UNITED NATIONS
Office on Drugs and Crime

POLICING

Police Information and Intelligence Systems

Criminal justice assessment toolkit

4

UNITED NATIONS OFFICE ON DRUGS AND CRIME
Vienna

POLICING

Police Information and Intelligence Systems

Criminal Justice Assessment Toolkit

UNITED NATIONS
New York, 2006

TABLE OF CONTENTS

1. INTRODUCTION

The concept of “criminal intelligence” is neither easy to explain nor to translate. A direct translation can have negative political and historical associations in some parts of the world that make the word inappropriate in may international settings. As a result, it is often easier instead to use the word “information” and, indeed, the terms “information” and “intelligence” are often used interchangeably.

Definitions of what constitutes intelligence differ. Some say intelligence is “information designed for action”, some say that it is “assessed information”. Some say that information is transformed into intelligence through the analytical process, whilst it has also been called, “information which is significant, or potentially significant, for an enquiry or a potential enquiry”. The common theme is that intelligence is a special type of information with additional value that can be recognised or assigned through some kind of analytical process. “Criminal intelligence” is simply any information with additional value that can be used by law enforcement to deal with crime.

Acknowledgement should also be made of the current debate within the law enforcement analyst community as to whether their work actually has anything to do with intelligence at all. Some say that crime analysis is not an “intelligence” function, other say it is fundamental to it. For the purposes of this document, no distinction is made. Whatever they term is preferred, crime analysts and criminal intelligence analysts fulfil the same role and perform it in the same way.

As a law enforcement strategy, criminal intelligence has been in existence for many years. Indeed, although it has only recently been formalised, many of the basic (and intuitive) approaches of the traditional investigator are the same. For instance, officers have always attempted to identify the common thread that links clues in a case together, or kept a mental note of the habits of prominent criminals, or cultivated special relationships with people in the criminal underworld who provide inside information. This has always been simply considered to be good police work. Consequently, even in countries where the term “criminal intelligence” has not been formally adopted, it should be possible to find key components of a criminal intelligence system, such as the gathering of information about criminals, storage of fingerprints and/or DNA and use of covert investigation techniques, including informants.

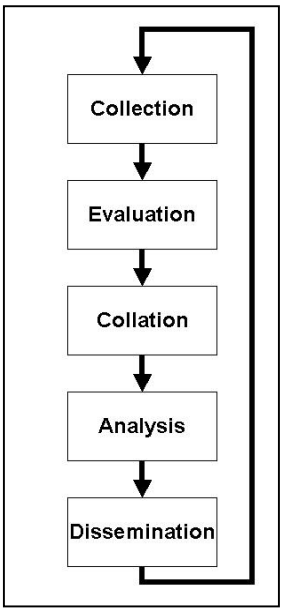
Sophistication in the use of police information and intelligence has been steadily increasing over the last half-century. Police information systems which were formerly based on the collation of index cards managed by a librarian have evolved with information technology into departments using dedicated software and the skills of a professional crime analyst. The application of the information has also become more sophisticated. Intelligence techniques and methodologies have been developed to identify crime threats or to profile existing crimes or crime figures. Strategically and tactically, intelligence is now available that can be used to make police decision-making more accurate and easier to justify.

As already stated, the way in which the value of information is recognised or attributed is usually through some kind of analytical process. Practitioners have identified a series of common stages through which this happens.

Whilst it is possible to find minor variations in these stages – all of them staunchly defended in different quarters –, this diagram represents the most common steps in developing intelligence. The arrow from the last box back to the start indicates that the process is an “intelligence cycle” through which information and intelligence is continually refined. Sometimes an additional box labelled “Direction” will be placed at the top of the cycle to represent how, in some models, there can be an element of management and tasking to the process. (A further diagram depicting simple intelligence flows is annexed to this document.)

Once information has been collected or gathered, it will be “evaluated” according to the reliability of its source as well as the relevance and validity of its content before being filed, cross referenced and ordered ready for use, that is, “collated”. The actual analysis will then consider the information in context, draw conclusions as to what it means and produce reports, briefings and other documentation representing that meaning. The results or products of this process will then be distributed , or “disseminated” to those who need to know it. The “need to know” principle is fundamental to working with sensitive information and intelligence. It means that, unless there is a clear professional reason for sharing information with another person that information should not be shared – even if he or she has

the appropriate security clearance level to receive it. The fewer people who know about something, the easier it is to keep it confidential.



In recent years there have been some important developments concerning the use of criminal intelligence by law enforcement agencies in many parts of the world and these have resulted in an increasing recognition amongst practitioners that:

- timely and actionable criminal intelligence is essential to make an impact on the prevention, reduction and investigation of serious and organised crime, particularly when it is of a trans-national nature. ("Timely" means that it is provided in good time and "actionable" means that its detail and reliability supports the taking of action.);

- criminal intelligence can play a significant role in helping with the directing and prioritising of resources in the prevention, reduction and detection of all forms of crime – through the identification and analysis of trends, modus operandi, "hotspots" and criminals – both at the national and transnational level; and

- intelligence can form the bedrock of an effective policing model – often termed "Intelligence Led Policing" – where intelligence is essential to providing strategic direction and central to the deployment of staff for all forms of tactical policing activity, including community policing and routine patrols.

Whilst significant differences will be seen in the understanding and acceptance of information and intelligence as a law enforcement tool, the fact remains that, in many countries and international organisations, criminal intelligence has been adopted as the law enforcement strategy of choice to drive policing forward in the next century.

One final point of which to be aware is that national police secrecy laws may well apply to questions related to police information and intelligence so that an assessor may not always receive complete answers to his or her questions. Such a barrier is easy to hide behind where answers to questions would be inconvenient or controversial, for instance, where human rights have been violated, but, on the other hand, there may be no such sinister motive at all.

In addition to developing an understanding of the strengths and weaknesses of a state's approach to police information and intelligence, the assessor should be able to identify opportunities for reform and development. Technical assistance in the area of police information and intelligence systems in the context of a broader strategic framework may include work that will enhance the following:

- Drafting (or amendment) and implementation of legal instruments that provide responsible police powers related to the collection and use of information and intelligence together with appropriate safeguards;
- Drafting (or revision) of relevant guidelines and manuals;
- Development of an integrated system for managing and exchanging police information and intelligence;
- Creation of a national or central coordinating body for criminal intelligence and information;
- Development of independent safeguards and oversight mechanisms;
- Improvement in the technical infrastructure for the handling and integration of data (including enhancement of data security);
- Professional development of specialist staff (especially with respect to the skills of analytical staff and intelligence managers);
- Enhancing technical facilities available to staff working with information and intelligence (including support for the creation and development of key police databases and access to them);
- Facilitation and promotion of mechanisms (legal, institutional and technical) for sharing information between national agencies and international partners;
- Development of a methodology and structures for compiling a national organised crime threat assessment.

2. STATISTICAL OVERVIEW

Please refer to **Cross-Cutting Issues: Criminal Justice Information** for guidance on gathering the key criminal justice statistical data that will help provide an overview of public safety and police services delivery as well as the overall capacity of the criminal justice system of the country being assessed.

The availability of statistics related to policing will vary greatly. Statistics will also be variable in their reliability and integrity. Where possible, statistics provided by a government agency should be validated against statistics from other sources, such as non-governmental organisations or international bodies. As stated above, police information and intelligence can be a sensitive topic and may be protected by special secrecy laws that will preclude answers to some of the assessor's questions.

A. Is there a national department for statistics? What does it produce in respect of crime analysis? Where does it get its information, and from whom?

B. Is there a public or private sector crime research facility that provides analysis on crime trends or criminality? If yes, seek recent examples.

C. Are statistics compiled regarding the incidence of criminal offences against a variety of criteria? Are they compiled in relation to local, regional and national geographical areas? Are these statistics available to the public? Are they available to local, regional and national police commanders?

D. How many agencies are involved in criminal information and intelligence? Does any state security agency or department have any competence for combating crime? Who has competence to deal with counter terrorism?

E. How many law enforcement agencies have an information/intelligence database or network of databases? How many collate records in a paper-based filing system, such as index cards? How many have access to a police intranet, a closed computer network that is shared by police agencies and officers? How many agencies have something designated as criminal intelligence unit? How many have access to proprietary analytical software like ibase/i2, Xanalys Watson, or Unisys Holmes2?

F. Where intelligence-led policing has been adopted, are there figures on how many intelligence-led operations were conducted? What was the outcome?

3. LEGAL AND REGULATORY FRAMEWORK

Police information and intelligence can be heavily constrained by legislation that governs the type of information police may hold, the purposes for which it may be held and how it should be handled.

There may be laws that completely prevent any third party from knowing the content of government databases, including those of the police, or there may be Freedom of Information laws which, conversely, provide considerable access to them. However, there will always be some proportion of the information which may not be disseminated outside of those especially involved in it - whether because of cultural preferences for controlling information or because of operational reasons, i.e. not letting someone know that he or she is under suspicion.

The sensitive nature of some police information and intelligence, and the intrusive techniques that may sometimes be used to collect it, afford a particular importance to any supervisory mechanisms and security measures put in place. These will usually be contained within legislation or codes of procedure.

Every country will have something called "classified information" that is considered to be sensitive or secret. This will normally be "protectively marked" by having labels attached such as "confidential" or "secret". Because these labels or markings can be different from country to country, it has become common practice for government and military organisations working trans-nationally (for instance in the EU or NATO) to provide a "table of equivalence" indicating what each classification level is called and what it means. The most common terms used in English will be "restricted", "confidential", "secret" and "top secret", but there may be others.

Where information has been "classified" under one of these headings, special handling restrictions will come into play and access will only be given to people with the appropriate level of clearance. The special handling restrictions may define not only who can see the classified information, but also the conditions under which they may see it, in what medium it may be stored, how it may be transmitted and how it must be destroyed. It is quite possible that, under national police laws, any information in the possession of or generated by the police is automatically "classified" even though the content has no particular confidentiality.

In the last quarter of the 20th Century, prompted by unprecedented advances in information technology, a new doctrine of the protection of personal data (sometimes shortened to "data protection") has evolved. This has become highly developed in some countries, but not at all in others and is a highly complicated area of law. Those countries that subscribe to this doctrine believe that any data that can directly or indirectly identify a living individual (the "data subject") are owned by him or her and should not be held by others unless very strictly controlled. The data subject can consent to his or her data being held, but those data cannot be used for anything beyond the data subject's limited consent. Where the data are needed to prevent or combat crime, certain exceptions are made in respect of consent, but the other controls still apply. For instance, the doctrine says that: (a) data cannot be forwarded to anyone unless adequate controls and security for data protection are in place; (b) it should only be used for the purposes for which it was originally supplied; and (c) once those purposes have ceased to apply, the data should be deleted. This concept is by no means accepted by all countries, and there are, therefore, implications for information exchange between countries with data protection legislation and those without. To date, a universally acceptable solution to this dilemma has not been found.

Where data protection and privacy laws are well established, there will be an official independent supervisory body to which complaints may be made and which has powers to inspect and order changes to the way personal data is managed. In addition, a data subject will have the right to seek redress in the courts for any incompatible use of his or her personal data.

A. Is there existing legislation or written guidance on the gathering, storage, analysis and dissemination of criminal intelligence or information by or for the purposes of law enforcement? What does it allow? What are the constraints and limitations?

B. What laws or regulations apply to "classified" information? Is there a "protective marking" scheme? Is there a law on protecting "official secrets"? What consequences are there for someone who discloses classified information? Is it a criminal offence?

C. Is there legislation related to the protection of personal data (i.e. data protection), data retention and/or freedom of information? What does it say about data gathered for the purposes of law enforcement activity? Does the law place a responsibility on the agency holding the data to ensure its accuracy and relevance? Is there a statutory review period at the end of which a decision has to be taken as to whether the purposes for holding personal data still apply or whether they should be deleted? Is there the right for a data subject to sue for damages where his or her rights have been breached?

D. Is there an independent supervisory body for data protection and privacy complaints? What powers does it have? Is it consulted on new legislation related to information and intelligence? Does it oversee law enforcement information? Does it issue regular public reports on how law enforcement agencies deal with data?

E. What other organisations exist to oversee the way police information and intelligence is managed? What powers do they have?

F. Is there a parliamentary or other official committee that has oversight of police information and intelligence matters? What powers does it have? Does it receive strategic threat assessments from the police on serious and organised crime? See **Section 5.5** below. Does it receive other reports from the police on activities involving information and intelligence? Are its reports available to the public? What do they say?

G. Is there an executive advisory committee that coordinates national intelligence matters? Is the law enforcement sector represented on it?

H. Is the "need to know" doctrine described in legislation? If not, is it found in regulation or guidelines? Can officers describe what the "need to know" rule means and why it is important?

I. Is there legislation and/or regulation on information security? Is there a protocol, regulation, order or set of instructions detailing minimum standards in information security?

J. Is there legislation allowing the police to:
   - Collect information, including personal data?
   - Store and use that information for the investigation, detection and prevention of crime?
   - Share information with other law enforcement agencies, nationally and trans-nationally?
   - Share information with international law enforcement organisations, such as Interpol?

K. Is there legislation requiring the retention of billing records and subscriber usage details by mobile telephone companies and internet service providers?

L. Are there police orders, guidelines or regulations regarding the use of criminal intelligence and information? What do they say? Is there a code of practice on the dissemination of data? When were they last updated? Are operational police officers and investigators aware of them?

M. Has the United Nations Convention Against Transnational Organised Crime (UNTOC) been signed and ratified? In particular, have the provisions on the sharing of information and intelligence been implemented?

4. INFRASTRUCTURE

Although the assessor should not expect to find well-developed criminal intelligence processes in place, the presence of police information and its structured use will be ubiquitous. This need not involve computerised systems and the systematic and structured filing of paper records can be equally effective.

Although the use of police information and intelligence may have been given a strong legal basis, unless good practice is integrated into police culture, together with appropriate procedures and adequate resources, the legislation will have little impact.

In some countries there may be a special central agency for criminal intelligence, in some there may be dedicated units within existing policing agencies (even at local police station level), in others, the concept will not appear at all.

Where a national law enforcement framework consists of a number of different agencies or institutions (e.g. national police, gendarmerie, crime police, customs, border guard etc., the volume and quality of information exchanged, and the speed with which requests are answered, will be indicative of the level of cooperation. Where no national criminal intelligence or information database exists, which is highly unlikely, the information and intelligence held will undoubtedly be fragmented and duplicated. Strong information exchange mechanisms can help to mitigate this.

Facilities for the use of technical surveillance, such as telephone interception and listening devices, can sometimes be concentrated in national security agencies. In such cases police requests for assistance will therefore be in competition with and subordinate to national security priorities.

4.1 POLICY

While almost all countries will have information sources and files of collated information of one kind or another, very few will have a uniform structured policy on how to combine them.

However, any integrated information and intelligence framework will embrace and engage every all level and aspect of law enforcement: Strategy will be decided on the basis of analysis; Priorities and resources will be allocated on the basis of analysis; Operations and police patrols will be directed on the basis of analysis.

A. Is there a national strategy, national plan or similar document outlining priorities and objectives for “policing”? Within it, is there any reference to criminal intelligence or the gathering of information for the purposes of investigating crime, or policing generally? Who is responsible for this activity?

> Intelligence-led policing is a strategy or tactic by which information and intelligence is used to inform the allocation of resources against those threats that have been shown, through analysis, to cause the greatest harm.

B. Is there a national criminal intelligence strategy? What is in it? Who is in charge? Is the concept of intelligence-led policing described? Do other national crime strategies mention criminal intelligence? If yes, what do they say?

4.2 INSTITUTIONS

A. If there is a national or principal agency dealing with criminal information and intelligence? If yes, what level of seniority does its executive manager have? To whom does he or she report? Does the organisation coordinate and lead on all activities related to criminal information and intelligence? What are its objectives? If it has a mission statement, what does it say? Does it have a business plan? How does that business plan expect to enhance and develop police information and intelligence in the future?

B. Where a national or principal agency for criminal information and intelligence exists, how many staff does it have? Do its staff have police powers? Is it empowered to collect information and intelligence in its own right? Is it empowered to manage a network of informants?

C. Which other organisations or agencies are involved in gathering, storing and using police information and intelligence?

D. Where each law enforcement body is responsible for managing its own information and intelligence, is there a set of common standards for:
   - the collection, assessment and analysis of the information and intelligence?
   - the recording and logging of information and intelligence?
   - security standards?
   - reports and briefings?

E. Are there criminal information and intelligence departments, units or sections at regional level? How many analysts, if any, do they have?

F. Are there criminal information and intelligence departments, units or sections at local police station level? How many analysts, if any, do they have?

G. Are criminal information and intelligence departments units or sections organised and managed as part of an independent crime police directorate or are they accountable to the local police manager?

H. Are other police officers, prosecutors and judges trained in the collection and use of criminal information and intelligence? Are there special courses for managers of investigations on how to use analysts and how to task and direct their work?

4.3 STAFFING

Although not impregnable, prevailing wisdom states that technical and physical security systems are now so strong that criminals find it more cost effective to try to corrupt the people who administer them instead. It is, therefore, important to ensure the integrity of the staff working with police information and intelligence.

Due to the sensitive nature of criminal information and intelligence, those chosen to work in the area need to have higher credentials in terms of integrity than in some other policing roles. This is often measured through a system of positive security vetting that investigates the background of intelligence staff and assesses the risk that they may pose.

A. Do staff recruited to work with information and intelligence undergo any addition selection procedures to assess their trustworthiness, that is, there a positive vetting system? Is that assessment reviewed regularly? What happens if someone “fails” the assessment? How often does that happen?

B. There may not be anyone formally designated as an analyst and, where such a post does exist, he or she may not have been formally trained. However, there will often be someone who is responsible for maintaining local files and to whom other officers will turn when they need some background information on a criminal.

Skilled and experienced analysts are key to achieving an effective information and intelligence capacity. Analysts are expensive to train and, if their work is undervalued they can soon sell their skills in the private sector for far greater financial rewards. Retention of analyst staff is an acknowledged problem.

C. Are there members of staff designated as “analysts”? How are they selected? Are they recruited from the pool of police officers or are they recruited directly from the general public? Are they recruited after an objective selection procedure? What are the selection criteria? What qualifications are required? Does the selection procedure include psychometric testing?

D. How are analysts formally trained? Do they receive regular refresher training? Is there a career development and promotion structure for analysts? What proportion of analysts remain at least 5 years in police service after being trained? How do the salaries of analysts compare with police officers on patrol?

E. Where staff have access to computers, are analysts provided with specialist analytical software? If yes, what? Are technical resources adequate to allow full use of this software? Where computers are available, are they reliable, e.g. in terms of memory and power supply?

4.4 ORGANISING THE INFORMATION

Information is the mainstay of crime investigation and although many countries will still not have introduced computer databases, similar results can be achieved through careful and accurate filing of paper files or index cards. The difference will normally be seen in the physical size of the file, the skills of the librarian and the speed of retrieval.

Computer databases represent a significant investment, which is often underestimated. Hardware can soon become obsolete and software licences require regular and expensive subscriptions. However, there are important benefits to be had in terms of managing volume data that would soon become otherwise unmanageable.

While the use of information technology can reduce the numbers of staff required to perform certain functions, any cost-benefit received is greatly reduced where human resources costs are low. Although, of course, a computer is much faster and the level of accuracy much greater, there is little that can be achieved by information technology that cannot be done by manual activity.

4.4.1 Where Information Is Kept Only In Hard Copy

A. Are police records, files or indexes of useful information maintained? If yes, what do they contain? In particular do they contain crime reports, criminal records and fingerprints? Where are such files and records located? Is there a national or principal location, agency or registry for the files? If not, do different police agencies have their own central registry of such information? Do local police areas or districts keep such records? Is there any cross-referencing or indexing of the information? How easy is it to access and retrieve these records?

B. Where they exist, how many files or records are there? How many new records are received on a daily basis? Who does it? Where does the information come from? How much old information is weeded (deleted) because it is no longer of use? What procedure is in place for making that decision?

C. Can officers make direct requests for searches of information and intelligence files or is a senior officer or prosecutor required to authorise such a request? Do such requests have to be made in writing? On average, how long does it take for a request to be answered?

D. At what levels (local, regional, and national) do police officers and/or analysts have access to national police information and intelligence files and records? How is this information sent? Is the transmission method secure and free from tampering?

Although the use of DNA in investigation is rapidly increasing, it is a relatively new field and it is accepted that the necessary technical support and expertise will be beyond the majority of countries. Questions on DNA are included in this tool only for the sake of completeness and are not to be considered indicative of any technical deficiency.

E. Are DNA samples collected? How are they stored? How many files exist? Is DNA information shared with international law enforcement agencies such as Interpol?

It is important to note that Interpol has other databases that are useful for organizing information. These include, for example, the following databases: Fingerprints, Lost or Stolen Travel Documents (SLTD), Child Sexual Abuse Images, Stolen Works of Art, and Stolen Motor Vehicles.

F. Do other files or records of collated information exist that may be of value for law enforcement, such as vehicle ownership, driving licence holders, credit ratings, residence? Do visitors to the country or region have to register with the local police, often done automatically through the hotel register? If so, at what level is this information collated? If citizens are issued with personal identification cards, are they issued by the police? Is this information available for the purposes of law enforcement investigation?

G. Where files are accessed or requested, is there a log maintained of who accessed or made the request, when, and why? Is access restricted to those who need to know it?

H. Are offices equipped with shredding machines for the destruction of sensitive documents? Are there special waste sacks for the disposal of confidential paperwork? What rules govern the control and use of these?

4.4.2 Where Information Is Also Kept Electronically

A. Is there a national or principal database dealing with criminal information and intelligence? If not, do police agencies have their own information and intelligence databases? Are these different databases linked? Is it possible to do one search across all the databases in real time? If not, how easy is it to search all the databases applying the same search criteria?

B. Where a national or principal criminal information and intelligence database exists, what is its infrastructure and architecture? How much data does it contain? How much new data is input on a daily basis? Who does it? Where does the data come from? How much old data is weeded (deleted) because it is no longer of use? What is the procedure for making that decision?

C. Can officers make direct requests for searches of information and intelligence files (paper and electronic) or is a senior officer or prosecutor required to authorise such a request? Do such requests have to be made in writing? On average, how long does it take for a request to be answered?

D. At what levels (local, regional, and national) do police officers and analysts have access to national police information and intelligence files and databases? Are there access terminals in the main police offices at the local, regional and national level? Are lines to these offices encrypted? Are terminals protected by personal passwords and/or other security?

E. What arrangements exist for storing and searching, crime reports, criminal records, fingerprints and, if collected, DNA? Can any police officer access these records or is prosecutorial or judicial permission required? Is there a national DNA database? Is DNA shared with the Interpol DNA database? Is there an Automatic Fingerprint

Identification System (AFIS) in place? Where AFIS is present, where are the AFIS scanners located? Do all suspects have their fingerprints scanned on the AFIS system? How many fingerprint and DNA records are held? What happens to DNA and fingerprint records if the suspect is later proven not guilty?

F. Do other databases exist (such as vehicle ownership, driving licence holders, credit ratings, residence) that may be of value for law enforcement? Do visitors to the country or region have to register with the local police (often done automatically through the hotel register)? If so, at what level is this information collated? Is it included in any database with wider access? If citizens are issued with personal identification cards, are they issued by the police? Do the police store the details from identification cards electronically? Are the data available for the purposes of law enforcement investigation?

G. Where computer systems are in place, how reliable is the technical infrastructure? Is there significant "down time" when the information cannot be accessed due to technical failure? Is access to all databases protected by a personal password and/or additional security measures? Does the system allow for a hierarchy of access so that information is available on a "need to know" basis, that is, only by those who need to know it in order to do their job?

H. Are confidential databases accessible only on stand-alone computer terminals (i.e. not connected to the internet or intranet)? Are there precautions against unauthorised copying of information (these may be as basic as sealing a floppy disk drive, disabling CD write software or blocking the USB ports)? Is every attempt at access logged against the user's name, the date and time of access? Is a strong anti-virus software used? Where information is sent out of the building, are secure lines with encryption devices used?

I. Are offices equipped with shredding machines for the destruction of sensitive documents? Are there special waste sacks for the disposal of confidential paperwork? What rules govern the control and use of these?

J. Where is the hardware for police information and intelligence systems located? Are the buildings and/or offices structurally secure? Is there perimeter security preventing unauthorised access? Are staff and technicians vetted or security cleared? Is the building subdivided into security zones with staff access being restricted as appropriate?

5. CRIMINAL INTELLIGENCE AS A PROCESS

Wherever the concept of criminal intelligence has been formally adopted, the key stages of the intelligence cycle will be represented in some form or other: Collection; Evaluation: Collation: Analysis; Dissemination and, sometimes, Direction.

The following list reflects the minimum structure, functionality and facilities required for a rudimentary, but effective use of police information and intelligence:

- Rules on how information may be collected (and for which purposes);
- Rules on information security;
- Protective marking (classification) system;
- Knowledge and practice of " the need to know" principle;
- Rules on to whom information and intelligence may be distributed;
- System for collating information of interest and importance (on paper and/or computer);
- Active encouragement and facilities for all officers to submit such information;
- A system of quality assurance (and source evaluation) for any information submitted;
- System for collating key information catalogues (such as crime reports, criminal records and fingerprints);
- Access and search facilities for these;
- A mechanism for requesting information from other agencies, organisations or countries;
- Trained analysts;
- Guidelines and standards on the content of analytical briefings, reports and other intelligence products;
- Active consideration of analytical products as part of the management process.

Such components would be the same at the national, regional and local level, save for the question of scale and may be more or less sophisticated depending on the quantity and nature of specialist equipment and software available.

5.1 COLLECTION

The place or person from which information is obtained is called a "source". Information and intelligence can be sourced anywhere and at anytime. However, the most important (and often most underutilised) source for criminal intelligence is the patrol officers who are in constant contact with the community and are the first to attend crime scenes. The more developed the concept of criminal intelligence is, the greater the volume of information and intelligence contributed by these patrol officers will be.

5.1.1 Primary Sources

A. Are police officers able to submit an intelligence log (either on paper or electronically) as a matter of routine? Are officers encouraged to do so? Is there any kind of performance measure related to the submission of information and intelligence by police officers?

B. Is there a common national standard for recording information and intelligence? Are common formats and terminologies used?

C. Is there a network of specialist police officers deployed to gather and develop criminal information and intelligence? If yes, how many? What are their job descriptions? How are they managed?

D. Once police operations have taken place, are they formally debriefed in terms of what lessons have been learned? Is this information forwarded as information or intelligence? How and to whom?

The term "open source" refers to any information that can be legitimately obtained (i.e. "sourced") free on request, on payment of a fee, or otherwise. It is often said that strategic analysis relies for 90% of its evidence and research material on open sources. There are commercial concerns that offer powerful search engines and provide access to the world's media, academic journals and government reports. However, these services can be expensive. At the other extreme, reference to the local press and other media can also be useful.

E. Do analysts have access to open source information? What are the major sources available to them? Are these in hard copy (e.g. newspapers) or electronic? Are there subscriptions maintained to commercial information providers (such as Reuters or Lexis-Nexis)?

5.1.2 Covert Surveillance

Covert surveillance is a particularly intrusive method for collecting information. The use of covert surveillance measures involves a careful balancing of a suspect's right to privacy against the need to investigate serious criminality. Provisions on covert surveillance should fully take into account the rights of the suspect. There have been various decisions of international human rights bodies and courts on the permissibility of covert surveillance and the parameters of these measures. Reference should be made to these. An extensive discussion is contained in the commentary to Article 116 of the Model Code of Criminal Procedure (MCCP)(DRAFT, 30 May 2006). In those societies where the authorities exercise forceful control over the populations, the use of these techniques may be indiscriminate. Other systems will require a number of strict safeguards against abuse including the requirement that the offence be serious, that the use of the technique be vital to the case and that essential evidence cannot be secured by less intrusive means. Judicial or independent oversight is common and is required under international human rights law.

A. Are the following covert surveillance techniques deployed:
   - Interception of telecommunications?
   - Interception of email traffic?
   - Interception of post/mail?
   - Use of listening devices?
   - Use of tracking devices?
   - Use of surveillance teams?
   - Use of photographic surveillance?
   - The use of fake personal and company identities?
   - Covert search of letters, packages, containers and parcels;
   - Simulated purchase of an item;
   - Simulation of a corruption offence;
   - Controlled delivery.
   - Covert real-time monitoring of financial transactions;
   - Disclosure of financial data. This measure is carried out through obtaining information from a bank or another financial institution on deposits, accounts or transactions
   - Use of tracking and positioning devices.

See also **MCCP (DRAFT, 30 May 2006)** for a listing of covert measures.

B. Is there legislation in place allowing their use? What preconditions must be satisfied before they can be used? Who authorises their use: prosecutor, judge or senior police officer? Are there time limits within which they must be used? Is there any independent oversight and monitoring of these techniques? Can the results of these techniques be used as evidence in court? Are there special rules of evidence that apply? If so, what?

C. How many telephone interceptions ("wiretaps") are made each year? How many other forms of interception are made each year?

D. Are these techniques employed directly by the police or is another government agency involved? What do practitioners think about the capacity to use these techniques? Is it sufficient for national needs? If not, what else do they think would be needed?

5.1.3 Informants

The use of informants or human sources for gathering information and intelligence is age-old. In some countries the use and handling (i.e. “management”) of informants is centralised, in others, informants are the unsupervised personal contacts of individual officers. Informants may have many different motivations. They may, on the one hand, be “concerned citizens” providing information out of a sense of civic duty or, on the other, hardened criminals seeking to oust the opposition. Information may be provided as a bargaining chip for some personal advantage, or, most commonly, be traded for cash. Because of the secrecy involved in handling informants, and because of the potentially large sums of money, there is an enormous capacity for abuse. Generally speaking, the reliability and source of any information provided by an informant needs to be carefully assessed and, where possible, corroborated. At the same time, it must also be recognised that the police owe a duty of care to their informants and must protect them from retribution.

See also **Section 5.7, POLICING: THE INTEGRITY AND ACCOUNTABILITY OF THE POLICE**

A. Is there legislation in place allowing the use of informants?

B. How are informants managed? Are their details registered in a confidential file? Are the personal details of informants known only to those dealing with them? Is there a senior office with responsibility for supervision of informant handling? Is there a specialist informant handling unit? If yes, how many informants are currently active?

C. Is there special training in the use of informants? Are all investigators permitted to run informants or is this restricted to specially selected officers? Is the identity of informants protected when giving testimony in court? Is there a policy on informants’ protection and court testimony?

D. How are informants paid? Are they paid by results or depending on the amount of information they provide? Is the investigator handling the informant also involved in making the payment or is it done separately? How is the money accounted for? Are receipts required? Who audits payments made to informants?

5.1.4 Widening the net

No one can ever be in full possession of all the information or intelligence that exists on a subject. Gaps in the research material can seriously spoil the final product. However, an analyst can improve the situation by attempting to acquire all the available data on a subject by tapping into the information held by others.

Information sharing is a reciprocal concept based on mutual advantage and, unless information flows in both directions, the stream of information will soon dry up.

See also **Section 6, Partnerships** below

5.2 EVALUATION

Best practice has evolved whereby all information or intelligence submitted is evaluated on the basis of (a) the previous history of reliability of the source and, (b) to what degree the source has direct knowledge of the information he or she is providing (for instance, did the source acquire the information directly, or did he or she hear it from someone else?). There are different systems in use for this, but, essentially, the idea is the same: to provide an estimate of risk and reliability for the information. Often the evaluation will result in a ‘source evaluation code’ consisting of a letter and a number chosen from a standard grid of options. The evaluation needs to be kept under continuous review as new information may be discovered which changes the perception.

Allied to this evaluation, there may be a further “handling” or “dissemination” code added that limits the extent of permission for further distribution. This is intended to protect the information or intelligence from any unauthorised disclosure.

A. Is a reporting officer required to make a source evaluation of the information and intelligence he or she is recording? How is this marked on the information or added to the record? Is a code added to the record stating to whom the information may be disclosed, sometimes called a dissemination or handling code? Is this evaluation kept under constant review?

B. Is information and intelligence supervised and quality assured after submission? If so, what quantity of reports are returned for correction or further completion? How many reports are discarded because they do not meet required standards?

C. Are there rules preventing the use of information that has been obtained in breach of human rights (e.g. through torture)?

5.3 COLLATION

A. Are all records and logs received, either on paper or electronically, filed, cross-referenced, and ordered, ready for use? Who does this? Is data warehousing software used?

5.4 ANALYSIS

There are two basic categories of analysis: strategic analysis, which takes a higher "helicopter" and a longer-term perspective; and tactical analysis, which focuses on immediate, operational issues. Strategic information and intelligence considers trends and emerging threats. Tactical information and intelligence looks at an existing situation or current operation, often in real time.

Analysis considers information in context, draws conclusion as to what it means, highlights gaps in existing knowledge, suggests what is likely to happen next and makes recommendations as to possible future action.

The work may be prompted by anomalies, trends or connections noticed by the analyst him or herself during the course of his or her general research, but, more commonly, it will be initiated by senior managers asking a question or providing specific terms of reference.

The results may be presented in a number of different formats depending on the requirements of the person commissioning the work. These may range from in-depth reports on complex strategic issues to a short oral briefing about a particular operation.

Good criminal intelligence products are cogent, concise and accessible with clear and unequivocal recommendations justified by strong evidence. Unfortunately, where information flows and sources are weak, the analytical product will also be weak.

A. Are there trained analysts? If not, are there officers tasked with maintaining and collating police information and records and to whom other officers can turn for background information or advice about a criminal?

B. Are there guidelines on what different types of analytical report should contain? Are analysts aware of them? When were they written? Do they have a prescribed format? Do analytical reports contain executive summaries detailing the main evidence, conclusions and recommendations? Are they written in plain and unequivocal language? Do the conclusions and recommendations provide sufficient detail on which to base operational action? Are the recommendations supported by evidence?

C. Are reports produced that describe certain crimes or criminal behaviour and their common characteristics, i.e. "problem profiles"? Are reports produced on prominent criminals, their lifestyles, associates and criminal activities, i.e. "target profiles"? Are reports produced about the way in which a criminal market conducts itself, i.e. "market profiles"?

D. Hot spot analysis has become a common tool for mapping the density and other geo-temporal characteristics of criminal activity. Modern software can provide highly detailed interactive maps that contain an enormous amount of detail. However, similar results can be obtained through the use of coloured pins and flags on a printed map.

E. Where analysts are employed, do they undertake hot spot analysis? Do they do this manually or using a computer? To whom are the maps distributed and for what reason? Are there examples of where these have influenced policy or prompted a tactical response?

F. The link chart is also a common analysis tool that represents pictorially the relationships between different aspects of an enquiry or investigation, for instance individuals, locations, telephone numbers, motor vehicles, etc.

It is particularly useful when trying to collate and visualise connections between large quantities of data and can be helpful when presenting evidence in court. Advanced software (such as I-Base or Xanalys) exists for producing link charts, but they can also be produced manually.

G. Do analysts know how to produce link charts? Are they produced manually or by using computer software?

H. Do they perform other types of analysis, such as telephone and financial analysis?

I. How often are analysts asked to produce a specific report? What do police managers think about the concept of criminal information and intelligence? What do investigators and patrol officers think? How do those who manage investigations, including prosecutors or judges where applicable, think that their work is supported by analysis? Are there any examples in which a case has been solved or substantially advanced because of the intervention of an analyst?

J. Are analysts asked to work in real time on active operations? Are they co-opted onto major incident investigation teams or joint multi-agency task forces? What is the role assigned to them? Do they produce profiles and analyses that are used to inform and direct the decision making of the senior investigating officer or prosecutor?

5.5 DISSEMINATION

Analytical reports, unless written for public consumption, should only be distributed to those who “need to know it” (see above).

In formulating national management of and strategic approaches to the fight against organised crime, many governments have found value in compiling a national threat assessment for organised crime. Such a document collates and amalgamates all available information about who is responsible for the most crime, the harm they cause, and how their criminal activity is likely to develop in the future. At the same time, the document highlights any new phenomena or threats that appear to be growing in significance and which could be prevented by early intervention from becoming a major problem.

National strategic assessments of this kind are based on an accumulation of contributions developed at the local level and combined in order to acquire a national picture. Local conclusions can then be moderated and corroborated against those in other parts of the country.

Objective evidence provided in such a threat assessment is invaluable for policy makers who can then use it to design responses that will have maximum impact with the greatest economy through the targeted allocation of resources.

However, as with other forms of analytical product, the end result will depend on the quality and completeness of the data provided as well as the skills of the analyst preparing it.

5.5.1 Strategic Assessments

A. Is there a national crime threat assessment or other strategic crime report? Does it assess and describe existing and emerging criminal activity on the national level? Who coordinates it? Who defines its terms of reference? For whom is it produced? Does the document satisfy the terms of reference?

B. Are there regional and local crime threat assessments or strategic crime reports? Are they used to supplement and develop the national crime threat assessment or other strategic reports? Do they assess and describe existing and emerging criminal activity on the regional and/or local level?

C. Are strategic assessments and analyses provided to the office of the chief of police in the organisation? Does the chief of police provide feedback on their content? What use is made of them? Are there examples in which such reports have led to new policies or strategies, or changes in them?

5.5.2 Tactical Assessments

A. Do uniform police patrols receive regular information and intelligence briefings concerning their area of patrol? If yes, how often and what do they contain? Do the briefings suggest trends and possible developments in the area? Do police patrols think these briefings assist them?

B. Do the local police commander and crime manager receive regular, if not daily intelligence briefings on the crime activity in their area? How often are intelligence briefings provided? What do they contain? Does the briefing provide sufficient detail for choices to be made on the management of resources and officer deployment?

C. Are the results of analysis provided to partner law enforcement agencies? Are they provided to international organisations or police liaison officers from other countries? Is feedback received on them? Are the results of analysis received from partner agencies and organisations?

D. Are different versions of intelligence products produced for different audiences, i.e. is there an “open” or “unclassified” version for public consumption, as well as classified versions for internal use?

5.6 DIRECTION

The idea of directing the collection and development of police information and intelligence is found in all formal criminal intelligence management structures, sometimes called “criminal intelligence models”. The intention is to focus activity on the most harmful crime problems, and the most active criminals, who are identified through analysis of the available information, and to allocate sufficient resources to negate that harm. The approach is methodical and predominantly proactive, but has different needs at different levels.

In a criminal intelligence model, the structural apparatus for targeting effort, sometimes called “tasking and coordination”, will be duplicated at each level in the hierarchy and is intended to have a cumulative effect.

Mention should also be made of the COMSTAT process. This is a police management system that brings police managers together in open meetings to confront them on the crime figures in their areas and on their personal intentions on how to deal with them. It has been credited with a good deal of success and has the merit of closely associating commanders with the performance of their command.

This level of direction and participation of senior managers is unlikely to be present in the majority of countries.

A. Is there an organisational tasking and co-ordination mechanism that makes policy and resource decisions based on analytical reports? Does it issue instructions on what

criminal intelligence is required and where the focus of proactive police activity should be? How often does it do this? How are these instructions disseminated to the appropriate officers?

B. Is there a meeting or mechanism through which police managers and commanders are expected to justify their performance against crime?

6. LOCAL USE OF INFORMATION AND INTELLIGENCE

Even where the use of police information and intelligence is not widespread or systematic, the main ideas may still be useful at the local level with a minimum of sophistication and equipment. The assessor is reminded that the essence of structured criminal intelligence and its practical application can be achieved through the use of a pen, a sheet of paper and old fashioned commonsense.

The assessor may wish to consider if, in the absence of formal criminal information and intelligence structures, whether the basic elements already exist, albeit in rudimentary form. If so, could they be replicated elsewhere or constitute the foundation of an extended network?

The questions below should be considered as indicative of a basic criminal intelligence capacity.

A. Do local police stations have something called or otherwise identified as a criminal intelligence unit? If yes, where is it located? How is it staffed? What do the staff do? Do officers know about this unit? Do they know what it does? To whom is this unit accountable?

B. How is this unit equipped? Does it have computers? If yes, does it have any specialist criminal intelligence software? Where computers are present, are there printers and paper available? Where computers are not present, are there typewriters? Is the equipment sufficient for the numbers of staff?

C. Where there are computers, is there access to specialist databases or information? If yes, what information can be accessed? Is access to computers secure? Is it protected by personal password or similar? Do officers share their passwords? Is information and intelligence structured to ensure only authorised personnel can access particularly sensitive data? Are logs automatically created on who has accessed the data, when, and why? Is there any direct access to central or national records?

D. Where there are no computers, is there an office, part of an office or room in which information is collated and filed? What are the criteria for information to be filed here? Are there rules and guidelines on what information these files can contain? What sorts of information does it actually contain? How is it filed? Is the information cross-referenced and indexed? Who is responsible for the collation and filing? Has that person received any training?

E. Is access to this room restricted to authorised personnel only? Is access physically controlled by means of a key, keypad, or swipe card? Is sensitive information stored under additional security measures? How is access granted to these files? On what basis? Is an access log maintained? What does it say about patterns of access, who consults which files and how often?

F. Can files be removed from this room? On what basis? How is the removal recorded?

G. In all cases, how is new information added to the files? How are new files opened? Who has the authority to do this? How is this information submitted? Do officers receive training on this? How is new information submitted by officers supervised? By whom?

H. How is information provided by informants recorded? Is an informant's real identity kept secret?

I. Are there document shredding machines or confidential waste sacks for the disposal of sensitive information?

J. For what is police information and intelligence used? Is it used for:
   - Checking the status of someone stopped on the street?
   - Identifying a suspect?
   - Locating a suspect through known associates?

K. Is it also used for:
   - Identifying prominent criminals or trends in criminal offences?
   - Identifying appropriate subjects for proactive operations?
   - Identifying priorities for the allocation of resources?

L. Are the identities of the most prominent local criminals and their associates made known to officers, especially those on routine patrol? How? Are their photographs on display or otherwise disseminated to officers? Are officers encouraged to submit any sightings or other information about these criminals? How is this done? Do they receive training on what to look for and how to report it?

M. Where available, how do officers access information related to:
   - Crime reports?
   - Criminal records?
   - Fingerprints?
   - Modus operandi?
   - Vehicle ownership?
   - Residence?
   - Warrants for arrest?
   - Other court orders?

N. How quickly can such information be obtained?

O. What arrangements are in place to request information from other agencies or organisations? How does this work? How long does it take? Do officers tend to use informal personal networks to obtain such information? Why?

P. Do local officers employ covert techniques for obtaining information (such as telephone interception or listening devices)? Is the equipment to do this available locally? What permissions are needed? What are the limits on the uses of these techniques? How long does it take?

Q. Can local investigators acquire telephone subscriber information? How? What permissions are needed? How long does it take?

R. Is current and developing criminal behaviour brought to the attention of local officers? How? Do officers receive regular briefings on crime and criminals in their area? How? Are these briefings used to direct routine police patrols? How?

S. Is there anyone tasked with reviewing all available information in order to identify trends or common characteristics in criminals or criminal behaviour? If yes, has that person received any formal training in analysis? Does that person conduct his or her research using computers or manually? What sources of information or data are available to him or her? Are there any sources of information to which this person believes he or she needs access, but does not have?

T. Are statistics from crime reports gathered and collated? Who does this? How are the statistics presented? To whom are they given?

U. Is crime activity in the area plotted and visually displayed on any maps? Is this done electronically or manually? What information do the maps show?

V. Where a central or national agency or registry exists for police information and intelligence, how is local information forwarded to it? What are the criteria for such submissions? Who decides whether it should be forwarded?

W. Where analysts are employed, on what basis does an analyst start a research project? Is he or she given specific terms of reference? How does that person document or report the results of his or her research? Are standard formats used? To whom are the results given? For what are they used?

X. Are strategic documents produced that examine how much and what kinds of crime are committed and how this impacts on the local community? Do such documents identify areas that need additional police attention? Are they submitted to a central point for collation and amalgamation with similar documents from other areas? Are they then used to compile a strategic national overview of criminal activity?

Y. On what basis do local police commanders allocate their resources? Are local crime patterns considered as part of the decision-making process? On what basis do local police commanders request additional resources from their superiors? Do they use evidence from local research in support of their requests?

7. PARTNERSHIPS AND COORDINATION

7.1 PARTNERSHIPS

While the police have considerable opportunities for gathering and collecting information and intelligence, there are also large stores of data held by other public and private interests all of which have a potential value for police purposes. Working in partnership with others increases the number of potential sources of information. Indeed, there may be situations in which a partner agency is the only possible source of a particular item of information.

Law enforcement officers often feel more comfortable when exchanging information through personal informal networks. It is often the case that informal contact is faster and more efficient. However, there are inherent dangers is obtaining information without the safeguards, checks and balances in the formal procedure – not least of which is the question of admissibility of the information in court. An effective and properly functioning mechanism for exchanging information (especially across borders) gives less cause for an investigator to "call a friend" and allows that officer to act with confidence on the basis of information received.

However, it is not always easy to establish partnerships with other agencies either at home or abroad. Sometimes this is because there are legal constraints restricting the sharing of data (especially personal data), or because of concerns about security. There will also be times when potential partners have different organisational objectives or agenda.

A. How do law enforcement agencies or organisations share information and intelligence? Does this happen formally or informally or both? How is information shared? Are common standards used in terms of evaluation and formatting of the information provided?

B. What kinds of information are shared? Is information of potential interest forwarded to partners automatically? Do joint investigations occur? How often?

C. Is the information and intelligence stored in state prosecutor databases available for police investigators? Do state prosecutors have access to data stored in police databases?

D. Do the police seek information and intelligence from other non-law enforcement agencies such as prisons, banks and the tax authorities? Are there protocols in place to allow this to happen? How does this system work? How often are requests made? How often are the requests fully answered? How long does it take?

E. Is there some form of regular joint meeting between organisations to discuss general strategic or specific tactical criminal intelligence assessments? How often? Who is involved? Are there notes of these meetings? What are the outcomes?

F. In a post-conflict situation, is there any joint intelligence-sharing protocol with the peacekeeping forces?

G. Are there protocols in place for exchanging data bilaterally with other countries or international organisations, such as Interpol? Which countries or organisations are involved? Is authority required from a senior officer, prosecutor or judge before this can be done? Are there limits on the types of information that can be shared? If so, what are they?

H. Can this been done directly or is a formal Letter of Request (Rogatory Letter) required? Do officers know how to make such a request? Is there a central office or bureau that deals with such requests? How long, on average, do requests take to answer?

I. Are police liaison officers posted to other countries? How were these countries chosen? Do the duties of police liaison officers include building contacts for the exchange of information and intelligence?

J. Is the country a member of any regional law enforcement sharing body, e.g. ASEAN, SECI, CARICC? What are the national obligations and privileges in respect of that body? How does the country interact with that organisation and the other members of it? How much information and intelligence is received from it? How much information and intelligence is sent to it?

K. Can data be entered and searched in international databases, such as Interpol's DNA database? Can this be done directly and in real time via secured telecommunication systems, such as Interpol's I-24/7? If so, which law-enforcement agencies have direct access to these telecommunication systems? If not, how is data entered and searched in the international databases? How long does this take?

7.2 DONOR COORDINATION

Being aware of the activities of donors in the areas of crime investigation as well as the development of police information and intelligence systems will prevent unnecessary duplication and allow coordination of initiatives.

A. Are there (or have there been) internationally funded initiatives aimed at developing police information and intelligence? What are the objectives of these projects? Are they being achieved? Is there evidence of duplication? Is the implementation of these initiatives being coordinated? Are mechanisms in place that will ensure the sustainability of any sponsored activity? Which countries or organisations are involved? What mentoring mechanisms are there in place? Are any stakeholders and/or donors obvious by their absence?

B. Do (or did) these initiatives offer training? If so, are they training trainers (to deliver cascade training programmes) or are they focusing on individuals? Is a system of computer-based training being offered? Was a training needs assessment conducted in advance of these programmes? Are any of those identified needs still to be addressed?

C. Do (or did) these initiatives provide equipment? If so, was the need for this equipment identified through an independent evaluation or was it the result of a government list? Are other donors providing the same or similar equipment? Are there plans for how the equipment will be maintained and replaced? Are there examples of the same or similar equipment being provided and then being misappropriated or not being used at all?

D. Where information systems are being provided, was a user requirement prepared? Who prepared it? Does (or will) the system fulfil this requirement? Will the system be scalable, i.e. can it be expanded in the light of increased future need? Who owns the source code?

E. In respect of these initiatives were any post-implementation reviews conducted that may have helped to identify good practice for replication elsewhere? Are the results of such initiatives collated and coordinated to inform future planning?

ANNEX A. KEY DOCUMENTS

UNITED NATIONS

- Convention against Transnational Organised Crime (UNTOC), (2000) and its related protocols on Trafficking in Persons, Smuggling in Persons and the Illicit Manufacture of Firearms and Ammunition (outlining important investigatory measures when tackling serious and organised crime);
- Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment
- Convention against Corruption
- Single Convention on Narcotic Drugs
- Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances
- Convention on Psychotropic Drugs
- The Compendium of United Nations Standards and Norms in Crime Prevention and Criminal Justice, 2006, which contains source documents on crime prevention and criminal justice, and Human Rights texts including:
  - Declaration on the Protection of All Persons from Being Subjected to Torture and other Cruel, Inhuman or Degrading Treatment or Punishment, 1975.
  - Minimum Rules for Non-Custodial Measures (Tokyo Rules).
  - Basic Principles on the Role of Lawyers
  - Guidelines on the Role of Prosecutors
  - United Nations Standards Minimum Rules for the Administration of Juvenile Justice (Beijing Rules).
  - Code of Conduct for Law Enforcement Officials
  - Rules for the Protection of Juveniles Deprived of Their Liberty.
  - Declaration of Basic Principles of Justice for Victims of Crime and Abuse of Power
  - Guidelines for Child Victims and Witnesses
  - Declaration on the Elimination of Violence against Women
  - Declaration on the Protection of All Persons from Enforced Disappearance
  - Declaration on the Rights of the Child
  - Standard Minimum Rules for the Administration of Juvenile Justice

- United Nations Survey of Crime Trends and the Operation of Criminal Justice Systems

DRAFT

- Model Police Act
- Model Code of Criminal Procedure
- Model Criminal Code

PLEASE NOTE: *The Model Police Act (MPA), the Model Code of Criminal Procedure (MCCP), and the Model Criminal Code (MCC) are being cited as models of codes that fully integrate international standards and norms. At the time of publication, the MPA, the MCCP, and the MCC were still in DRAFT form and were being finalised. Assessors wishing to cite the MPA, the MCCP, and the MCC with accuracy should check the following websites to determine whether the finalised Codes have been issued and to obtain the finalised text, as referenced Articles or their numbers may have been added, deleted, moved, or changed:*

http://www.usip.org/ruleoflaw/index.html

or http://www.nuigalway.ie/human_rights/Projects/model_codes.html.

The electronic version of the Criminal Justice Assessment Toolkit will be updated upon the issuance of the finalized codes.

REGIONAL

- Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (1981), Council of Europe
- Recommendation R(87)15 on regulating the use of personal data in the police sector (1987) Committee of Ministers of Council of Europe

- Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and trans-border data flows (2001) Council of Europe
- Proposal for a Council Framework Decision on the exchange of personal data processed in the course of the activities of police and judicial cooperation (2005) European Commission (www.statewatch.org/news/2005/sep/com-data-protection-prop)

OTHER USEFUL SOURCES

- Ainsworth, P.B. (2001)"Offender Profiling and Crime Analysis" Willan Publishing
- Brown, S.D. (2006) "Criminal Intelligence: Data Prospecting or Seeking Significance". International Association of Law Enforcement Intelligence Analysts (IALEIA) Journal No 17 vol. 1
- Bruce, C.W. Hick, S.R. & Cooper, J.P. (Eds) (2004) "Exploring Crime Analysis" IACA Press
- Dixon, T (2003) "Intelligence Management Model for Europe: Guidelines for standards and best practice within the analysis function" (www.tulliallan,police.uk)
- IACA, (2004) "Exploring Crime Analysis: Readings on Essential Skills" International Association of Crime Analysts
- Law Enforcement Analytic Standards (2004) U.S. Dept of Justice and IALEIA (it.ojp.gov/documents/law_enforcement_analytic_standards)
- Ratcliffe, J.H. (2003) "Intelligence-led Policing" Australian Institute of Criminology: Trends and Issues in crime and Criminal Justice No 248 (www.aic.gov.au)
- Ratcliffe, J.H (Ed.) (2004) "Strategic Thinking in Criminal Intelligence" Federation Press
- Peterson, M.B. Morehouse, R & Wright, R (Eds) (2000) "Intelligence 2000: Revising the Basics" LEIU & IALEIA

NATIONAL

- Criminal Code
- Criminal Procedure Code
- Other sources of criminal law
- Standard operating procedure, implementing/clarifying regulations
- Police training manuals and course materials

ANNEX B. ASSESSOR'S GUIDE / CHECKLIST

The following table is designed to assist the assessor in keeping track of what topics have been covered, with what sources, and with whom.

	TOPIC	SOURCES	CONTACTS	COMPLETED
2.1	STATISTICAL OVERVIEW	• Ministry of Interior Reports • Ministry of Justice Reports • Ministerial Websites • National & local Crime Statistics • NGO Reports • UN Regional & Country Analyses	• Any Office of National Statistics	
3.1	LEGAL AND REGULATORY FRAMEWORK	• Government department such as the Ministry of Justice or Ministry of the Interior; • Government websites (especially for police) • Police agency's publicity literature • The internet can be a valuable source of national legislation (e.g. www.wings.buffalo.edu/law/bclc/resource); • Global Legal Information Network www.glin.gov • www.interpol.org	• Government Minister responsible for Justice and/or Internal Affairs; • Representative from the government's legislative drafting department; • State Prosecutor, Attorney General or Director of Public Prosecution; • Policing agency's legal department • Representative of local criminal bar association • Head of criminal intelligence agency; • Head of national security agency	

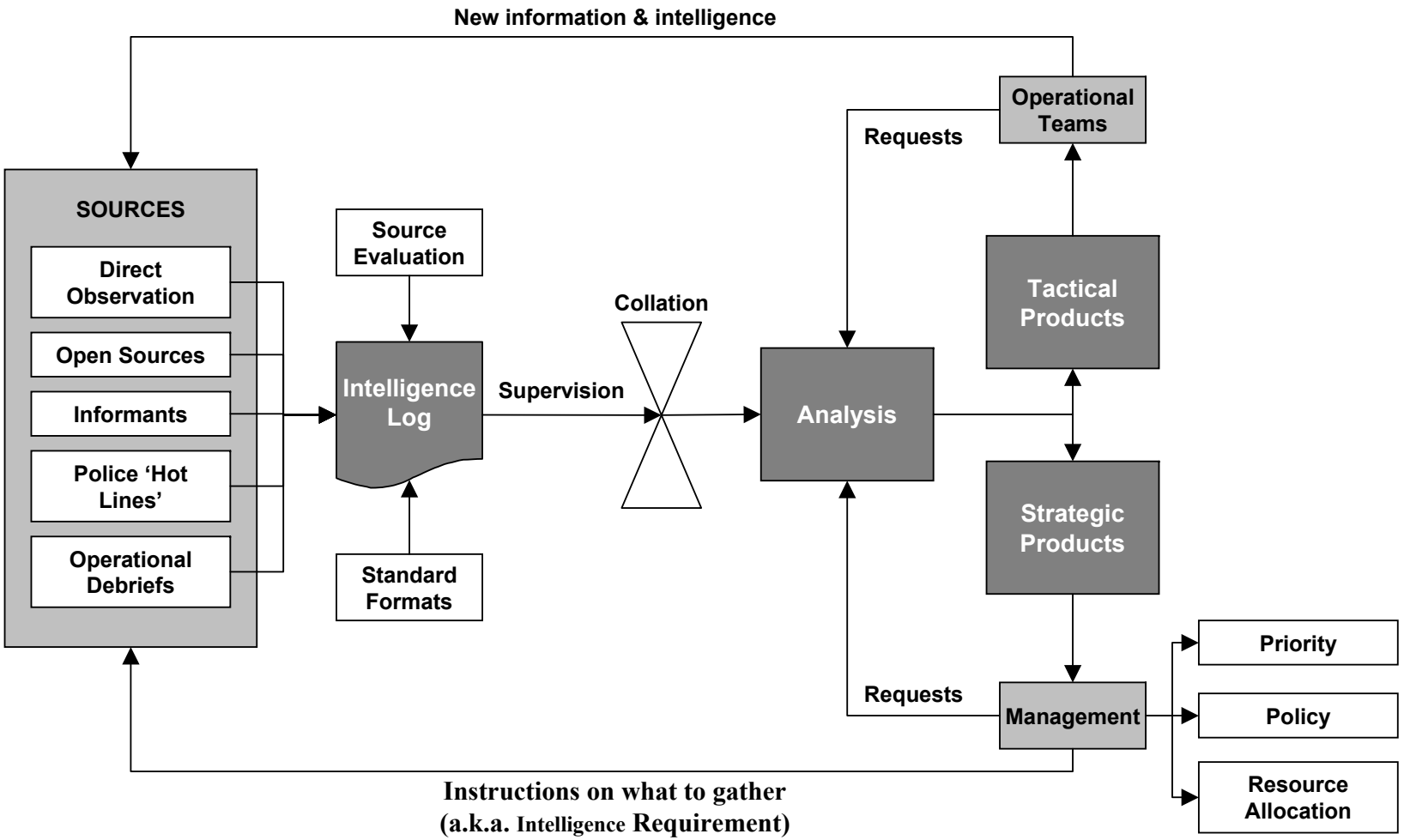
	TOPIC	SOURCES	CONTACTS	COMPLETED
4.1	POLICY	• Manuals of guidance on criminal intelligence/information; • Standard operating procedures policy/guidance on criminal intelligence/information gathering, analysis and dissemination; • Inspection reports by external organisation(s); • Guidance/rules on the security of intelligence and information;	• Government Minister responsible for tackling crime – possibly Minister of Justice or Interior; • Senior civil servants; • Head of criminal intelligence agency; • Head of national security agency; • National or regional Prosecutor; • Judges of criminal cases; • Police Inspectorate or oversight/accountability body; • Researchers/academics who focus upon crime, human rights issues; • Senior crime managers; • Senior crime intelligence managers • Leaders of law enforcement agencies; • Representatives of a police board or oversight committee; • Head of criminal intelligence organisation; • Local police commanders; • Head of local criminal intelligence unit; • Senior officers in charge of crime investigators; • Intelligence officers; • Crime investigators/Detectives; • Analysts; • Informant handlers; • Surveillance operatives; • Trainers; • Patrol officers • Representatives of the public (an oversight committee, local councillors); • Researchers in crime investigation and intelligence issues. • Independent human rights/civil liberty/anti corruption groups; • Journalists (international, national or local, specialising in crime issues).	
4.2	INSTITUTIONS	• Organisation chart of national police responsibilities • Charter or legislation setting up a criminal intelligence organisation • Policy and standards for information and intelligence handling and security • Relevant training manuals • •	• Chief of police • Head of criminal intelligence agency; • Head of national security agency; • National or regional Prosecutor; • Judges of criminal cases; • Police Inspectorate or oversight/accountability body;; • Senior crime managers; • Senior crime intelligence managers • Representatives of a police board or oversight committee; • Local police commanders; • Head of local criminal intelligence unit; • Intelligence officers; • Patrol officers	

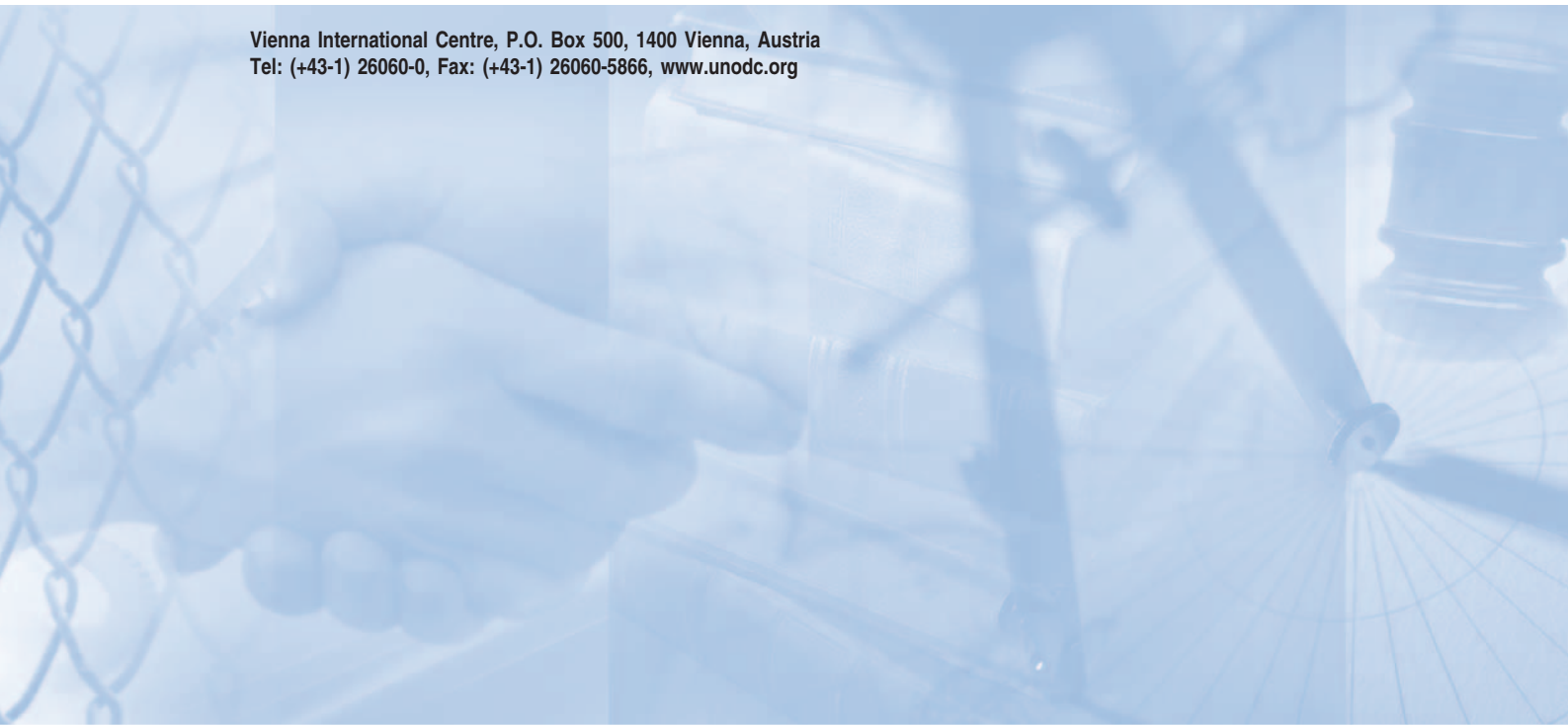
	TOPIC	SOURCES	CONTACTS	COMPLETED
4.3	STAFFING	• Security vetting and clearance criteria • Analyst and intelligence officer job descriptions and selection criteria; • Training programmes for analysts & other staff (particularly managers), • Visit intelligence unit(s) in relevant organisations. • Guidance on the selection of staff for criminal intelligence activities (in their broadest sense); • Programmes for training of staff involved in criminal intelligence activities	• Head of police personnel, recruitment and promotion department; • Head of Police Training • Person in charge of staff security vetting • Analysts • Police staff working with information and intelligence	
4.4	INFORMATION & INTELLIGENCE SYSTEMS	• User requirement • Available databases • Storage & retrieval systems for paper records (especially fingerprints & photographs) • Data model & architecture • Protocols on information security • inspection of computer • Inspection of server rooms • Database performance reports	• Chief Information Officer for law enforcement • Any IT consultant employed by the police; • Any officer who uses the databases • Officers or staff who populate the system(s) • Any information security officer • Any data protection officers • Representative from any privacy or data protection body. • Analysts • Trainers	

	TOPIC	SOURCES	CONTACTS	COMPLETED
5.1	COLLECTION 5.1.1Primary Sources 5.1.2 Covert Surveillance 5.1.3 Informants 5.1.4 Widening the net	• Analyst and intelligence officer job descriptions; • Training programmes for analysts,; • Databases available to investigators; • Programmes of training for investigators; • Manuals of guidance on criminal intelligence/information; • Standard operating procedure policy/guidance on criminal intelligence/information gathering, analysis and dissemination; • Guidance on the use and supervision of informants, surveillance and other sensitive policing techniques; • Guidance/rules on the security of intelligence and information; • Programmes for training of staff involved in criminal intelligence activities • Selection of strategic criminal intelligence assessment reports; • Examples of local strategic and tactical criminal intelligence assessments or reports; • Notes or minutes of meetings where intelligence material has been used to make decisions (tasking and coordination, deployment and operational meetings); • Databases available to intelligence units and other staff; • Open source access • Examples of forms or templates (electronic and paper) used for collecting or disseminating information/intelligence • Visit intelligence unit(s) in relevant organisations.	• Head of criminal intelligence agency; • Head of national security agency; • Independent human rights/civil liberty/anti corruption groups; • National or regional Prosecutor; • Judges of criminal cases; • Senior police officers with responsibility for crime investigation and criminal intelligence; • Journalists (international, national or local, specialising in crime issues). • Leaders of law enforcement agencies charged with the criminal intelligence function; • Head of crime investigation department; • Head of criminal intelligence unit; • Local police commander; • Rank and file staff (analysts, informant supervisors and handlers, detectives); • NGO researchers; • Head of police personnel, recruitment and promotion department; • Heads of law enforcement agencies (such as police, customs, border guards); • Local police commanders; • Head of local criminal intelligence unit; • Senior officers in charge of crime • Head of any information management department	
5.2	EVALUATION	• Intelligence logs and information • Guidance on applying evaluation	• Rank and file staff (analysts, informant supervisors and handlers, detectives); • Officer responsible for supervising intelligence logs;	
5.3	COLLATION	• Systems of filing • Data model used • Software in terms of data mining and case management systems • Test or training platforms	• Any intelligence manager • Persons responsible for collation • Persons responsible for monitoring and supervising intelligence logs and data input	
5.4	ANALYSIS	• Analysts software suppliers; • Examples of forms (electronic and paper) used for collecting or disseminating information/intelligence; • Samples of link charts; • Samples of hot-spot maps.	• Head of police training department. • Head of criminal intelligence organisation; • Principal Analyst; • Analysts.	

	TOPIC	SOURCES	CONTACTS	COMPLETED
5.5	DISSEMINATION	• Examples of daily or other briefings to operational teams and police managers; • Samples of strategic threat assessments, tactical reports and other analyses. •	• Strategic police managers; • Operational Police managers; • Prosecutors and/or investigation managers; • Patrol officers; • Representatives of 3rd party law enforcement agencies.	
5.6	DIRECTION	• Notes or minutes of meetings where intelligence material has been used to make decisions (tasking and coordination, deployment and operational meetings); • Any instructions issued on what kind of information or intelligence to collect or terms of reference for an analytical report • Any instructions on what intelligence is needed/ analytical terms of reference (i.e. “intelligence requirement”) produced	• Strategic police managers; • Operational Police managers; • Prosecutors and/or investigation managers; • Head of criminal intelligence agency; • Head of national security agency; • Independent human rights/civil liberty/anti corruption groups; • National or regional Prosecutor; • Judges of criminal cases; • Senior police officers with responsibility for crime investigation and criminal intelligence; • Leaders of law enforcement agencies with responsibility for criminal intelligence function.	
6	LOCAL USE OF INFORMATION AND INTELLIGENCE	• Visit to local intelligence unit or collators office • Any reports or analyses produced • Any briefing materials on local crime patterns • Any proactive operation plans or proposals • Any instructions on what intelligence is needed/ analytical terms of reference	• Local police commander • Local manager of investigators • Patrol officers • Person in charge of collating information • Any local analyst • Any staff member compiling crime statistics	
7.1	PARTNERSHIPS	• Written protocols or directions requiring inter agency working; • Manuals of Guidance/Standard Operating Procedures; • Notes of meetings between criminal intelligence and crime investigation agencies and/or with prosecutors; and with other agencies; • Memoranda of Understanding or service level agreements •	• Head of criminal intelligence agency or unit; • Head of crime investigation agency/department; • Head of Customs, Border Guard or specialist law enforcement agency (anti money laundering, counter corruption unit etc); • Criminal intelligence operatives; • Crime Investigation Supervisors and Investigators; • Prosecutor; • Analyst; • Interpol and any regional police organisation;	
7.2	DONOR COORDINATION	• Internet Websites • Programme and project documents; • Project terms of reference; • Public brochures and literature; • Regional organisation offices • Memoranda of Understanding with international community, organisations or donor countries (e.g. UN, European Commission, OSCE, ASEAN, Interpol etc) • International and Regional organisations, • Embassies/Ministries	• Senior police managers • Local representatives of other international initiatives (particularly foreign law enforcement liaison officers). • Representatives of relevant international or regional organisations working in the country; • Embassies/Ministries for donor activity. • Programme and project managers for international initiatives • Local UN representative • Local representatives of other international/regional organisations • Embassies (especially foreign law enforcement liaison officers).	

BASIC INFORMATION FLOW





UNITED NATIONS
Office on Drugs and Crime

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

Printed in Austria
V.06-58030—November 2006—1,000

back to first page