statement dictating the existence and function of its intelligence operations program.

Guidelines - The mission statement should contain a concise, well-defined mandate describing the program; the use of the intelligence process in support of the program; and the programs expected results. The statement should clearly delineate the program's focus on specific criminal activities and emphasise the use of intelligence as a crime prevention tool dedicated to the concept of community-oriented policing. The statement should specify the programs primary function is to help the agency's chief executive officer (CEO) make rational choices regarding unanticipated criminal threats and the deployment of resources in response to those threats. At the very least, the statement should contain the following:

Sample Mission Statement

The Department's Intelligence Operations Program will collect and analyse information on individuals and groups suspected of being—or known to be—involved in the following
Criminal activities: , , , , , and
provide this information to the CEO for crime prevention and decision-making purposes.

2. Standard - Every agency should recognise that active management and supervision of the criminal intelligence function are necessary to provide appropriate direction and control, staffing, and logistical support.

Guidelines - Management and supervision of an intelligence operations program are responsible for providing proper direction, guidelines and procedures, staffing, equipment, training, and direct access to the agency CEO.

3. Standard - Every agency should implement a policy and procedures manual detailing its intelligence operations program, mission, methods of operation, file guidelines, and security procedures.

Guidelines - The manual should depict the program's operational policy and procedures; protocol for creating an intelligence-related record on a subject; entering the record into a file and / or database; and / or opening an investigation on a subject. The protocol should be based on the subject's involvement, or suspected involvement, in the specific criminal activities focused upon the agency's mission statement. A criminal predicate is required for all file entries.

4. Standard - Every agency should implement a set of guidelines that regulate the contents of its intelligence-related file.

Guidelines - The guidelines should conform to state and federal regulations and prescribe the criteria for the retention and purge of intelligence-related records contained in file. The information must be evaluated for its validity and the source assessed for reliability. Access to the information should be restricted to protect the source, investigation, and a subject's right to privacy.

5. Standard - Every agency should implement a process for systematically exploiting intelligence-related information that is intended to prevent and reduce crime.

Guidelines - That exploitation should consist of the following intelligence process:

- *Collection* - A planned effort focused on obtaining information identifying suspected or known criminal activity that impacts the jurisdiction.
- *Evaluation* - A determination regarding the validity of obtained information and an assessment of the reliability of the source.
- *Collation* - An orderly arrangement of information that systematically connects elated activities in the file.
- *Analysis* - Conversion of information and intelligence that results in useful knowledge and appropriate recommendations to the CEO and the agency.
- *Dissemination* - The intelligence product is provided to personnel who have a 'need to know' and a 'right to know'.

6. Standard - Every agency should implement appropriate training for all personnel assigned to, impacted by, or overseeing the intelligence operations program.

Guidelines - Personnel assigned to the agency's intelligence operations program should be trained in all aspects of the intelligence process, along with the guidelines and liability issues pertaining to the collection, retention and dissemination of intelligence-related information. An understanding of intelligence, how it works and why it is important with a distinction between intelligence and information should be part of the training foundation. The training should emphasise analysis and clearly explain the terminology and definitions pertaining to intelligence. The agency's CEO, the rest of the agency's personnel, the agency's legal advisor, and appropriate elected and public officials should also be trained or briefed in the intelligence process and the role it plays in the agency's community-oriented policing program.

7. Standard - Every agency should provide the intelligence operations program with secure quarters and allow the program to be a separate entity within the law enforcement agency.

Guidelines - Criminal intelligence is a pro-active crime prevention function that operates differently than an enforcement unit. It frequently deals with sensitive information obtained from diverse sources with various levels of credibility. This information must be handled differently than routine investigative information. The intelligence process involves evaluation and analysis and requires that the needs of law enforcement are balanced against the individual's right to privacy. The dissemination of this intelligence must be in

conjunction with established "right to know" and "need to know" standards. These requirements support the need to assign the intelligence function to a separate unit and to maintain the intelligence file in a secure location.

8. Standard - Every agency should implement security precautions for their intelligence-related database and information.

Guidelines - A directive should be written to govern the security precautions of the agency's intelligence database and to protect the confidential storage of information in that database. The directive should also declare the files retained by the intelligence operations program are kept separate from the agency's other files.

9. Standard - Every agency should hold the intelligence operations program accountable for producing both strategic and tactical products and for maintaining appropriate liaison with local, state, and federal law enforcement agencies.

Guidelines - The CEO should expect a high level of accountability from personnel assigned to the intelligence operations program and require both tactical and strategic products on a regular basis. The CEO should require the program to liaison with neighbouring agencies and participate in regional and state networks so information of mutual interest can be shared and exchanged.

10. Standard - Every agency should implement a procedure for evaluating the effectiveness of its intelligence operations program.

Guidelines - Objectives should be established by an agency so the management and operations of the intelligence program can be evaluated on a regular schedule.

11. Standard - Every CEO with a criminal intelligence function should actively champion it and describe it as a pro-active crime prevention tool that supports community oriented policing.

Guidelines - The CEO should actively support the intelligence operations program and ensure it receives the political and budgetary commitment it deserves. The support should extend to obtaining community support for this pro-active law enforcement effort at preventing crime.

Appendix I EVALUATIONS

1. POSSIBLE QUESTIONS TO BE INCLUDED IN COMPLIANCE AUDITS / SURVEYS FOR INTELLIGENCE UNITS - PAUL ROGER

Personnel Security

- What personnel security vetting procedures exist in respect of personnel working within the intelligence area?
- Are periodic security updates conducted for intelligence personnel on a regularly basis?
- Are guidelines in place for disclosure by members should their personal circumstances change?
- What measures are taken by the intelligence unit and its personnel to guard against subversion[3] or other risks to the intelligence unit?

Physical Security

- Is the intelligence unit physically secured? (If yes, how?)
- Does the security prevent access by unauthorised persons?
- Is access and egress of authorised personnel monitored and recorded?
- Is access ability terminated when personnel are on leave or cease to work in the intelligence unit?
- Are there guidelines on staff taking intelligence material home or out of the building?
- Are there guidelines for transferring material to or from floppy disks?

Capture of Intelligence Material

- Do you have a data capture plan? (Attach copy of relevant documents)
- Does this plan detail procedures / guidelines that govern what intelligence is to be collected and the methods for collection? (Attach copy of relevant documents)
- What procedures are practiced to ensure that only designated data is captured and entered onto the intelligence database?
- Who is responsible for collecting data?
- Who is responsible for ensuring correct procedures are followed in respect of collection?

Storage of Intelligence Material

Hard Copy Storage

- What procedures are in place to govern the storage, handling and security of hard copy source material? (Give details or attach copies of relevant documents.)
- Do you retain hard copy source documents regarding intelligence information?
- Where are they stored?
- Who has access to these documents?
- How is access controlled?

[3] In the context of personnel security, subversion is the altering of a person's loyalties, or changing a person's moral standards, by the application of some form of coercion. This coercion normally takes the form of bribery, blackmail, psychological pressure or physical threats. Subversion, as a general threat, is best countered by education of staff as to methods, thus allowing individuals to recognize and counter it.

Electronic Storage

- Are there guidelines for recording intelligence material on electronic (IT) systems? (Give details or attach copies of documents.)
- Are there adequate access checks and scrutiny, e.g. passwords, etc How often are passwords changed?
- Is facility access deleted when personnel are on leave or cease to work in the intelligence unit?
- Is the IT system capable of producing an audit trail for any system interrogation?
- Is access graded on a 'need to access' basis?
- Are files adequately safeguarded through back-up and recovery routines, and off-site storage of critical files, programs and systems?
- Is the IT system isolated from other networks and, if not, are appropriate 'firewalls' in place?

Integrity of Intelligence Material

Quality Control

- What quality control procedures are in place to ensure quality of data is maintained?
- In respect of electronic databases, what procedures are in place to ensure quality of data?
- Is there a clear responsibility in a particular position for the continued development, maintenance and implementation of quality control systems?

Culling and Destruction

- Do you have procedures for the culling and destruction of intelligence material?
- What criterion is used during the culling process?
- Who is responsible for culling and the subsequent destruction?
- Are staff aware of any relevant Archive or related legislation?
- When hard copy material is culled, is corresponding electronic data also culled? (If yes, who is responsible for culling electronic data?)
- Are records maintained of culling and destruction exercises? (If yes, are they available for inspection?)

Availability of Intelligence Material

Access

- What electronic databases are maintained that contain intelligence material?
- Who has access to these databases?
- What levels of access do officers possess (e.g. read / write etc.)?
- Who is responsible for controlling access?
- Who audits access?
- How often are audits conducted?
- How are audits performed (e.g. reactively, proactively, regularly, randomly etc.)?
- What records are maintained in respect of audits of access?
- Is access immediately deleted when personnel leave or transfer?
- Are regular reviews undertaken to determine the continued necessity for current personnel to have intelligence system access?

Dissemination of Intelligence Material

At Own Initiative

- Are there procedures covering the dissemination of intelligence material? (If yes, attach procedures.)

- Who may authorize dissemination of intelligence material?
- What records are kept of dissemination of intelligence material?
- Are these records audited?
- If audits are conducted, who by?
- Are records kept of such audits for inspection purposes?

Responses to Requests

- Do you have procedures that govern the way intelligence personnel will respond to a request for information? (If yes, attach procedures.)
- What criterion is used in reaching a decision regarding the need and right of the requesting person to receive information?
- What records are kept of requests and responses?
- Are these records audited?
- If yes, by whom and how frequently?
- Are records kept of such audits?

Transmission of Material

- Do you have procedures which govern the methods of enveloping, dispatching and recording of such dispatch of classified material from the intelligence unit? (If yes, attach procedures.)
- What methods of dispatch are used for intelligence documents dispatched from your unit (e.g. courier, safe hand, internal dispatches, postal services etc.)?
- What criterion is used in reaching a decision as to which method of dispatch to use?
- Are there appropriate mechanisms in place to identify the non-receipt of classified material? (If yes, attach procedures.)

Accountability and Management of System

Responsibilities

- Is there regular assessment of the purposes and goals of the intelligence system and an evaluation of the extent and effectiveness of the achievement of these goals?
- Are there clear lines of responsibility and accountability for the functions of the intelligence unit?
- Are individual responsibility statements regularly reviewed and updated?
- Are there adequate resources to meet the responsibilities in a practical way?
- Is a regular Security Risk Review of the intelligence unit and its systems carried out?
- Are managers and those responsible for the effective operation of the intelligence system adequately trained and kept up to date in the required operation of the system?
- Are delegations and authority limits regularly reviewed?

Awareness

- Are staff generally aware of the security and privacy implications of the intelligence function and the collection and storage of intelligence material?
- Is there an adequate system to ensure any amendments or updates to procedures are read and understood?
- Are staff aware of actions they should take and procedures to follow should they encounter any departures from approved policy and procedures in the operation of the intelligence system?
- Does unit management clearly demonstrate that it insists on the highest standards of ethical and professional behaviour?

2. NUMERIC INTELLIGENCE EVALUATION SYSTEM FROM HARRIS (1976:134-138)

This approach is based on an evaluation in terms of questions relating to the major elements of the functions within the intelligence process. On the basis that each function is essential to the process, each is assigned a value of 100 as follows:

Collection / flow of information	100
Processing / collation of information	100
Analysis	100
Production / dissemination of information	100
Management procedures	100

Points are then assigned based on the following breakdown of each function.

a. Collection

1	Intelligence unit receives as part of normal flow of information, copies of all (the bulk of) investigator reports (except in large units where reports relating to known or suspected persons associated with organized crime and major criminal activity would be sufficient).	30
2	Intelligence unit has its own investigators or can task the department's investigative unit to probe areas determined to be important as a result of the intelligence unit's assessment. A procedure exists for the tasking of non-intelligence unit personnel on the basis of agreement between the intelligence and operational unit commanders or orders of the department chief.	25
3	Department has an effective procedure operating whereby the officer on patrol can report on specified subjects directly to the intelligence unit.	20
4	Intelligence unit receives (or at least records information contained in) sensitive reports from undercover units, informants, or other specialized sources.	15
5	Intelligence unit has a plan of action to gain information from other law enforcement agencies—local in area, state, and federal.	10
	Total	100

b. Processing/Collation

1	Information, once filed, can be quickly and correctly retrieved	30
2	The information filing system has a capability to focus data received by major crime figures, area/location, type of crime, and other subjects the analysts find useful.	30
3	Unit has an information flow system that causes reports to be reviewed distributed, and earmarked for filing in a manner that ensures the analysts (or other persons responsible for performing analyst functions) reads important reports relating to his/her area of responsibility.	25
4	There is an efficient and effective operating system for updating biographies (abstracts or biographic forms) of known or suspected major criminals in the area (not necessarily restricted to persons residing within the boundaries of the jurisdiction).	25
5	There is an operational plan for purging the files of outdated and non- pertinent material.	10
	Total	100

c. Analysis

1	The intelligence unit has one or more persons tasked to analyse information received to develop / project / estimate: - patterns of organized crime by type of crime; - patterns of association among persons believed to be part of organized crime; - interrelationships among criminals and types of organized crimes in which they are suspected of being involved.	50
2	The intelligence unit has a procedure whereby the person or persons responsible for analysis are available to assist departmental investigators, in person or by phone, by applying information in the intelligence file and his / her own expertise to a current investigation.	50
Total		100

d. Production/Dissemination

1	The intelligence unit is responsive to requirements of on-going investigations, including having a procedure to keep its members aware of major cases.	40
2	The intelligence unit produces periodically and / or on order reports on major trends in criminal activity in its jurisdiction, emphasizing new or developing types of organised crime activities.	30
3	Intelligence reports are disseminated as widely as possible within limits set by need-to-know and sensitivity of information (the rule should be positive, giving the benefit of dissemination to those who need and can use the information).	30
Total		100

e. Management Procedures

1	The intelligence unit has a procedure for obtaining the reactions of consumers to its products.	25
2	The intelligence unit has a collection plan to assist it in focusing its efforts on the most important of the crime problems. The plan is periodically updated (monthly) and is coordinated with the chief of investigations and approved by the department head.	20
3	There is an element in the department's training program to prepare personnel for the specialised activities of the intelligence unit, especially analysis and intelligence investigation.	20
4	Security guidelines are in existence and observed, especially in limiting access to the files to analysts and file clerks, distributing intelligence reports only to those with a need-to-know within the organization and only to other law enforcement agencies on the outside with which there is an agreement for the protection of the intelligence material.	20
5	There is a procedure for evaluation of the effectiveness of the intelligence unit's operation.	15
Total		100

In evaluating performance, each element will be graded in terms of the following scale:
1. The element is being implemented effectively -1.0
2. The unit is organised to accomplish the element but the operation is only partially effective- 0.80/0.70/0.60
3. The unit is in the process of organising to accomplish the element but is not yet operational - 0.50
4. The unit has been organised to accomplish the element but the operation is ineffective - 0.30
5. The unit has not / does not recognise the requirement to accomplish the element - 0.0

An example of how this system would apply follows.

A. The intelligence unit is responsive to investigations including having a procedure to keep its members aware of major cases. The evaluator found there was no procedure to keep its members aware of major cases; thus he gave the unit 0.60 of the total value of the item or 0.60 times 40 which equals 24 points.

B. The intelligence unit produces periodically and/or on order reports on major trends in criminal activity in its jurisdiction, emphasizing new or developing types of organized crime activities. The evaluator, after reviewing reports, found that they were being produced, but only infrequently highlighted new and developing organised crime activity. Thus, he gave the unit only 0.70 of this value, or 0.70 times 30 which equals 21 points.

C. Intelligence reports are disseminated as widely as possible within limits set by need-to-know and sensitivity of dissemination. The evaluator finds that the unit stresses dissemination and gives the unit full value, or 1.00 times 30 which equals 30 points.

Total for this portion of evaluation: 75 points

REFERENCES

1. Arizona Department of Public Safety (1995) Policy Fifty-Seven - Criminal Intelligence. Phoenix, AZ: Arizona Department of Public Safety.
2. Bureau of Justice Assistance (1993) "Criminal Intelligence Systems Operating Policies" 28 Code of Federal Regulations Part 23.20. at www.iir.com/Publications/23cfr.htm
3. B. Fiora, "Writing Intelligence Reports that Get Read" (Competitive Intelligence magazine, Vo.5 No.1 January-February 2002)
4. California Department of Justice (1993) The Bureau of Intelligence Operations Manual. Sacramento, CA: California Department of Justice.
5. Commission on Accreditation for Law Enforcement Agencies, Inc. Standards for Law Enforcement Agencies, Fourth Edition. Fairfax, VA: Commission on Accreditation for Law Enforcement Agencies, Inc.
6. Criminal Justice Commission, Security Guidelines)(1995:5.8)).
7. CPOA standards
8. Europol Guidelines on Intelligence
9. Europol Analytical Unit, The Hague 10-21 May 1999
10. Griswold v. Connecticut (1965) 381 U.S. 479
11. Godfrey and Harries "Basic Elements of Intelligence"
12. Harris, Don R.. (1976) Basic Elements of Intelligence - Revised. Washington, DC: Law Enforcement Assistance Administration, September.
13. ICPO-Interpol Guidelines on Criminal Intelligence Analysis (Vers.3, 2000)
14. International Association of Chiefs of Police (1998; Criminal Intelligence Model Policy. Alexandria, VA: International Association of Chiefs of Police. (1985) Law Enforcement
15. Krizam, Lisa (1999) Intelligence Essentials for Everyone. Washington, DC: Joint Military Intelligence College.
16. Mathams, R.H. (1995) "The Intelligence Analysts' Notebook", Strategic Intelligence: Theory and Applications, Douglas H. Dearth and Thomas Goodden, 2nd ed. Washington, DC: Joint Military Intelligence Training Center.
17. Martens, Frederick T. (1987) 'The Intelligence Function," Major Issues in Organized Crime Control, Herbert Edelhertz, ed. Washington, DC: U.S. Department of Justice.
18. National Committee on Criminal Justice Standards and Goals (1976; Report of the Task Force on Organized Crime. Washington, DC: Government Printing Office.
19. Peterson Marilyn B. "Collating and Evaluating Data"
20. Peterson Marilyn B. "Analysis and Synthesis
21. Policy on the Management of Criminal Intelligence. Gaithersburg, VA: International Association of Chiefs of Police.
22. Roger Paul "Security and the Intelligence Process
23. Schneider, Stephen (1995) "The Criminal Intelligence Function: Toward a Comprehensive and Normative Model IALEIA Journal, Vol. 9, No. 2, June.
24. Report on Police, National Advisory Commission on Criminal Justice Standards and Goals, 1973. Commissioned by the Law Enforcement Assistance Administration (LEAA) on October 20, 1971 to formulate national criminal justice standards and goals for crime reduction and prevention at the state and local level. Richard Wright "Management of the Intelligence Unit"
25. The Commonwealth of Australia Protective Security Manual. (1991)
26. UNDCP Intelligence Policy and Training Manual (2000)
27. Wright, Richard (1998) Ten Steps to Establishing a Criminal Intelligence Unit, Issues of Interest to Law Enforcement Criminal Intelligence: A Vital Police Function. Marilyn B. Peterson, ed. Sacramento CA: Law Enforcement Intelligence Unit.