CHAPTER 5:
INTELLIGENCE METHODOLOGIES OF LAW ENFORCEMENT AND POSITIVE INTELLIGENCE: COMMON GROUND

1. INTRODUCTION

In the previous chapter an example was given of policy developed not to be involved in extralegal actions initiated by another country, such as rendition which is unacceptable in many legal systems. Such controversial responses to international crime do not provide a proper basis for intelligence cooperation. Until well into the 1960's there was a strong feeling of resistance, even amongst the police in many countries in Europe against the use of undercover tactics by law enforcement agents, as well as an apathy to police reliance on informants and non-police agents (Nadelmann, 1993: 225). The methodology of respectively law enforcement (special investigative techniques), and positive intelligence practices are analysed in this chapter. The common areas, upon which cooperation between law enforcement and positive intelligence could be based, are identified.

As has been pointed out in Chapter 2, there are various responses to international crime, namely law enforcement, that is prevention or investigation of crime with a view to criminal prosecution or actions such as asset forfeiture or the freezing of assets (in the case of suspected terrorist funds); military responses; intelligence responses; and joint responses which may include elements of law enforcement; military and civilian intelligence. Military responses and covert action, whether undertaken by the military or civilian intelligence are sometimes counter-productive and as shown in the previous chapter may negatively impact

on sovereignty and eventually even on existing levels of cooperation. The ideal seems to be to focus on law enforcement, but to find common ground where intelligence assistance from positive intelligence is utilised maximally in support of law enforcement. From the international obligations in respect of the combating of organised crime and terrorism (Chapter 3), it is clear that international cooperation in respect of special investigative techniques are required in order to effectively prevent international crimes and to investigate those crimes with a view to successful prosecution. Hereunder particular attention is given to the law enforcement response to international crime, which includes the investigation of international crime; measures to prevent those crimes as well as the enforcement of laws pertaining to immigration and customs as part of crime prevention.

2. INTELLIGENCE METHODOLOGY OF LAW ENFORCEMENT

In the previous chapter, differences in the organisational culture and other differences, such as focus, between law enforcement intelligence and positive (mostly civilian) intelligence were analysed. It is also necessary, in order to determine the most likely areas of cooperation between law enforcement intelligence and positive intelligence, to compare the methodologies respectively used.

2.1. Law enforcement methodology to investigate crime

The main law enforcement response is the detection and investigation of crimes that have been, or are in the process of being committed. Normal policing methods are part and parcel of every police investigation, also in respect of international crime. The nature of international crime involving political and jurisdictional issues and planned and executed by criminal groups or enterprises in addition, however, also requires highly specialised methods to be employed for effective investigation and prevention. Special investigative techniques,

sometimes referred to as 'special investigative tools' may be used both to investigate crimes already committed, or crimes which are in the process of being planned or committed, thus for crime prevention.

2.1.1. Special investigative techniques

The realisation that the use of traditional investigative methods to investigate transnational organised crime is very difficult and ineffective, called for the use of special investigative tools or techniques (UNAFEI, 2001(a): 228). Traditional techniques of crime investigation had to be adapted in order to cope with "increasing complexity of terrorist networks, which are often connected with other forms of serious crime, such as organised crime or drug trafficking" (De Koster, 2005: 5). Special investigative techniques are aimed at the systematic and surreptitious (without alerting the suspect) gathering of information by law enforcement officials to detect and investigate crimes and suspects (De Koster, 2005: 5). Until recently, one of the problems experienced with the use of special investigative techniques, was that in many countries there was simply no legislative sanction or empowerment of law enforcement to use those techniques, although in most countries they were also not explicitly prohibited (UNAFEI, 2001(a): 230). That this situation has largely changed in Europe is clear from the analysis made for the Council of Europe of legislation dealing with special investigative techniques, not only in Europe, but also the US and Canada (De Koster, 2005). Replies received to questionnaires sent by the EU to the countries involved showed that the main special investigative techniques are used basically everywhere in the EU countries as well as the US, and Canada which were included in the study.

There are no particular differences in respect of the use of such special investigative techniques between EU Member States. The Netherlands and Belgium were identified as countries using the "full panoply of such techniques" (De Koster, 2005: 16). The 1988 *UN Convention on Narcotic Drugs and Psychotropic Substances* and the *UN Convention against Transnational*

Organized Crime both oblige States Parties of the UN to provide for the use of special investigative techniques in their domestic legal systems and identify the following special investigative techniques: controlled delivery, surveillance, including electronic surveillance and undercover operations. These special investigative techniques are discussed in more detail hereunder, with specific reference to intelligence cooperation on national and international level. As a result of the intrusive nature of special investigative techniques, they should be regulated by law, empowering law enforcement to apply such techniques when there is sufficient reason to believe that an offence has been committed, or is being planned or preparations made for the commission thereof by persons whether yet identified or not. Further legal requirements are that less intrusive measures must be unavailable or exhausted before such techniques are applied; there must be proportionality: the need to use the technique for the public good needs to override the intrusion of the individual to privacy; and there must be a measure of judicial or similar independent control (De Koster, 2005: 20, 21). In order to identify supportive roles for positive intelligence towards law enforcement, it is necessary to describe the respective techniques in some detail, as well as to reflect on the common problems and solutions in respect thereof.

De Koster describes different categories of secret criminal investigation procedures, with or without interaction with suspected offenders or criminal organisations and deception. Examples under these categories include the use of informants; monitoring (surveillance) of individuals by tailing, observing, photographing and filming, tapping or monitoring of telecommunications and the opening of mail; undercover operations by an investigator or a person (agent) who conceals his or her identity, appointed by the police and who interacts with suspected offenders and gathers evidence and information through deception-infiltration and ‘front-store’ operations; and traps and enticement, enabling the commission of an offence to be observed or to gather evidence (2005: 15). The first special investigative technique is ‘controlled delivery’.

2.1.1.1. The technique of controlled delivery

Controlled delivery can be regarded as a type of undercover operation. It is, however, unique and quite distinguishable from other types of undercover operations and therefore dealt with separately. This technique is one of the most effective investigative tools and indispensable in fighting transnational organised crime, in particular illegal trafficking of different commodities including drugs and firearms (UNAFEI, 2001(a): 228). Controlled delivery is defined as follows: "the technique of allowing illicit or suspect consignments to pass out of, through or into the territory of one or more states, with the knowledge and under the supervision of their competent authorities, with a view to the investigation of an offence and the identification of persons involved in the commission of the offence" (UN, 2004: 6). In many instances when a consignment of drugs or other contraband is found in transit, it is simply confiscated. The technique of controlled delivery is used to bring to justice also the organisers and principals involved in illicit trafficking (Cutting, 1983: 15). Controlled deliveries are referred to as 'internal' when the delivery is in the same country as where the detection took place; 'external' when the destination is another country as that where detection took place; and a 'clean delivery', if circumstances allow the substitution of the drugs with another substance.

Contraband concealed in unaccompanied consignments of goods, unaccompanied luggage or parcel post presents the best opportunities for controlled delivery (Cutting, 1983: 17). It is important to keep the detection secret and to ensure the security of the contraband at all times to avoid it being intercepted along the route by the smugglers. Clean controlled deliveries are preferred as it reduces this risk. If a clean controlled delivery is not possible, more surveillance might be required, even if it could increase the risk of detection. Documentation in respect of the delivery provides useful information as about the consignee to organise the controlled delivery and to ensure the normal route is followed (the smugglers often do a trial-run to establish and monitor

procedures). Surveillance (including photo/video surveillance) in respect of the address for delivery and the consignment is essential for evidential purposes. The cooperation of the freight or postal service needs to be obtained in order to ensure that there is no indication of the fact that it is a controlled delivery. It is important that there is no suspicious delay in the delivery schedule as a result of the controlled delivery (Cutting, 1983: 19).

With external controlled deliveries of unaccompanied consignments early dialogue between the law enforcement authorities in respectively the countries of detection and intended delivery is essential. The following factors must be considered: (Cutting, 1983: 20)

— Relevant legal provisions in all countries involved;
— sufficient time to develop a joint plan of action with all role-players in the countries involved;
— the availability of sufficient control and surveillance and adequate communications facilities between the authorities; and
— whether it would be possible to identify the principals and organisers in the country of destination and balancing the benefits with the resources required to execute a controlled delivery.

It is difficult to perform a controlled delivery in respect of accompanied consignments, but possible in respect of 'hold luggage' of air passengers on high risk routes, if there is sufficient cooperation between the law enforcement agency and airline personnel to link passengers with luggage in which drugs was found. The same factors as mentioned above are relevant in such controlled delivery (Cutting, 1983: 22). The application of the technique of controlled delivery is complicated, especially in the case of external controlled delivery. Lessons learnt from particular experiences indicate that the success of controlled delivery "hinges upon domestic cooperation and coordination among law enforcement agencies, as well as international cooperation and coordination" (UNAFEI, 2001(a): 231). The need has been identified for a system in the law enforcement

agency in each country to exchange intelligence and information to be shared and coordinated in order to be able to establish multi-agency task forces when required. The intelligence and information units should double-up as contact point for international mutual assistance. New technologies must be developed and employed to reinforce the use of controlled delivery, such as sophisticated monitoring devices (tracing transmitters, response senders and receivers, thermo-imaging cameras, etc.) (UNAFEI, 2001(a): 231).

Controlled delivery has been successfully used in the investigation of crimes such as money-laundering; drug trafficking; illegal firearms; stolen property trafficking and human trafficking (UNAFEI, 2001(b): 468). The use of controlled delivery requires skill, professionalism and team work. The economic and technological gap between developed and developing countries and the lack of resources such as skilled personnel and modern investigation equipment for evidence collection affects the application of controlled delivery (UNAFEI, 2001(b): 468).

Positive intelligence agencies may possibly assist with controlled delivery by providing information on addressees of seized consignments, within the time limits available to perform a controlled delivery. Positive intelligence may also assist with technologically advanced equipment to monitor the consignments during a controlled delivery to ensure that it remains under control, especially with controlled delivery of firearms. Furthermore, intelligence assistance from customs authorities to profile and identify suspect consignments which may offer opportunities for controlled delivery is important. In respect of surveillance, positive intelligence may assist with it, but it is preferable that surveillance during delivery should be performed by law enforcement agents as the results of such surveillance would need to be tendered in court, taking into account that the whole chain of events need to be proven in court.

The advances in border control, in particular the development of e-borders in the UK has boosted law enforcement and provide huge volumes of intelligence on the movement of persons. One of the advantages thereof is the possibility to profile high and low risk passengers and intelligence agencies to have access at all times of passenger data (Privacy International, 2005: 2). This system therefore could be invaluable in respect of courier accompanied consignments, as discussed above. The issue of 'e-borders' in the UK will be referred to in more detail in the analysis of surveillance. The most recent recommendations of the UN in respect of the improvement of international cooperation to combat money-laundering and various other forms of organised crime, include the following: (UN, 2008(g): 12)

— Maintaining timely and clear communications amongst central authorities and attention to regular consultations with states that have a high volume of requests for assistance and prior consultation in respect of time-sensitive cases;
— the consideration by Member States of common practices and procedures to enhance mutual legal assistance, extradition and controlled delivery capacity where there are different legal systems involved;
— the institutionalisation of the sharing of information between Member States (between source, transit and destination countries and intergovernmental organisations); and
— states situated along major drug trafficking routes should consider establishing joint investigations and teams of law enforcement officers dealing with drug trafficking and organised crime.

Other forms of undercover operations also need to be described in detail, in order to determine their relevance in respect of intelligence cooperation.

2.1.1.2. Other undercover operations/techniques

These techniques inherently involve an element of deception and may require cooperation with persons whose motivation and conduct are questionable. The use of such techniques therefore needs to be carefully considered and monitored (UNAFEI, 2001(a): 232). Furthermore, agents or informants used in undercover operations may be expected to become involved in criminal activities themselves. The use of undercover operations may amplify crime in many possible ways by, for example, generating a market for the purchase or sale of illegal goods or services and generate capital for another illegality; it may coerce, trick or persuade a person not otherwise predisposed to commit the offence; it may generate a covert opportunity structure for the agent to commit crime; and it may lead to retaliations against informants (Choo & Mellors, 1995: 4). Undercover operations may vary in nature from a very short duration to lasting a number of years; directed at a single crime or a whole criminal enterprise; the mere buying or selling of illegal drugs, property or firearms; or the operation of an undercover business (Ohr, 2001: 48). Undercover operations enable law enforcement agencies to infiltrate the highest levels of organised crime groups by “posing as criminals when real criminals discuss their plans and seek assistance in committing crimes”. This method is extremely dangerous as it puts the life of the agent at risk should he or she be exposed (UNAFEI, 2001(a): 232, 233).

Common problems that have been identified in respect of undercover operations are as follows: (UNAFEI, 2001(a): 234, 235)

— Criminal groups expect new members to undergo unlawful ‘tests of innocence’ by requiring them to commit criminal acts. This is especially problematic where the agent is expected to commit an act of violence against any person: In the US the undercover operation must be terminated if a crime of violence is imminent, whether the undercover agent is required to perform such act or not, if the crime cannot be

stopped in another manner, such as warning the victim, or the arrest of the suspects who pose the threat.

— The stress to handle a full time pretence and danger of exposure (monitoring and full-time back-up is required).

— The refusal of some countries to use this investigative tool, preventing undercover agents to operate in more than one country.

It is important to protect the identity of the undercover agent by means of a fully substantiated past history (called a 'legend' or 'backstopping'); careful briefing concerning the criminal targets; planning for different scenarios that may cause suspicion or hostility towards the agent; and by selecting agents through psychological profiling to ensure they will fit into the cover identity (UNAFEI, 2001(a): 235). In view of different legal systems in various countries; the inherent risk of infringing on fundamental rights and freedoms; and to determine the type of intelligence cooperation that could be provided by positive intelligence to police undercover operations it is necessary to describe the different forms of undercover operations.

a. Undercover operations in the European Union in general

As previously mentioned above legislation in the Netherlands and Belgium reflects all the types of special investigative techniques generally applied in the EU. Belgian law provides for infiltration, described as a police officer, known as an infiltrator, who uses a false identity and who sustains a relationship with persons who are involved or suspected to be involved in crime. In exceptional circumstances and under authorisation of a judge, the infiltrator may also be a private person (De Koster, 2005: 74). Within the framework of infiltration the following 'police investigation techniques' may be used: (De Koster, 2005: 75)

— Pseudo purchase- police officers posing as potential buyers of illicit goods or services;

- trust-winning purchase- to pose as potential buyer of illicit goods, or services in order to gain the vendor's trust or gather further information;
- test purchase- posing as potential purchaser of goods or services (of which transfer actually takes place) to check the vendor's allegations and the authenticity of the goods offered;
- pseudo-sale - posing as a potential vendor of illicit services or goods;
- trust-winning sale posing as a potential vendor of illicit services or goods where the transfer thereof actually takes place, in order to gain the purchaser's trust or to gather information;
- controlled delivery- as described previously, as well as 'assisted controlled delivery' described as allowing the transportation, under constant police control of an illegal consignment of goods that is known to the police, that the police transport themselves, or where they provide assistance, where there is no police intervention at the final destination; and
- front-store operations where the police run one or more businesses, possibly using false identities, and supplying goods and services to the criminal community.

b. Undercover operations in the United States

The Attorney General in the US has issued *The Attorney General's Guidelines on FBI Undercover Operations; The Attorney General's Guidelines regarding the Use of Confidential Informants* and *The Attorney General's Guidelines on General Crimes, Racketeering Enterprise and Terrorism Enterprise Investigations* providing the regulatory framework for the use of undercover operations and informants in the US (US, 2008(d)). The *Attorney General's Guidelines on FBI Undercover Operations* provide for the use of undercover investigative activities involving the use of an assumed name or cover identity by a law enforcement employee working for or with the FBI. When a series of such related undercover activities consist of more than three contacts between the undercover employee

and the individuals who are under investigation, it is referred to as an undercover operation (US, 2002(b): 1). Provision is made for the use of a 'proprietary' or undercover business enterprise, similar to the front-store operations described in respect of the EU. Joint undercover operations between the FBI and other law enforcement agencies are allowed (US, 2002(b): 2).

Sensitive circumstances requiring authorisation by the FBI Headquarters and special measures for review include: (US, 2002(b): 6, 7)

— Investigations into criminal conduct by elected or appointed officials or political candidates for a judicial, legislative, management or executive-level position of trust in all levels of government;
— investigation of any public official or by any foreign official, or government or religious organisation, political organisation, or the news media;
— activities having a significant intrusive effect on the legitimate operation of government on different levels;
— the establishment of an undercover propriety for purposes of the investigation;
— if goods or services reasonably unavailable to the subject of the investigation which are essential for the commission of the crime must be provided;
— commission of felonies by the undercover employee, by law or constitutes serious crime;
— if there is a significant risk of the undercover employee to be arrested;
— if there is a significant risk that a third party will enter into a professional or confidential relationship with a person participating in an undercover operation acting as an attorney, physician, clergyman or member of the news media;
— a significant risk of violence or physical injury to individuals; and
— participation in activities of a group investigated as part of a terrorism enterprise.

Police undercover operations aimed at law enforcement must be clearly distinguished from covert action and clandestine operations. The element of secrecy is common to all three actions. The difference between the concepts lies mainly in the intention with which the action is taken. Covert action is used as means of furthering foreign policy in the national interest. In the case of covert action the option to deny involvement (plausible deniability) is kept open. In other words, the action may be visible, but any possible link or sponsorship between the government and the action is protected by secrecy. In the case of clandestine operations, secrecy needs to be maintained only for a limited time. Both the clandestine action as well as the result thereof is kept secret, but the emphasis is on concealing the action, rather than the sponsorship thereof by government. Covert action is therefore disguised, but not hidden whilst clandestine action is hidden, but not disguised (Van Rensburg 2005: 18-20). Police undercover operations can therefore be regarded more similar to clandestine operations. The confidentiality of undercover operations mostly needs to be maintained for a limited time only, whilst in covert action the identity of participants normally needs to be protected indefinitely. It is common in police undercover operations that the police agent is used as a witness in a subsequent criminal prosecution.

The Attorney General's Guidelines on FBI Undercover Operations further provide that activities that would be regarded as illegal would they not have been part of an undercover operation, need to be justified by being necessary to obtain information towards the success of the operation; to maintain the cover credibility of the undercover employee; or to prevent death or injury. Undercover employees are prohibited from participating in any act of violence, except for self-defence; must avoid unlawful entrapment (enticement); or the use of unlawful investigative techniques, such as unlawful interception of communications ('wiretapping' and mail-opening), breaking and entering, and trespassing which amounts to an illegal search (US, 2002(b): 12).

c. Undercover operations in the United Kingdom

The *Regulation of Investigatory Powers Act 2000 (RIPA)* in the UK provides for the use of clandestine human intelligence sources (CHIS). In terms of the Act the *Covert Human Intelligence Source Code of Practice* had been issued to further regulate the use of covert human intelligence sources (UK, 2002(a)). The Act does not specifically use terms such as informant; agent; front store operation; pseudo purchases and pseudo offences, as in the Belgian legislation, but uses the wide term 'CHIS'. A person is regarded as a CHIS if he or she establishes or maintains a relationship for the purpose of covertly obtaining and disclosing information. The term could include the activities specifically mentioned in the Belgian legislation and referred to above (De Koster, 2005: 475). According to the *CHIS Code of Practice,* authorisation can be granted for the use of a source inside or outside the UK, and also for members of law enforcement or other agencies in the UK in support of domestic and international investigations (UK, 2002(a): 6).

2.1.1.3. Surveillance, including electronic surveillance

Surveillance firstly means the physical surveillance of a suspect by following him or her or to observe over a prolonged period the activities of the suspect. Secondly surveillance includes the interception and or recording of communications by or with suspects. These communications may be oral; it may be through post or courier services or through any electronic means ranging from radio to satellite, telephone, or the Internet. Electronic surveillance is regarded as the single most important law enforcement weapon against organised crime or violent crimes such as terrorism (UNAFEI, 2001(a): 235). The use of the suspect's own words as evidence in a court of law is extremely effective. In addition, the interception/surveillance of communications allows law enforcement to prevent or disrupt the commission of crime. It is recognised that international cooperation, including the exchange of expertise is necessary to use this tool

effectively. A number of factors inhibit the effective use of electronic surveillance, amongst which are the lack of legislation in many jurisdictions to regulate the use of the tool; controversy regarding the use of the tool, sometimes fuelled by the abuse thereof in certain instances even for political purposes; the lack of voice experts; lack of funds to purchase the right equipment; the emergence of new communications technology; lack of cooperation by communications service providers; and the refusal of some countries to cooperate in the application of this tool (UNAFEI, 2001(a): 238. Linked to the surveillance of communications, is the accompanying communications data, namely the information on the communications, such as the numbers, destinations, and duration of calls which may be used in data-mining to identify suspects.

2.1.1.3.1. Surveillance regimes in different jurisdictions

Legislation in the different jurisdictions provide the framework which permits the scope of surveillance powers, as well as the use of surveillance materials for intelligence or evidence, and the sharing or exchange of information relating to surveillance between jurisdictions. The surveillance regimes in the US and the UK respectively are analysed against the background of international intelligence cooperation

a. Surveillance in the US

In the US, law enforcement agencies use *Title III of the Omnibus Crime Control and Safe Streets Act (Wiretap Act) 1968* to perform interception of communications for crime intelligence gathering and use as evidence in court. (US, 1968). Participant monitoring (where a participant to a communication records the communication without the knowledge of the other participant(s), is allowed by law without any further judicial or other authorisation (De Koster, 2005: 492). Interception may only be authorised for certain serious crimes and the intrusiveness of the interception needs to be minimised. Authorisation needs

to be obtained from a court, upon the strength of a statement under oath setting out the details of the crime suspected to have been committed or is in the process of being committed, naming the suspect whose communications are to be intercepted, as well as the facts and information on which the application is based. (De Koster, 2005: 493). There are two separate systems in the US to obtain authorisation respectively for law enforcement and for interception for foreign intelligence gathering (by civilian intelligence agencies) (UK, 2008(b): 38). The latter system (under the *FISA*) is referred to hereunder in more detail under the discussion of methodologies employed by positive intelligence agencies. Simple observation of a suspect is broadly permitted, unless advanced technology is used or the observation done from certain private areas (De Koster, 2005: 492). Authorisation for surveillance can be given for surveillance inside or outside the US, for purposes of court proceedings in the US (UK, 2002(b): 6). Materials obtained through authorised covert surveillance (not electronic surveillance of telephonic communications) may be used as evidence in criminal proceedings (UK, 2002(b): 7).

b. Surveillance in the United Kingdom

General observation by law enforcement officers to prevent and detect crime, maintain public safety and prevent disorder, is not regulated by *RIPA*, even when performed covertly and equipment such as binoculars, cameras or other equipment to merely reinforce sensory perception are used, as long as it does not involve the systematic surveillance of an individual (UK, 2002(b): 5). Provision is made for the authorisation of 'directed surveillance' where non-intrusive covert surveillance is undertaken for the purpose of a particular investigation or operation which may result in the obtaining of private information of an individual. 'Intrusive surveillance' is defined as the covert surveillance in relation to anything that takes place on any residential premises or in any private vehicle and which involves the presence of an individual on the premises or in the vehicle or is carried out by means of a surveillance device (UK, 2002(b): 7,

8). The Secretary of State may authorise the interception of communications upon an application setting out the grounds for the application, the manner of interception, the identification of the targeted person, description of communications to be intercepted; the necessity of the interception; and proportionality. A warrant may be issued in the interests of national security, for purposes of preventing or detecting serious crime; or for purposes of safeguarding the economic well-being of the UK. The procedures are the same for law enforcement and positive intelligence agencies. The dissemination of intercepted material is limited to persons authorised in terms of the warrant, additional persons within the intercepting agency or another agency, who have the necessary security clearance, but still subject to the need-to-know principle and that the person's duties relate to the purpose for which the warrant was obtained (UK, 2002(c): 29).

In the UK provision is made for investigation of protected electronic information. Terrorists and criminals use information security technologies to protect their electronic data and the privacy of their communications (cryptology). This technology is also essential for e-commerce and online business. *RIPA* provides for access to such technology to ensure that the effectiveness of public authorities are not undermined by the use of cryptology to protect electronic information (UK, 2007(c): 6, 7). These powers enable law enforcement to require disclosure of protected information in an intelligible form; disclosure of the means to access protected information; and disclosure of the means of putting protected information into an intelligible form (UK, 2007(c): 8). In practice the authorities are enabled to obtain either the encryption keys or the communications in an intelligible form from telecommunications service providers where the keys are held by them (UK, 2007(c): 16). Communications data which includes 'traffic data' and 'service use information' is invaluable in the investigation of serious crime. Communications data embraces the 'who', 'where' and 'when' of a communication, and not the contents such as images or data (UK, 2007(b): 13).

RIPA provides for access to telecommunications data from postal or telecommunications operators (service providers). Traffic data identifies any person, equipment and location to or from which a communication is or may be transmitted, as well as information of which communication data attaches to which communication (UK, 2007(b): 14, 15).

Traffic data includes information on the origin or destination of a communication, including incoming calls; the location of equipment, such as the location of a mobile phone; information identifying the sender or recipient; routing information identifying the equipment being used; web browsing information; addresses or markings on postal items and online tracking of communications such as postal items and parcels (UK, 2007(b): 15, 16).

2.1.1.3.2. The use of intercepted communications as evidence

In some jurisdictions, such as the US, intercepted communications have been used as evidence in court for decades. In the UK, however, the situation in this regard is anomalous: Intercepts in terms of a UK interception warrant may not be used in a UK court of law, but such material intercepted in a foreign country under the laws of that country may be used as evidence in a UK court of law. Other exceptions to the rule against the use of such material in a court are the recording of a telephone communication by a participant thereto; and the recording of a conversation by a hidden microphone not connected to the telephone (UK, 2008(b): 9). The usefulness of intercepts is confirmed by a report of the UK Serious Organised Crime Agency (SOCA) in stating that electronic interception of telephonic communications is the single most powerful tool for responding to serious and organised crime for the following reasons: (UK, 2008(b): 11)

— The low risk to police officers (in fact in many instances ensuring the safety of police officers);
— the fact that the criminal is not aware of the intercept taking place;

— it can be used quickly and is flexible;
— the relative cost-effectiveness, and the fact that it is less intrusive than covert entry, surveillance or eavesdropping; and
— it can be used both for prevention of serious crimes and as a tool to collect evidence of crimes being committed.

The Privy Council which reviewed the use of intercepts as evidence came to the conclusion that all types of evidence should be used, but pointed out that the use of intercepts as evidence is curtailed by the danger that such use could compromise the capabilities of intelligence agencies and could thus reduce the effectiveness thereof (UK, 2008(b): 13, 14). In the UK there is exceptional good support in the field of the interception of communications between positive intelligence and law enforcement. The positive intelligence agencies in the UK expressed fear that a regime of general use of intercepts as evidence could be harmful to the support of positive intelligence to law enforcement, in view of the potential damage of the exposure of intelligence capabilities (UK, 2008(b): 19).

The Privy Council of Review formulated certain requirements which must be met for intercepts to be used as evidence to be operationally workable: (UK, 2008(b): 23, 24)

— The ability of the intercepting agency to decide whether a prosecution should proceed where intercepted materials are involved;
— limitation of disclosure of intercepted materials to cleared judges, prosecutors, defence lawyers;
— no obligation on the intelligence or law enforcement agency to retain intercepted material for longer than operationally required;
— the standard of transcribing of intercepts to be limited to the objectives (including using as evidence) of the intelligence or law enforcement agency;
— the authority to use intercepts as evidence should not reduce the effectiveness of intelligence and law enforcement agencies to be able to

perform real-time interception in order to disrupt, interdict or prevent terrorist and criminal activity;

— strategic intelligence gained from intercepts should be kept available for as long as required regardless of the progress of criminal cases and that intercepted information may be used for tactical and strategic purposes;

— "Intelligence agencies must be able to support law enforcement by carrying out interception, for 'serious crime' purposes, of targets nominated by law enforcement, and to provide the product or reports on it to those agencies", subject to similar disclosure obligations as other intelligence interceptions;

— the defence in criminal trials shall be denied 'fishing expeditions' as to the use of interception by any agency.

The Privy Council, nevertheless in view of security concerns and to protect interception as investigative tool, recommended that the present legislation, namely not to use intercepts as evidence, should not be amended and that more research should be done before any change be made (UK, 2008(b): 50).

From the above, it is clear that the sharing by positive intelligence of information or materials obtained through clandestine means is inhibited if there is any possibility that such materials might be used as evidence, especially if there is any possibility that the disclosure of such materials may compromise intelligence methodology.

2.2. Other law enforcement methodologies to investigate and prevent international crime

The prevention and combating of crime, including international crimes require measures over and above the application of investigative techniques, such as border control measures and the deployment of police liaison officers, as set out hereunder.

2.2.1. Border control measures

The special investigative techniques referred to above can be used both for crime investigation and prevention. Persons involved in international crime, whether as perpetrators or fugitives need to travel and commodities being illegally trafficked, need to move across borders. Measures to access information on both issues are invaluable for crime prevention, in addition to instances where it can be used to support criminal investigations. Controls are placed at border posts for the enforcement of immigration laws. Electronic surveillance shifted from the targeted use of law enforcement and intelligence agencies' powers of access to passenger information towards a routine and comprehensive capture of almost all data through facilities of carriers of passengers and their obligations to government agencies to have access. The 'e-Borders' system of the UK has as objective to provide the ability to: deny travel; to assess in advance of arrival of passengers the security threats posed by the passenger; to share information between police, security and intelligence agencies and to use passenger information to inform those agencies. It is planned to retain passenger information over a period of time to provide an audit trail and thus to be able to profile passengers (Privacy International, 2005: 3). The scheme includes the use of biometrics, such as scanning the iris of passengers as method of identification (Privacy International, 2005: 1). Of particular significance is that "all travelers and visitors will also be put through a profiling algorithm to discern whether or not they pose a threat as a smuggler, general criminal or terrorist" (Privacy International, 2005: 2).

Technology used at airports include the following: (Reagan, 2006: 25)

— Fingerprints of incoming passengers obtained through a fingerprint scan are run according to the US VISIT programme against an FBI database;

— 'intelligent video software' is used to monitor hundreds of video feeds simultaneously and can alert officials to unattended baggage or security breaches;
— automated luggage scanners process huge numbers of bags;
— backscatter X-ray machines are considered which can scan for high density objects such as plastic explosives, firearms and other metal items;
— detectors used for detection of traces of explosives and narcotics through air particles; and
— the use of high-tech scanners to scan the contents of containers- it can also be detected whether a container had been opened after being sealed for shipping.

2.2.2. Police liaison officers

The internationalisation of crime has led to an increased use of police liaison officers stationed in countries as part of the diplomatic staff at embassies and other foreign missions cooperating on the 'micro level', especially in the fields of terrorism, football hooliganism, organised crime and drug investigations, not only in the EU, but also elsewhere (Benyon, 1994: 503, 504). These liaison officers are placed as Legal Attachés (Legats), in other words, declared agents of the foreign state, with the function to liaise and cooperate with the host country's police services in the combating of crime, especially transnational crime of mutual interest. The DEA and FBI in the US extensively use this system to foster and expand international police cooperation, especially exchange of information. In addition, agents of the FBI and DEA increasingly travel overseas for investigations (Nadelmann, 1993: 150 – 159). As pointed out in Chapter 3 police liaison officers of the EU are placed in INTERPOL and at the EU Commission in Brussels to facilitate cooperation and the exchange of information.

The methodology used by positive intelligence is analysed hereunder.

3. METHODOLOGY USED BY POSITIVE INTELLIGENCE

The statement of Watt that the 'war against terrorism' has moved entirely into the field of intelligence is supported, especially in view thereof that the above methods are all intelligence dependant and intelligence-driven. It is, however, "more akin to police work than that of the military". In the intelligence process individuals need to be identified, their position in the target group needs to be determined, and they need to be located, especially when hiding amongst communities sympathising with them. What is required is coordination of intelligence emanating from various national agencies, centralised in a computer database or archive and a wide as possible sharing of information (Watt, 2002: 295). In the collection of intelligence, there are a number of similarities between the methodology used by law enforcement and positive intelligence, in particular the gathering of HUMINT; COMINT; and technical intelligence. Of importance, however, are differences in the extent, capabilities 'legality' and purpose for which intelligence is being gathered by respectively crime intelligence and positive intelligence agencies. The collection of COMINT and SIGINT by positive intelligence is firstly analysed.

3.1. Communications intelligence and signals intelligence collection by positive intelligence

COMINT collection, and in particular SIGINT collection in the US and the UK are analysed herunder.

3.1.1. Communications intelligence and signals intelligence collection in the United States

The NSA is the main collector of COMINT and SIGINT in the US providing services and products to the US Department of Defense, the IC, government agencies, industry partners, and select allies and coalition partners. These

services relate to cryptology (the making and breaking of codes) whilst the SIGINT function involves the selection, processing and dissemination of intelligence information from foreign signals for intelligence and counter-intelligence purposes and to support military operations (National Security Agency, 2009). In the US a warrant under the *FISA* needs to be obtained in order to intercept communications where one party to the communication is abroad, in other words to collect foreign intelligence. *FISA* is not applicable to the surveillance of communications collected outside the US and not targeted against US citizens or permanent residents. Such a warrant may authorise the domestic surveillance (in the US) of US persons where there is probable cause that the target of the surveillance is an agent of a foreign power and that the facilities or place at which the electronic surveillance is directed is being used by such an agent of a foreign power. In respect of domestic intelligence gathering through wiretaps a warrant under *Title III of the Omnibus Crime Control and Safe Streets Act of 1968* is required (US, 1968).

After the 11 September 2001 events in the US, the US President authorised during 2001 the NSA in terms of the US Constitution to commence with a counter-terrorism operation referred to as the 'Terrorist Surveillance Programme' (TSP). It was acknowledged that the NSA as part of this programme used interception ('wiretaps') without warrants of telephone and e-mail communications where one party to the communication is located outside the US where the NSA "has a reasonable basis to conclude that one party to the communication is a member of al Qaeda, is affiliated with al Qaeda or a member of an organization affiliated with al Qaeda, or working in support of al Qaeda". In effect, the President in 2001 authorised the NSA to circumvent the *FISA* court-approval process and to engage in forms of surveillance that *FISA* would prohibit (Cole & Lederman, 2006: 1355, 1356). The fact that the President of the US had authorised the said interception was kept secret for some time, but when it became known (only in 2005), led to huge controversy and legal arguments on the legality of the action. Eventually the US government continued the TSP, but

'legalised' the program by obtaining FISA authorisation for the programme. The US Attorney General announced that a *FISA* judge has authorised the government to conduct electronic surveillance of international communications into or out of the US where there is probable cause to believe that one party to the communication is a member or agent of Al-Qaida or an associated terrorist organisation (US, 2007: 56, 57). The controversy of the program has culminated in a Supreme Court case where the case against the NSA, the President of the US and other US government agencies was dismissed by the court for lack of jurisdiction upon various technical points (US, 2007(d): 65). It seems as if the controversy had not been laid to rest yet as a class action was subsequently instituted against the same parties (US, 2008(f)). The present controversy is very similar to a series of surveillance controversies, including the Watergate scandal in the US which led to the adoption of *FISA* (Khan, 2006: 68).

In respect of the sharing of information between law enforcement and civilian intelligence, the 'wall' that separated the two before the events of 11 September 2001, has since been removed through the *PATRIOT Act*, and the *Homeland Security Act of 2002*. In terms of the *PATRIOT Act*, information derived from *Title III* (domestic interception) relating to foreign intelligence or counter-intelligence may be disclosed to any federal official, including law enforcement, intelligence, protective, immigration national defense, or national security officer. In terms of the *Homeland Security Act of 2002*, prosecutors and law enforcement agents may disclose to "appropriate foreign government officials" information involving a threat of domestic or international terrorism, obtained from grand jury and *Title III of the Omnibus Crime Control and Safe Streets Act of 1968,* surveillance, for the purpose of responding to such threat (Sandoval, 2007: 23, 24). This may be done when prosecutors request other countries to assist in the investigation of terrorism cases. The advantages that this provision has for international cooperation is not only obvious, but has already reaped results in the disruption of a plot to blow up airplanes from England to the US during 2006 (Sandoval, 2007: 23). Despite the fact that grand jury investigations of various terrorist plots

had generated valuable intelligence, the discretion left to investigative- or law enforcement officers on whether to share intercepted information was often used as an excuse not to share information. When a witness in a grand jury, for example would testify that persons in the Middle East are planning to bomb a major European Airport, a prosecutor is now permitted to communicate that threat to an appropriate foreign government official to prevent or respond to the threat (Sandoval, 2007: 26).

Of particular importance is the alleged extent of the surveillance and subsequent data-mining of the TSP. The TSP is referred to as 'dragnet' surveillance in which the NSA and other government agencies have "indiscriminately intercepted the communications content and obtained the communications records of ordinary Americans as part of the program". This was allegedly done through nationwide sophisticated communications surveillance devices connected to key facilities of Internet and telephone service providers. The product of this surveillance was the content of a significant portion of the phone calls; e-mails; instant messages; text messages; web communications and other national and international communications of "practically every American who uses the phone system or the Internet…in an unprecedented suspicionless general search through the nation's communications networks". The telephone transactional records of who communicated with whom when and where was also obtained by the intelligence agencies. In a vast data-mining exercise, the contents and traffic patterns of these records were analysed by computers according to user-defined rules to target specific communications for interception (US, 2008(f): para 7 - 11). The extent of the TSP seems to be massive. It is alleged that the Daytona database management technology used to manage the 'Hawkeye' call detail record (CDR) contains records of nearly every telephone call made on the US domestic network since 2001, totaled 312 terabytes of information (US, 2008(f): para. 85 - 87).

3.1.2. Communications intelligence and signals intelligence collection in the United Kingdom by civilian intelligence

The counterpart of the US NSA in the UK is the General Communications Headquarters (GCHQ). The GCHQ is not only responsible for protecting the security of communications of military and security establishments in the UK (official use of cryptography), but also for providing signals intelligence collected from a variety of communications and other signals such as radars. The Composite Signals Office is part of the GCHQ. This office operates from a number of locations in the UK (Cornwall, Yorkshire and Cheltenham) and abroad (Pike, 2003(a)). The extent of interception performed at the Menwith Hill facility has been reflected in the previous chapter in relation to sovereignty. As mentioned, more than two million intercepts are performed per hour at this site. The facility is an extensive one covering 4,9 acres of buildings. There are 26 dome antennas on the premises (it is described as an extensive complex of domes, vertical masts and satellite dishes) (Pike, 2003(a)). GCHQ is involved in all types of communications in the world and its systems are linked together to other sites around the world by means of one of the largest wide area networks in the world. Its communications are protected through encryption. The GCHQ has a strong research and development capacity with a huge number of engineers and mathematicians employed to develop soft-and hardware solutions to a number of obstacles “not normally encountered in the commercial world” (Pike, 2003(a)).

3.2. International cooperation on signals intelligence collection

In Chapter 2, reference is made to the UKUSA SIGINT collection agreement between the UK, US, Canada, New Zeeland and Australia. This is an example of the most comprehensive SIGINT cooperation globally. As far back as 1996, the veil was lifted on the extent of this cooperation and in particular on the global system which was code-named ‘Echelon’. The world’s bulk electronic

communications systems are linked through satellite; hi-frequency radio transmitters; microwave towers; land-based communications systems; and undersea cables. Each one of the UKUSA partners has a number of interception stations all-in-all providing global coverage of communications transmitted in all the above modes. Through the Echelon system, the interception stations of all the allies are interconnected and computers are used to search in accordance with pre-programmed dictionaries of keywords and fax, e-mail and telex addresses, the bulk communications to locate, automatically collect and relay the intercepts to the specific user country. Out of millions of communications the actual intercepts that are needed to be read by intelligence personnel are reduced by this computerised 'funnel' to a manageable few hundred or thousand. A specific 'host' country where an interception station is situated would not even know what is intercepted or relayed to the ally. In respect of the selected channels every word of every message is automatically searched, without the need for the flagging of a particular telephone number or Internet address (Hager, 1996: 2, 3). The Intelsat and Inmarsat satellites had been targeted for collection since the 1970's. New telecommunications systems such as the 66 satellites of the Iridium system might pose new challenges for interception, but it could probably be assumed that there is a global coverage of most bulk telecommunications systems (RSA, 1999: par 1.17).

The NSA and GCHQ facilities, such as Menwith Hill, in effect form part of this interlinked global system for SIGINT interception. What is clear from the above is that positive intelligence has a massive capacity for interception of almost all communications globally without the danger of an overload of intelligence through the computerised selection. The legality of such intercepts relies in many instances on the fact that interception is performed outside the jurisdiction of the 'user country'. In addition to that the authorising legislation such as *FISA,* defines foreign surveillance in a wide and technical manner which allows operational latitude in terms of interpretation. There is also a history in many countries of wide application of interception capabilities through programmes such as the

TSP, which cannot be easily challenged legally as long as the intercepts are used for intelligence purposes only and not as evidence. This factor reduces or denies such intercepts from being used as evidence and might in addition compromise interception capabilities. Law enforcement may, however, benefit otherwise from SIGINT intelligence on an operational level- the pre-empting of terrorist attacks; planning for the interdiction of shipments of drugs, firearms or other goods being illegally trafficked; or targeting such consignments for controlled deliveries; the unraveling of criminal networks and targeting of persons or criminal entities for other court-directed investigative technology. Such intelligence could also be used for the tracing of suspects or fugitives.

Although the UKUSA arrangement is between five countries, the bilateral intelligence cooperation between the US and the UK is exceptional. It has transcended from cooperation simply between intelligence officers to early involvement of prosecutors from both countries to develop a case strategy; to share information about the facts of the case; key evidence; and 'any other information'. Involvement of prosecutors may solve jurisdictional issues such as where and how the investigation may most effectively be prosecuted; whether prosecutions should be initiated or discontinued; and how aspects of the case could be pursued more appropriately in each jurisdiction. This type of cooperation can exclude problems emanating from different laws and legal systems and to determine the course of action most favourable for the solution and prosecution of the case at hand. This cooperation takes place on the strength of a document *Guidance for Handling Criminal Cases with Concurrent Jurisdiction between the United Kingdom and the United States of America,* signed in January 2007 by the Attorneys General of the two countries (Aqua, 2007: 39, 40).

By pursuing the investigation in the country with law more favourable to the investigation, more successes can be ensured. Evidence of successful cooperation in this regard is the foiling of a terrorist plot in the UK. The plot was designed to simultaneously attack aircraft destined from the UK to the US by

detonating liquid explosives on board. Intelligence of the plot shared by the US with the UK led to the arrest in the UK of at least 26 persons and assets of 19 persons were frozen. In following up the massive volume of intelligence from the US, collected before and after the arrests, the UK authorities promptly reacted through thirty six searches of residences and businesses, vehicles and open spaces and seized bomb-making equipment and chemicals and more than 400 computers, 200 mobile phones, 800 items for electronic storage of data, such as memory sticks, CD's and DVD's, 6 000 gigabytes of data and six 'martyr videos' (Aqua, 2007: 37).

3.3. Military intelligence and law enforcement

The violent and transnational nature of many of the international crimes, sometimes require military assistance in the form of direct military operations, or the type of intelligence in which military intelligence specialises, such as imagery intelligence. The role of military intelligence in support of combating international crime is analysed hereunder.

3.3.1. Direct military operations

It is clear that in some instances the military option is the only viable option to address international crimes. This is in particular true in respect of war crimes, genocide and crimes against humanity; piracy and terrorism. Such military action should preferably be based on resolutions of the UN Security Council. A classic example of a successful military operation against a particular incident of terrorism in the form of a hijacking of more than a hundred passengers is Operation Thunderbolt, when the Israeli Defence Force sent a military rescue mission from Israel to Uganda to rescue hijacked passengers of an El Al flight held at the Entebbe Airport in Uganda. In this case the government of Uganda at the time was supportive of the hijackers and the operation had to be executed against all odds over a distance of 2 500 miles by a 500 strong long-range

penetration force (Stevenson, 1976: vii). As was pointed out before, covert action will always remain controversial, especially assassinations. Berkowitz proposes the innovative use of military force in an overt manner by means of direct action, which is in line with international law. 'Direct action' is defined as "short duration strikes and other small scale offensive actions by special operations forces or by special operations- capable units to seize, destroy, capture, recover, or inflict damage on designated personnel or matériel". This reference is to the use of troops to ambush terrorist groups; raid weapons shipments in transit; and rescue hostages, obviously within the international arena and not domestically, but in some instances without necessarily obtaining the support of the country in which or from which the operation is launched (Berkowitz, 2003: 133). The following solution offered for the combating of piracy could well be true for the combating of terrorism: (Le Roux, 2007)

> Combating piracy requires collective maritime early warning and intelligence mechanisms, maritime air surveillance and reconnaissance capabilities and fast-reaction naval vessels that can support law enforcement agencies in apprehending and combating heavily armed pirates. Developing these capabilities collectively will do more for human security in Africa than conventional armed forces designed to combat non-existent enemies.

Solutions very similar to the above have been implemented successfully between three countries in Asia to dramatically reduce the number of piracy incidents. The highest number of sea piracy incidents recorded was for a number of years in Malaysian waters, especially the Malacca Straits. This number was drastically reduced by bilateral and trilateral cooperation through the establishment of the Tripartite Technical Expert Group on Maritime Security. This Group serves as a forum for law enforcement and security experts, inclusive of military and civilian experts of Malaysia, Indonesia and Singapore. Views and intelligence are exchanged in the Group and data on incidents and armed robbery are verified

and evaluated to formulate a common policy to address the problem. The following practical steps were undertaken by the participants: (Permal, 2006: 2, 3)

— The Malacca Straits was divided into zones to enable the identification and monitoring of ships in each zone;
— shore hotlines between the operations centres were established and a common frequency used to facilitate the reporting of incidents and a quick response thereto;
— air surveillance, referred to as 'Eye in the Sky' was introduced;
— cooperation with other user states, such a Japan was established to contribute where the facilities of the participating states were lacking;
— naval communications and security and intelligence cooperation were established with the US; and
— a full scale maritime operation was launched.

It is clear that the key to the success of the above operations is strategic and tactical (operational) intelligence cooperation to determine policy and strategy; to provide warning intelligence and operational intelligence for a rapid and effective response to prevent and combat maritime terrorism in the Malacca Straits. This example is a benchmark for cooperation elsewhere, including along the Horn of Africa. Many of the steps taken above have already been instituted along the coast of Somalia, in particular navy patrols with the UK, US, Russia, China and India amongst 12 nations contributing ships- the US with the Combined Task Force (CTF-151) deployed since January 2009. A problem is, however, the overlap between piracy and terrorism- firstly in legal terms as both terrorists and pirates are non-state actors, often operating from "extraterritorial enclaves" usually aiming acts of destruction against civilian targets. Secondly, on a financial level, there is speculation of pirates funding Islamic terrorists, such as the al Shabaab group (Hanson, 2009). The biggest problem, in terms of law enforcement is on where to prosecute pirates captured in naval operations- Somalia from where the attacks are launched and serves as a safe haven for the

pirates, is as has been pointed out, a failed state. Other countries are not forthcoming to prosecute arrested pirates which may lead to impunity. The US is negotiating with Kenya to fulfill this role (Hanson, 2009). This once again proves the difficulties experienced with jurisdiction, not only in terms of intelligence cooperation, but also in respect of law enforcement. Nadelmann states that: "All governments today face the challenge of controlling growing domains of transnational activities that either ignore or take advantage of national borders, even as their own powers remain powerfully circumscribed by the political, geographical and legal limitations that attend the notions of national sovereignty" (1993: 477).

The experience in Northern Ireland and the UK had been that the best results which emanated from cooperation between law enforcement intelligence and military intelligence were on the tactical level (Watt, 2002: 293). When active cooperation between law enforcement and the military forces commenced in the US in 1982, it immediately led to spectacular results. The cooperation included surveillance which was integrated with the traditional role of the Navy, Air Force and Army Reserve and where these forces were put on the lookout for ships profiled on the basis of crime intelligence as being possibly involved in drug trafficking. The military forces also assisted in information gathering missions. Naval officers were placed in the National Narcotics Border Interdiction Systems Information Centers as intelligence analysts and advisers. Within one year, this cooperation, led to the seizure of 11 vessels, the arrest of 115 persons and the interdiction of 412 222 lbs of marijuana (Venzke, 1983: 5, 6). This interaction has grown exponentially since then.

3.3.2. Interrogation outside the United States

In reaction to the 11 September 2001 events, the US Congress passed the *Authorisation to use Military Force (AUMF) (Public Law No. 107-40 of 28 September 2001)*. In a subsequent executive order the President of the US

established military commissions which tried non-US citizens arrested in the US and on the battlefields of Afghanistan for being suspected of terrorism and deported them to Guantánamo Bay. These persons were labeled as unlawful enemy combatants thus not entitled to US constitutional protection, nor entitled to the rights of prisoners of war (Piret, 2008: 83). One of the reasons for the incarceration of these persons was 'special interrogation', in other words intelligence gathering through interrogation. The interrogation program through which some suspects were detained for months or years in Guantánamo was carried out by the CIA. The US Supreme Court strongly disapproved of this and found that these persons were entitled to constitutional protection, despite not being held on US soil. The court strongly disapproved of the Government's policy, which was described as "creating black holes where it could do anything without legal constraint" (Piret, 2008: 102). In the meantime, President Obama of the US, through presidential orders announced the closure of the program, within one year and prohibited "the C.I.A. from using coercive interrogation methods, requiring the agency to follow the same rules used by the military in interrogating terrorism suspects…" (Mazzetti & Glaberson, 2009). This practice placed the US in disrepute in respect of the methods used and had not been conducive to international intelligence cooperation.

3.3.3. Imagery intelligence collection

One of the main focus areas of military intelligence, in addition to COMINT and SIGINT is imagery intelligence (IMINT). Satellite imagery collection has to a large extent replaced reconnaissance photography for military purposes. The US commenced the satellite imagery collection during the 1950's and since then huge sums of money had been poured into it with an ever-increasing capability. The satellite imagery collection program of the US and the Soviet Union played a significant role in the arms race and negotiations as it could be accurately used to establish not only capacity and identifying exact numbers and location of nuclear weapons and missile sites, but also violations of the *Strategic Arms Limitations*

Talks (SALT) agreements (Klass, 1971: 196 – 205). For purposes of the verification of a *Strategic Arms Reduction Talks (START)* agreement six additional Lacrosse imagery intelligence satellites have been acquired by the US to the value of US $500 million each (Global Security, 2006). Imagery intelligence satellites orbiting at altitudes of several hundred kilometers are able to produce high resolution images of objects on the surface of the earth with a resolution of better than 10 cm. These images are used for the location of vehicles, ships, airfields and other locations of military interests.

4. CONCLUSION

It is clear from the above that special investigative techniques used to investigate international crime are similar to civilian intelligence methodology. At the same time the differences between positive intelligence and law enforcement agencies in terms of mandate, the extent of operations and accountability are apparent. Intelligence emanating from positive intelligence agencies which can be useful as evidence in courts of law is mostly not suitable for presentation firstly as a result of fears of positive intelligence of compromising intelligence capabilities and secondly as a result of the fact that the mandate of positive intelligence is extremely wide, accountability in respect thereof is problematic and its methodology is used in a manner which could be legally questionable if information gained from it is used as evidence in a court of law. The experience is, however, that both in the US where intercepts are generally used as evidence, and the UK where domestic intercepts may not used, but intercepts received form other countries may, such evidence is invaluable.

For effective use in courts, it is preferable that both positive intelligence and law enforcement intelligence perform intercepts subject to the same legal controls such as in the UK. It is further clear that SIGINT collection by positive intelligence is the most likely area for cooperation between law enforcement and positive intelligence. This would require law enforcement to share their targets with positive intelligence for flagging in dragnet processes such as bulk interceptions

and data-mining. However, the focus of such cooperation would seldom be in terms of obtaining evidence- rather in operational or tactical support of special investigative techniques and mostly for crime prevention or interdiction actions. Such cooperation could also be supportive of joint legal and military action, as in being able to respond to piracy and terrorism. The issue of bulk interception remains a contentious one in all jurisdictions. However, intelligence agencies acting under the guise of diplomatic immunity can without much effort use this methodology in a host country, and if the host country would not also use the same methodology, it could place itself at a huge disadvantage in terms of counter-espionage and foreign intelligence gathering. Positive intelligence does much to find innovative ways of circumventing legal and jurisdictional issues. This is evident from the TSP described above. The solution seems to lie in the acceptance of the principle of bulk interception linked with data-mining techniques with the necessary authorisation and accountability regimes in place- for example the *FISA* Judge in the US. The limitations of mandates of the interception agencies and for example approving the 'dictionary' used to extract certain communications from bulk communications could be made subject to approval. The use and disposal of intercepts emanating from bulk interceptions could also be prescribed.

It is clear that the traditional demarcation between defence and security (law enforcement) and the view that law enforcement's role is an internal one has changed as a result of international threats. As a result of the concept of intelligence-led policing, the police services are viewed as part of the broader IC. The importance of positive intelligence keeping law enforcement informed is gradually realised. In view of different responses available to combat international crime, it is important to keep in mind that it is not only a matter of how law enforcement could be supported or strengthened by positive intelligence agencies, but rather how as far as possible intelligence capabilities and available information could on national, regional and international level be pooled to ensure that the most appropriate and effective action in the circumstances is taken

against international crime. The intelligence available through law enforcement investigations might be critical in respect of military operations where the same is necessitated for example action against piracy or terrorism. In the next chapter the mechanisms for intelligence cooperation on the national level in different jurisdictions will be described and analysed. Covert action is not an area in which international cooperation is viable- maybe only between the most trusted of allies. The main focus area for intelligence cooperation in respect of the combating of international crime should be in respect of interdiction, prevention and investigation through special investigative techniques. The maximum success could be achieved through appropriate legal structures and powers which provide for both positive intelligence and law enforcement to have similar types of oversight and empowering laws to regulate their activities, especially in respect of the combating of international crime. Controversial intelligence gathering methods, including the creation of 'black holes' where intelligence agencies could operate totally unchecked, is not conducive in the long run to intelligence cooperation on a wider scale, and may even damage relations with the best of allies.

A solution to improve international intelligence cooperation is to provide for an international instrument which could lay down some of the rules and ethics required to ensure that support from positive intelligence to crime intelligence is actionable and useful in respect of tactical response as well as crime prevention and prosecution. This proposal is also made by Watt (2002: 297). Such cooperation should include interaction during the investigative stage, not only between the investigators, but also the prosecutors in the respective countries, in order to determine the most appropriate strategy to pursue the case in the respective jurisdictions. It is clear that powerful nations with huge intelligence capabilities can achieve much more positive results by means of intelligence support to other countries to ensure effective investigation and prosecution in those countries, rather than through extralegal actions such as rendition aimed to bring the suspect before US courts at all costs, or to submit the suspect to

interrogation in a country where no assurances can be given that torture and the death penalty would not be applied. There is also a lack of general standards for entering into agreements on intelligence cooperation between services or agencies of countries, as pointed out in Chapter 4.

CHAPTER 6
MODELS FOR INTELLIGENCE COOPERATION ON NATIONAL (INTERAGENCY) LEVEL

1. INTRODUCTION

In the preceding chapters various examples of changes in the UK as well as the US following the 11 September 2001 events, for example the removal of the wall of division between civilian and law enforcement (crime) intelligence, resulting from highly controversial domestic intelligence activities of the CIA and other intelligence agencies, and the strengthening of interception and other investigative powers have been discussed. There are events and inquiries, other than those of 11 September 2001, in both these countries, which had an effect on intelligence and intelligence cooperation in both the UK and the US, notably the Commissions of Inquiry in both countries on issues relating to intelligence on WMD in Iraq, which led to the second war in Iraq; as well as the Al-Qaida attacks in the UK on the London transport system in 2005. The emphasis throughout is on intelligence sharing between all members of the civilian IC in both countries and law enforcement. Mention has already been made of fusion centres in the US as the vehicle for intelligence sharing.

The purpose of this chapter is to analyse the recommendations of the respective commissions in terms of proposals in respect of structural (institutional) changes; policies relating to intelligence and intelligence cooperation dealing also with interagency relations; and intelligence activities and the products thereof. Since these recommendations have been implemented, some time has lapsed and the practical problems in respect of some of the recommendations have already emerged. These problems will be analysed against the background of the

intelligence model of the countries in question as to assess to what extent the intelligence model or elements thereof, is capable of serving as a possible benchmark for other countries. It seems as if intelligence cooperation on national level between civilian and crime intelligence firstly depends on the policing model being followed. The similarities between the UK and the US, in terms of intelligence-led policing and community policing as a basis for intelligence cooperation and intelligence sharing will also be discussed. The initial recommendations of the Commission which inquired and reported on the events of 11 September 2001; the intelligence failures related thereto; and subsequent recommendations and implementation thereof are set out. The focus in this chapter is mostly on intelligence cooperation in respect of terrorism and organised crime and to some extent the proliferation of WMD. Intelligence cooperation in respect of the other international crimes mentioned in Chapter 1, namely war crimes, genocide and crimes against humanity, and mercenary acts will be dealt with in Chapter 8, dealing with intelligence cooperation on international level.

2. CASE STUDY OF THE INTELLIGENCE MODEL IN THE UNITED STATES POST-11 SEPTEMBER 2001

Even before the events of 11 September 2001, the following factors regarding intelligence in the US were already evident, but not addressed until these events acted as a catalyst for intelligence reform: (Hulnick, 1999: 191 – 208)

— The extremely complicated structure of the US “Spy Machine”;
— what was regarded as an almost impossible task to restructure the intelligence structures;
— the role of the Director of Central Intelligence (DCI) and the need to give ‘more clout’ to that position;
— the need for improving interagency and international intelligence cooperation and the proliferation of “dozens” of informal interagency cooperative groups at

various levels, linked electronically, with recommendations to expand such informal cooperation in addition to more formal coordination structures; and

— unnecessary duplication of effort- which was then regarded positively in the sense that overlaps and competitive intelligence were seen as a means to avoid intelligence failures.

It was therefore realised before 11 September 2001 that at least some changes to the US intelligence system were required. Unfortunately, it required events such as that of 11 September 2001, to make a more major overhaul of intelligence imperative and urgent. The recommendations of the National Commission on Terrorist Attacks upon the United States (referred to as the 9/11 Commission), relating to intelligence structures and cooperation, are analysed hereunder.

2.1. Analysis of the 9/11 Commission

The 9/11 Commission set out a global strategy to address terrorism. The report of the Commission contains wide-ranging recommendations not only relating directly to intelligence, but also policy, such as the recommendation to attack the sanctuaries or havens of terrorism which enable the assembling of funds, provisioning of training, weapons and command structures — in the safety of “lawless countries” with rugged terrain, weak government, sparse population, and room to hide (US, 2004(b): 366). Other recommendations include the targeting of the funding of terrorism (US, 2004(b): 382); the targeting of terrorist travel (US, 2004(b): 385); biometric screening systems for border control (US, 2004(b): 385, 389); exchange of terrorist information with “trusted allies” (US, 2004(b): 390); improvement of the security of identification systems (US, 2004(b): 390); and improved screening of travellers (US, 2004(b): 393). The focus of this chapter, however, is on the weaknesses of the structures and functioning of the IC and recommendations to address it.

The Commission pointed out that what is required in future is not only cooperation, but joint action. The terrorist threat has spread over the boundaries of many agencies, and although there was some sharing of information, a major problem remained coordination to ensure joint action (US, 2004(b): 400). The rationale for joint action is joint planning; the advantage of having someone in charge to ensure a unified effort; and the sharing of a limited pool of expertise (US, 2004(b): 401). A major problem identified was the duplicity of effort by various agencies, with “Counter-Terrorism Centres” with different names in the CIA, Defence Intelligence, the Department of Homeland Security and the FBI (US, 2004(b): 401). The Commission observed that a “smart’ government would integrate all sources of information to "see the enemy as a whole” (US, 2004(b): 401). The Commission therefore recommended a National Counter Terrorism Centre (NCTC) for joint operational planning and joint intelligence, staffed by personnel from the various agencies. The NCTC is supposed to task and utilise the CIA, FBI, Homeland Security and departments and agencies by pooling all-source domestic and foreign intelligence to lead with strategic analysis and warning intelligence (US, 2004(b): 404). Although the NCTC should perform joint planning of operations it is not supposed to be directing the operations, but rather monitor the implementation and bridging the divides between the respective agencies and between domestic and foreign intelligence.

The respective agencies must therefore relinquish some authority for the sake of joint planning, but retain operational responsibility (US, 2004(b): 406). The head of the NCTC, appointed by the President, must report directly to the DNI and indirectly to the President (US, 2004(b): 405). It is envisaged that interagency policy disputes should be addressed by the NSC. The Commission points out six problems with intelligence, experienced by the IC before and after 11 September 2001: (US, 2004(b): 408 -410)

— There is no single intelligence agency which has access to all intelligence, resulting in an inability to “connect the dots”, as each agency focuses on its own mission, making joint planning and coordinated execution

impossible — this is summarised as “structural barriers to perform joint intelligence work”;

— a lack of common standards and practises in respect of common and domestic information collection, analysing, processing, translation, sharing, and reporting — the ideal is, through such common personnel standards to “transcend own service-specific-mindsets";

— the inability of the DNI to direct national intelligence capabilities, especially those which are critical to the Defence Department, such as SIGINT and IMINT;

— as a result of the narrow focus of individual agencies, the use of resources is not focused or not easily redirected to address national needs;

— the Director of Central Intelligence (DCI) (as the post existed at the time of the Commission’s inquiry) has too many “jobs” and is not empowered to perform the joint management of the IC, and the DCI, for example neither has budgetary control, nor the ability to “hire or fire” managers, nor to set uniform standards for information infrastructure or personnel; and

— with a total of some 15 intelligence agencies comprising the IC, it has become too complex and secret, especially in respect of funding. The fact that budget and personnel issues were further divided between different departments, namely Defence and Justice (the Attorney General), contributes to a lack of control and accountability.

To overcome the above weaknesses, the Commission recommended the replacement of the position of the DCI, with a National Intelligence Director to “oversee national intelligence centres on specific subjects of interest across the US Government and to manage the national intelligence programme and oversee the agencies that contribute to it” (US, 2004(b): 411). The Head of the CIA; the Under-Secretary of Defence responsible for intelligence; and the FBI’s executive assistant director for intelligence or the Under-Secretary of Homeland Security for information analysis and infrastructure protection, are proposed by the Commission as the three deputies for the National Intelligence Director (the

post was eventually established as the DNI). The National Intelligence Director is recommended to be responsible for a unified budget for national intelligence that reflects the national intelligence priorities chosen by the NSC, and an appropriate balance among the varieties of technical, and human intelligence collection and analysis (US, 2004(b): 412). The National Intelligence Director should be empowered to determine information technology policies to maximise data sharing and to protect the security of information. He or she should also participate on the executive management of the NSC that can resolve differences in priorities between agencies and submit major differences to the President for resolution (US, 2004(b): 414). In respect of the CIA, the 9/11-Commission recommended the rebuilding of the CIA's analytical capabilities; that the clandestine service should be transformed with a focus on human intelligence capabilities; an improved language program; and ensuring a working relationship between human source intelligence collection and signals intelligence collection; to promote diversity in recruiting personnel, to be able "to easier blend in foreign cities". The Commission, however, recommended that the lead responsibility for paramilitary operations, both clandestine and covert, should be moved from the CIA to the Defence Department (US, 2004(b): 416).

The Commission identified the "human or systemic resistance to the sharing of intelligence" as the biggest impediment to all-source analysis. The need-to-know principle, according to the Commission needs to be replaced by the need-to share principle; avoiding over-classification of information and provide incentives for the sharing of information (US, 2004(b): 417). Information-sharing networks need to be established and the intelligence should be divorced from the reference to sources in order to ensure that the maximum number of recipients can access the information. A horisontal (decentralised) model for the sharing of information was proposed where each agency has its own database, but that the databases of the respective agencies are searchable across agency lines. Secrecy is maintained through an "information rights management" approach that controls access to the data, not access to the whole network. It is referred to as a

"trusted information network". Presidential leadership was called for by the Commission to ensure the establishment of such a trusted information network. The Commission also found that Congressional oversight over intelligence is dysfunctional and recommended a single principal point of oversight and review for homeland security (US, 2004(b): 420, 421).

The FBI's role remains vital and the Commission recommended that "a specialised and integrated national security workforce should be established at the FBI consisting of agents, analysts, linguists and surveillance specialists who are recruited, trained, rewarded and retained to ensure the development of an institutional culture imbued with a deep expertise in intelligence and national security". In this regard the Commission further recommended that all managers in the FBI should be certified intelligence officers — including those working on law enforcement matters specifically (US, 2004(b): 425, 426). The Commission recommended that the Department of Homeland Security and its oversight committees must regularly assess the threats against the US, as well as the plans to counter such threats (US, 2004(b): 428).

The *Report to the President of the United States: Commission on the Intelligence Capabilities of the United States regarding WMD* is also important for this study, as its focus is on intelligence from the perspective of terrorism through WMD and more generally the capabilities of US intelligence to monitor the proliferation of and control over WMD. Furthermore the Commission on WMD looked into the recommendations of the 9/11 Commission and made findings on the progress with the implementation of the 9/11 Commission's recommendations.

2.2. Analysis of the *Report to the President of the United States: Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction*.

The above Commission found that the US IC in respect of Iraq's WMD erred: (US, 2005(c): 3).

- Before the First Gulf War in that it completely underestimated the advances made in the Iraqi nuclear program; and
- thereafter by wrongly assessing that Iraq resumed its nuclear weapons programme; had biological weapons and mobile biological weapon production facilities and had stockpiled and was producing chemical weapons, before the Second Gulf War.

In respect of Al-Qaida in Iraq, the IC assessed before the war in 2001 that Al-Qaida had a limited ability to use unconventional weapons to inflict mass casualties. After the war there was surprise to the extent of the capabilities, which was also more advanced than estimated. The knowledge gained at that stage, however, prevented another intelligence failure (US, 2005(c): 268). The IC was able to penetrate the AQ Khan network responsible for proliferation and the nuclear development programmes in Libya, Pakistan, North Korea and Iran. The Commission commended the IC for its successes which led to Libya openly declaring its nuclear and chemical materials; abandon production development and handed over part of its missile force to US and UK officials for shipment out of Libya and cancel its long-range missile projects (US, 2005(c): 263) (US, 2004(a): 5). The Commission on the intelligence capabilities of the US regarding WMD pointed out that the IC first started to look seriously at the threat posed by biological weapons after the 11 September 2001 events when anthrax attacks in the US killed five people, crippled mail deliveries in a number of cities for more than a year, and decontamination efforts were costing in the region of $1billion. The estimated costs of producing the anthrax was in the region of US$2 500. The attacks could, however, had a much worse effect had the anthrax been released

in an urban area and in the open air. The Commission investigated the implementation of the 9/11 Commission's findings and recommendations and concluded that many of the shortcomings identified by the 9/11 Commission had improved to some degree, such as the analysis and sharing of information, and improving the quality of finished reports (US, 2005(c): 282, 283). The Commission on WMD, however, identified areas where improvements were still required. Of particular importance is the following, which had been described in Chapter 3 of this study as a major stumbling block for intelligence cooperation: (US, 2005(c): 288)

> Our study found evidence of bitter bureaucratic "turf battles" between agencies, and a pronounced lack of clarity as to the roles, responsibilities, and authorities of various entities tasked with the counterterrorism mission. Specifically, this interagency jockeying over overlapping counterterrorism analytical responsibilities indicates that major organisational issues affecting the allocation of resources, assignments and responsibilities, coordination of analysis, and effective warning remain unresolved.

The NCTC and the CTC continue to fight bureaucratic battles with a resultant unnecessary duplication of effort and unproductive competition amongst themselves. The Commission on WMD favoured competitive warning analysis, but warned that communicating the outcome of such analysis must be coordinated and integrated (US, 2005(c): 292). An example is mentioned of an incident in which a single raw intelligence report initiated five different agencies to write five different reports, with the same conclusion- a result that could have been prevented by a single coordinated report (US, 2005(c): 294). The time spent in the FBI on direct operational support also leaves little time for strategic work on new and emerging threats. There is ongoing evidence of a failure between agencies to cooperate and divide responsibility regarding analysis of

terrorist information. The failure to manage resources in respect of information on WMD has limited the capability to identify and warn against threats relating to WMD. Such failure is evident from the following: (US, 2005(c): 296, 297)

— There is no shared mission between the FBI and the CTC, despite being co-located at some places;
— the removal by the Department of Homeland Security of radiation detection devices to New York, which, when detected by the FBI, was regarded as a threat followed by an unnecessary and expensive response- and turned out to be only a legitimate removal of a medical isotope- all which could have been prevented by appropriate interaction; and
— difficulties experienced by the CIA to obtain information from the FBI where the focus of a terrorist investigation shifted from the domestic to the foreign domain.

The Commission on WMD concluded in respect of the sharing of information in relations between state, local and tribal authorities that despite more terrorist information being shared, there is a lack of a comprehensive policy on what information to share and how to provide it. Reference is also made to the "redundant lines of communication" presenting a deluge of information for which the authorities on the respective levels are not equipped or trained to process, prioritise or disseminate (US, 2005(c): 287).

Intelligence collectors furthermore continue to operate as if they own information and there is a lack of clear guidelines or consistent application of existing guidelines regarding the withholding of information, and a lack of a system to hold collectors accountable for inappropriately withholding information (US, 2005(c): 288). Despite the institution of the NCTC, which facilitated the sharing of information, there still was no single entity in the IC with the authority and responsibility to impose a centralised approach to the sharing of information. The Commission on WMD made a number of recommendations to improve

leadership in respect of intelligence coordination, namely that the DNI must establish mission managers on his staff to manage all aspects of intelligence on priority targets; the development of new technologies; the establishment of a leadership structure within his office to manage the intelligence collection process on an IC basis, whilst maintaining the "pockets of excellence" within the respective agencies; establishing a central IC human resources authority and establishing a National Intelligence University (US, 2005(c): 311). The purpose of the last recommendation is to recruit and maintain a professional workforce (US, 2005(c): 321).

The Commission points out some pitfalls towards integration of intelligence, such as the challenge to establish the same type of control by the DNI over the FBI, as that which the DNI has over the CIA and to ensure that the expansion of Defence Intelligence does not undermine the ability of the DNI to manage the IC (US, 2005(c): 331, 332). It must further be ensured that the DNI has the capability to manage intelligence collection efforts, in particular to develop clear procedures for the management of Defence Department agencies in the IC, including coordination of the Special Operations Command of the Defence Department and the CIA (US, 2005(c): 333). The Commission identified a shortcoming in that perceived 'legal issues' such as the legality of certain covert operations were claimed to be the reason for inaction. The Commission stated that although there are sometimes real and serious legal issues, in most cases it turned out to be "either myth that overcautious legal advisers have not debunked or policy choices swathed in pseudo-legal justifications". The reason for this tendency is the lack of a sizeable legal staff to focus on IC issues, and the fact that the rules and regulations governing the IC had been in existence for many years and the legal basis for some of those rules and regulations might have changed in the meantime. The Commission consequently recommended that the DNI establish an internal office consisting of a small group of lawyers "expressly charged with taking a forward-leaning look at legal issues that affect the IC as a whole" (US, 2005(c): 355).

One of the most important recommendations made by the Commission is that the information sharing environment should be expanded to include all information and not only information on terrorists (US, 2005(c): 432). The DNI is also recommended to set uniform information management policies, practices and procedures for the whole IC (US, 2005(c): 442). From the above, having clear policies especially setting out the roles of the different agencies is of vital importance. The most important policies which were developed as a result of that need after 11 September 2001 are dealt with hereunder.

2.3. Policies developed as a result of the recommendations of the above Commissions.

The policies that were approved were intended for the IC as a whole, as well as for the respective members of the IC. One of the key policy documents is the *National Criminal Intelligence Sharing Plan*.

2.3.1. The National Criminal Intelligence Sharing Plan

The US law enforcement structures are characterised by a proliferation of small agencies- some 75 percent of law enforcement agencies have less than 24 officers, which result in a lack of intelligence capacity in that agency. These local agencies, however, have valuable links to the communities they serve, and may contribute to the intelligence picture, but at the same time need to benefit from sharing intelligence with the broader IC (US, 2003(a): iii). *The National Criminal Intelligence Sharing Plan* places huge emphasis on the principles of intelligence-led policing and community policing, which will be discussed in more detail where reference is made thereto in the *National Intelligence Model* in the UK. The vision for the *Plan* is that it should serve as the following for local, state, tribal and federal law enforcement agencies: (US, 2003(a): 2)

— A model intelligence sharing plan.

- A mechanism to promote intelligence-led policing.
- A blueprint for law enforcement administrators to follow when enhancing or building an intelligence system.
- A model for intelligence process principles and policies.
- A plan that respects and protects individuals' privacy and civil rights.
- A technological architecture to provide secure, seamless sharing of information among systems.
- A national model for intelligence training.
- An outreach plan to promote timely and credible intelligence sharing.
- A plan that leverages existing systems and networks, yet allows flexibility for technology and process enhancements.

Through the *National Criminal Intelligence Sharing Plan*, agencies are encouraged to mandate participation in "pointer systems". Agents and investigators register through such a system investigative interest in a particular subject/suspect/target in order to ascertain which other law enforcement agencies and investigators, even within the same agency, may have a common interest , might share information, or might be participating in a joint investigation (US, 2003(a): 10). In respect of databases, the *National Criminal Intelligence Sharing Plan* suggests that existing systems be maximised by connecting them to expand collaboration efforts and database access, whilst still protecting confidentiality, by securing the network to become a 'trusted information system' (US, 2003(a): 19). The vetting of law enforcement officers by means of fingerprints as well as background checks to promote trust is emphasised (US, 2003(a): 24).

2.3.2. National Strategy for Information Sharing

This is the broad framework on a strategic level for information sharing in the US. It focuses on the development of what is referred to as the Information Sharing Environment (ISE). The *National Strategy for Information Sharing* emphasises information sharing (with the focus on terrorism), on the local level, federal level, between the IC and the private sector, as well as the sharing of information between the IC and foreign partners. The *National Strategy for Information Sharing* provides basically five guidelines, namely the need to "develop common standards in respect of all intelligence processes, consistent with the protection of (civilian) intelligence, law enforcement, protective and military sources, methods and activities"; that the 'war on terror' requires a national effort, involving agencies at all levels of government, as well as the private sector and the need to develop a common framework regarding the respective roles of the role-players; the development of the sharing of sensitive, but unclassified information; the need to facilitate and support the appropriate exchange of information with foreign partners and allies; and lastly the principle that information privacy rights should be protected (US, 2007(a): 13). Fusion, which will be dealt with hereunder more comprehensively is an important focus-area of the *National Strategy for Information Sharing*.

Although the *National Strategy for Information Sharing* is aimed at information sharing on terrorism, it is made clear that a culture must be fostered which recognises the importance of fusing not only information on terrorism, but in respect of all crimes with national security implications and "all hazards information (e.g. criminal investigations, terrorism, public health and safety, and emergency response)" (US, 2007(a): A1-1). The *National Strategy for Information Sharing* further emphasises coordination and coordination structures, such as the Interagency Threat Assessment and Coordination Group with the Department of Homeland Security, FBI, members of the (positive) intelligence community and State and local representatives (US, 2007(a): 18); This coordinating mechanism

must produce intelligence products such as “alerts, warnings and notifications of time-sensitive terrorism threats to locations within the US; situational awareness reporting regarding significant events or activities at the international, state and local levels” as well as strategic assessments of terrorism risks and threats (US, 2007(a): 19). In respect of international information sharing, the conclusion of formal agreements and “other understandings” is regarded as important in order to ensure the confidentiality of exchanged information – also to limit public disclosure or restrict the dissemination of exchanged information when requested to do so by foreign partners (US, 2007(a): 25).

The *National Strategy for Information Sharing* envisages that the exchange of classified information will remain restricted to rather formal context (US, 2007(a): 26). By establishing a “Single Information Environment” (SIE), it is endeavoured to avoid the fragmentation of the IC and what is referred to as ‘stove-piped solutions’. The ‘building blocks’ to the implementation of the proposals of the *National Strategy for Information Sharing* are: Governance, namely the oversight and leadership through which managers must drive initiatives within agencies and across agencies; policy, namely national and internal policies, rules of engagement standards and role of the internal and external role-players involved; technology, namely the technology, systems and protocols that must provide the platform for information sharing and security; organisational culture, involving the ‘will to share’, motivation and incentives to share information; and economics, which relate to the funding and providing of resources for information sharing initiatives (US, 2008(b): 19).

2.3.3. *United States Intelligence Community: Information Sharing Strategy*

The *US Intelligence Community: Information Sharing Strategy* is directed at the whole IC and focuses instead of on structures and technology more on the institutional cultures, which could be a major stumbling-block to the sharing of information. Especially the imbedded mindset of ‘need-to-know’ must be

addressed with the principle of 'need-to share' or 'responsibility to provide' (US, 2008(a): 6, 9). The vision of the *US Intelligence Community: Information Sharing Strategy* is an integrated intelligence enterprise that anticipates mission needs for information by making the complete spectrum of intelligence seamlessly available to support all stages of the intelligence process (US, 2008(a): 9). The new information sharing model must, in terms of the *Intelligence Community: Information Sharing Strategy* further be enterprise centric rather than agency centric, mission centric and self-generating, rather than static, attribute based rather than compartment based (based on security access), and a 'cultural' shift from data 'ownership' to 'data stewardship' (US, 2008(a): 9). Another aim is to promote access to information within a 'trusted environment' and security built into the data and environment (US, 2008(a): 9). Information must be available through an accessible IC infrastructure "that supports information discovery, retrieval and collaboration. Information must be made discoverable to both collectors and analysts within the needs of a mission: Discovery of all information allows the uncovering of information having a relationship to other data providing a better opportunity to 'connect the dots'" (US, 2008(a): 10). The 'trust model' envisaged in the *IC Intelligence Community: Information Sharing Strategy*, is based on the one hand on confidence by the users of information in the information itself, and on the other hand confidence by the providers of information on who will have access to the information, the measures to protect the information, and how the information will be used (US, 2008(a): 11). By developing a reward system for the sharing of information, it is hoped that the *Intelligence Community: Information Sharing Strategy* will remove the obstacles to sharing information. The DNI established the Intelligence Community Information Sharing Steering Committee and the Information Sharing Strategy determines that this Committee must merge other policies and initiatives on information sharing (US, 2008(a): 17).

2.3.4. *Information Sharing Strategy for the United States Department of Homeland Security and the Department of Defense Information Sharing Strategy*

The *Information Sharing Strategy for the US Department of Homeland Security* institutionalises the principles referred to in the broad *US IC: Information Sharing Strategy* referred to above, in the Department of Homeland Security (US, 2008(b)). The *Department of Defense Information Sharing Strategy* serves the same purpose for the US Department of Defense (US, 2007(b)). Both documents elaborate on the same principles, set out in the *US Intelligence Community: Information Sharing Strategy* within the context of respectively the Department of Homeland Security and the Department of Defense. The importance of these strategies is not so much their contents, which overlap with the *US Intelligence Community: Information Sharing Strategy*, but the fact that they serve as platform for the implementation of the *US Intelligence Community: Information Sharing Strategy*, and therefore reflects joint implementation of these strategies in two of the important role-players in the IC.

2.3.5. *National Fusion Centre Guidelines*

The concept of fusion is a well-known concept, used for many years in transportation, aviation, meteorology and the military, and has been introduced through the above guidelines as a method to improve information sharing. The *Fusion Centre Guidelines* is a joint product of the US Department of Homeland Security and the US Department of Justice. Fusion centers are intended to go beyond being simply ‘intelligence centers’, or ‘computer networks, but to support the implementation of “risk-based, information driven prevention, response and consequence management programs”. Fusion and more particular data fusion involves the flow and exchange of information and intelligence from different sources “across levels and segments of government and private industry”. These sources include law enforcement. The fusion process is aimed at both risk and

threat identification and how to address such risks or threats timeously and effectively (US, 2006(c): 11). The fusion centers must focus on strategic as well as tactical (operational) intelligence and function on an ongoing basis. Although they are in the first place aimed at countering or addressing terrorism threats they must collect, analyse and disseminate "all-crimes information" to identify emerging patterns and trends, and it must have the capability to 'blend' law enforcement information and intelligence and not only serve as a primary point of contact to report terrorist/criminal information to local and federal coordination structures, but also as a hub for the receipt and dissemination of law enforcement information received from federal structures (US, 2006(c): 13). Fusion centers must facilitate access to databases such as drivers' licences, and motor vehicle registrations; location information, such as addresses and contact information; law enforcement databases; national crime information centre; criminal justice agencies; private sector databases such as security industry, identity theft and gaming industry databases; and regional information systems and federal and international databases, such as that of the FBI and INTERPOL (US, 2006(c): 33, 34). Key issues are interconnectivity of data systems and security measures for the facility, data and personnel (US, 2006(c): 37, 43). To integrate functions two options are provided, namely co-locating of personnel (the preferred option) or virtual integration by means of communications networks (US, 2006(c): 47).

In respect of the staffing of fusion centers, some of the important issues are to provide a 24 hours a day service for seven days per week; a core staff dedicated to communications, administration, and information technology; a proportional representation of participating agencies; identification and use of subject-matter experts from law enforcement, public safety and private sector; legal counsel and liaising with the local prosecutor's office; and security clearances for personnel in accordance with requirements (US, 2006(c): 51). Intelligence-led policing must be implemented as part of the functions of the fusion centers (US, 2006(c): 55). The products of the fusion centers should include investigative and tactical response; pro-active strategic response; alerts and notifications; target

identification; criminal backgrounds and profiles; crime pattern analysis; association, link and network analysis; telephone toll analysis; flowcharting; financial analysis; and threat assessments (US, 2006(c): 57). In respect of resourcing and funding, the participating agencies should share costs in respect of all budgetary expenses such as accommodation, vehicles and salaries (US, 2006(c): 63). In view thereof that fusion centers represent the manner in which intelligence cooperation and information and intelligence sharing on local and national level have been institutionalised, it is important to also take into account the practical problems that emanated from their implementation.

2.4. Fusion Centres: Practice and problems

There is often insufficient terrorist activity to support a multi-jurisdictional and multi-governmental level fusion centre that exclusively processes terrorist activity (Nenneman, 2008: 2). To be able to maintain the skills and interest of analysts as well as the participation and data collection by the emergency responder community, the fusion center must also analyse and process other criminal activity (Nenneman, 2008: 3). The view has been expressed that “there is just not enough purely terrorist actionable intelligence to justify all of the fusion centers that are in operation…a purely terrorist orientation would lead the centers to become irrelevant to local law enforcement, since the FBI has the primary counterterrorism role” (Nenneman, 2008: 53). Another problem is the funding of fusion centers (Nenneman, 2008: 6). The value and usefulness of ‘local’ information is clear from the fact that in practice fusion centers source most of their information from local agencies and only a small percentage from federal sources (Nenneman, 2008: 29). Indications are that many fusion centers require improvement of analytical and writing skills; training to identify reportable intelligence; and training regarding intelligence methodologies, open source exploitation, anticipating law enforcement needs, advanced research skills, and analytical tools (Nenneman, 2008: 33).

It is planned to give fusion centers a dual mission- to counter terrorism as well as local threats, which will also benefit the public more (Nenneman, 2008: 55). Of importance is that a purely counterterrorism focus might lead to failure, as many terrorists revert to petty criminal activities to support themselves. Therefore identifying identity theft; counterfeiting; financial crimes; fraud and narcotics might lead to the uncovering of terrorists (Nenneman, 2008: 56).

Although law enforcement officers are required in the fusion centers, they are often not equipped to be fusion center analysts who are required to study huge volumes of material from different sources, and to recognise patterns and integrate them into a potential threat pattern (Nenneman, 2008: 61). The majority of analysis is, however, on the tactical 'case support' level and not the strategic level. In practice the security clearances required to have access to top secret information take two years to acquire and the rotation of personnel exacerbates backlogs with clearances (Nenneman, 2008: 63).

On a practical level the problem of over-classification of documents remains a problem (Nenneman, 2008: 68). The need for community orientated policing and community outreach programmes as part of the activities of fusion centers is underlined (Nenneman, 2008: 107).

For an understanding of the intelligence reforms following the report of the Commission, it is deemed necessary to reflect on the broader status of implementation of the recommendations pertaining to intelligence, as presented in the next section.

2.5. Status of implementation process of recommendations of 9/11 Commission and the Commission on weapons of mass destruction

The recommendation for the establishment of a DNI, with authority over the various agencies in the US IC, and principal intelligence adviser to the President,

in addition to a separate Director of the CIA, was implemented through the *Intelligence Reform and Terrorism Prevention Act, 2004* (referred to as the *Intelligence Reform Act*) (US, 2006(a): 1, 2). In respect of intelligence oversight on legislative level, a single or joint oversight body, as recommended by the 9/11 Commission was not established. The recommendation of the 9/11 Commission for the public disclosure of the US intelligence budget was also not followed. The *Intelligence Reform Act* furthermore gives effect to important recommendations of the 9/11 Commission to designate a single authority to oversee and implement uniform standards for access to classified information and reciprocity between agencies of clearances and to address the backlog on security clearances (US, 2006(a): 7, 8). The recommendations of the 9/11 Commission on border control have also been addressed in the *Intelligence Reform Act*. The Act calls for an accelerated deployment of the biometric entry and exit system to process and contain certain data on aliens and their physical characteristics; in-consular interviews for non-immigrant visas; and the expansion of the pre-inspection programs for visitors to the US, and placing US immigration inspectors at foreign airports. The *Intelligence Reform Act* also requires that airline passengers, amongst others, be pre-screened against terrorist suspect watch-lists. The Act also requires the integration of all databases and data systems that process or contain information on aliens by December 2006 (US, 2006(a): 34, 35).

The implementation of the 9/11 Commission's recommendations set out above makes it clear that huge strides have been made in terms of intelligence structures, policies, procedures and processes. A major problem with the new intelligence structures is the sustainability thereof, because of a too narrow focus on terrorism only. To sustain such elaborate intelligence structures on local level, and to sustain involvement on local level, the local needs in terms of crime threats, which may be unrelated to terrorism, must be taken into account. The approach in some fusion centres to have an 'all crimes' approach, is the correct approach. Such an approach will eventually pay off in terms of crime combating in general, but also combating terrorism, as a result of the interrelatedness

between terrorism, organised crime, piracy and even petty crime used by terrorists to sustain them. The parallel developments in respect of intelligence transformation in response to the changing nature of national threats in the UK are important to this study. The US does not have a civilian domestic intelligence agency, whilst the UK broadened the role of its civilian domestic intelligence agency, MI5 to support law enforcement, especially in relation to the combating of terrorism (US, 2003(b).

3. CHANGING ROLE OF CIVILIAN AND CRIME INTELLIGENCE AGENCIES IN THE UNITED KINGDOM TO COMBAT TERRORISM AND ORGANISED CRIME

The role of both civilian and crime intelligence agencies in the UK in respect of the combating of serious organised crime and terrorism is in a gradual process of development and restructuring in order to effectively address those crimes. The role of MI5 and the establishment of a crime intelligence *cum* crime investigation agency outside the police structures, the Serious Organised Crime Agency is discussed hereunder. To place such discussion in perspective, a brief background to intelligence structures in the UK is required.

3.1. Intelligence structures in the United Kingdom

The civilian IC in the UK consists of the Security Service (MI5) established in terms of the *Security Services Act of 1989*; the Secret Intelligence Service (SIS or MI6), established by the *Intelligence Services Act, 1994*, and the signals arm, the Government Communications Headquarters (GCHQ). (Todd & Bloch, 2003: 102, 103). The UK's intelligence services, including law enforcement intelligence had been involved over many decades with the internal strife related to Northern Ireland, which presented itself in the form of terrorist campaigns in various forms, including bombings and drive-by shootings. The immediate effect of the events of

11 September 2001 in the US was the establishment in the UK of a Joint Terrorism Analysis Centre (JTAC), a loose-standing structure consisting of representatives of 11 agencies and departments and which serves as the UK's "centre of excellence and expertise on assessing the threat from international terrorism". The terrorist threat from Al-Qaida in the form of terrorist attacks such as those on 7 July 2005 and 21 July 2005, involving explosions on the London transport network, led to a review of the intelligence services, namely MI5, MI6, and the Government Communications Head Quarters (GCHQ). The manner in which intelligence relating to WMD was dealt with also led to a Commission of Inquiry. The UK intelligence model needs to be analysed and compared with the US system, in particular the role of MI5 in relation to the combating of terrorism that needs to be analysed. Common features between the two models will be indicative of best practices and may serve as a benchmark for other countries. Firstly the broad crime intelligence framework of the UK, namely the *National Intelligence Model (NIM)* needs to be discussed and evaluated as a best practise, also in relation to the US.

3.2. *The National Intelligence Model*

The *National Intelligence Model (NIM)* complies with minimum standards in respect of all areas of policing. *NIM* is captured in legislation, namely the *Police Reform Act, 2002*, and is described as a "business model" for law enforcement (ACPO, 2005: 7). *NIM* is aimed at crime prevention, through crime analysis and understanding the incidents of crime, rather than simply responding to crime incidents. *NIM* furthermore envisages cooperation on local, national and international level to address local crimes as well as serious and organised crime through targeted operations by dedicated units. It is also aimed at improving intelligence sharing on local and national level between different government agencies and has been adopted by agencies such as the Serious Organised Crime Agency (SOCA) and the UK Immigration Services (ACPO, 2005: 12). Analytical options in *NIM* include crime pattern analysis; demographic/social

pattern analysis; network analysis; market profiles; criminal business profiles; risk analysis; target profile analysis; operational intelligence assessment; and results analysis (ACPO, 2005: 61).

NIM represents an intelligence-led policing approach, which includes the maximum access to all intelligence sources, a proper analytical process and capacity and the following intelligence products: Strategic assessments, that is, current and long-term issues affecting police; tactical assessments, relating to the day-to-day business of policing; target profiles to have a better understanding of an individual (victim or suspect) or a group; and problem profiles to better understand emerging crime or incident series, priority locations and other identified high risk issues, and to recommend opportunities for tactical resolution in line with control strategy priorities (ACPO, 2005: 64). Prevention, intelligence and enforcement are regarded as 'community police partners' in the *NIM*. The Strategic and Tactical Tasking Coordination Group is at the heart of the *NIM*. Like in the US system, access to community intelligence is also regarded as crucial in the UK system to integrate *NIM* with neighbourhood policing (ACPO, 2005: 121). Likewise, interagency sharing of intelligence, through established protocols is regarded as an important element of the *NIM* (ACPO, 2005: 121). *NIM* requires standardisation of processes and equipment and the integration of databases of partner intelligence and police agencies (ACPO, 2005: 118). Technical resources and expertise of other agencies must be available (ACPO, 2005: 144). *NIM* requires closer links between police services and external partners in the wider IC. It refers to the wider police family which includes wardens, rangers, traffic wardens, parish special constables, and volunteer associations such as neighbourhood and farm watches, as well as the establishment in many police forces of permanent joint intelligence units comprising of police, customs, immigration and other agencies (ACPO, 2005: 146). The *NIM* should be interpreted in the context of the *National Security Strategy of the UK*, which is dealt with hereunder.

3.3. The National Security Strategy of the United Kingdom

In the *National Security Strategy (NSS) of the UK*, terrorism, the proliferation of nuclear weapons and other WMD; and transnational organised crime are identified as being amongst the main threats to the UK (UK, 2008(a): 10 -13). It is stated that in addition to the traditional forces who were relied on in the past to address national threats, such as the police, border police, armed forces and civilian intelligence agencies, that there must be a greater involvement with business and local authorities and communities to plan for emergencies and to counter extremism (UK, 2008(a): 8). The *NSS* underlines the fact that there is a common thread between international crimes as drivers of threats to security, namely the transnational nature thereof, the role of non-state actors and the effect of dysfunctional states. The link between transnational organised crime and terrorism is also pointed out (UK, 2008(a): 22, 23). The main aim of the strategy is to ensure integration of government effort. In respect of intelligence structures structural changes are not recommended, but the important contribution of the following initiatives and strengthening them are confirmed: (UK, 2008(a): 4)

— The establishment of the Joint Terrorism Analysis Centre in 2003;
— the implementation of the cross-government counter-terrorism strategy (CONTEST) and cross-government counter-proliferation framework in 2006;
— the establishment of SOCA in 2006;
— the establishment of the Office for Security and Counter-terrorism, which is responsible to manage the cross-government counter-terrorism effort; the announcement of the new UK Border Agency; and
— the establishment of a new Cabinet Committee on National Security, International Relations and Development, in 2007.

The *NSS*, does however, envisage a National Security Forum, including representatives from government, politics, academia and others to discuss strategy and exchange ideas (UK, 2008(a): 60).

The UK has a separate strategy for countering international terrorism providing further guidance also of importance in respect of intelligence and the combating of international crimes.

3.4. The United Kingdom's Strategy for Countering International Terrorism

The *UK's Strategy for Countering International Terrorism* is a culmination of a continuous process of reviewing the intelligence structures relating to terrorism, initially capitalising on the UK's experience with domestic terrorism, and later influenced by the terrorist attacks of 11 September 2001 in the US and subsequently terrorist attacks in the UK, linked to Al-Qaida. The changing role of MI5 is firstly analysed.

3.4.1. The role of the Security Service

MI5 is, as already mentioned, a civilian domestic intelligence agency and is responsible for protecting the UK against covertly organised threats against national security, including terrorism, espionage and the proliferation of WMD. MI5 took over the overall intelligence coordination relating to the combating of the terrorist threat to the UK from Northern Ireland in 1992. The problems experienced at the time, and which led to this step, are described as follows: (Dillon, 1994: 178)

> The war against the IRA in Britain was always fought against the background of rivalry and squabbling within the security apparatus, which includes the army, MI5, MI6, the Anti-Terrorist Squad at

> Scotland Yard and regional police forces. There was a lack of co-ordination of anti-terrorist policy and a feeling within each grouping that the others were inadequately shaped for combating the IRA. One could compare it to a large bureaucratic structure where inter-departmental rivalry results in the non-sharing of information.

It is apparent that there were also no "strictures" or guidelines for agents used in the intelligence war in Northern Ireland. The work done by an agent of military intelligence to provide loyalist murder squads with details of the lifestyles of republican sympathisers, members of Sinn Fein and suspected IRA sympathisers and members were used by MI5 to expose the 'dirty war' of the military and to gain control of intelligence operations in the region (Dillon, 1994: 185). MI5 imposed strict rules on the other intelligence services about the handling of agents and the security of information provided by those sources and to guard against using *agent provocateurs.* The Task Co-ordinating Group was set up to coordinate all operations and use of agents (Dillon, 1994: 195, 196). MI5 closely supports the 56 police agencies in the UK to combat terrorism and gathers clandestine and open source intelligence information about the covert activities of suspected terrorists; assesses the threats emanating from such activities; takes appropriate actions to prevent or deter terrorist acts; and where appropriate shares information with other agencies and law enforcement.

The police forces are responsible to pursue counter- terrorism investigations by collecting evidence for use in legal proceedings with a view to criminal prosecutions (US, 2003(b): 6). The practical working arrangement between MI5 and the police is implemented through Executive Liaison Groups (ELGs). The ELGs provide a secure forum to safely share secret, sensitive and raw intelligence exchange with the police. This intelligence forms the basis for decisions on how to best gather evidence to prosecute suspects in court. Although the respective organisations work in partnership, MI5 takes the lead in collecting, exploiting and assessing intelligence, while the police take the

responsibility for the gathering of evidence, obtaining arrests and preventing risks to the public. ELGs meet regularly and are vital to the coordination of operations. They are kept abreast of developments in the investigation; and coordinate responses to developments and decide when to act, such as when to execute arrests or when to transfer the overall responsibility from MI5 to the police (UK, 2009(a): 8). There is also a special relationship between MI5 and what are called police Special Branches. Police Special Branches' function is to gather intelligence about security threats by various means and to assess this with a view to safeguarding the public and improving the functioning of local police. They also assist MI5 in countering terrorist threats. MI5 determines the priorities of Special Branches to gather national security-related intelligence. MI5 could also request Special Branches to run checks, which could assist MI5 investigations, without giving the Security Branches the background to the request (the need-to-know principle). The relationship in this regard has, however, improved from the need-to-know principle to the need-to-share principle (UK, 2009(a): 71). In this regard the UK model, namely to have a separation between domestic intelligence and law enforcement, was considered in the US, but it was foreseen that it would lead to a lack of coordination in view of the +13 000 state and local law enforcement agencies in the US (US, 2003((b): 8). It seems as if both a civilian domestic intelligence service, such as MI5 and a law enforcement agency which has intelligence functions, may fail to the same extent to coordinate and share intelligence. Creating a domestic civilian intelligence service in the US may not necessarily ensure that further terrorist attacks will not take place (Burch, 2007: 20).

3.4.2. Review of Intelligence preparedness following the London terrorist attacks on 7 July 2005

Following the terrorist attacks on the transport network in London on 7 July 2005 (three explosions of improvised explosive devices in the underground train system and one on a bus), the *Report into the London Terrorist Attacks on 7 July*

2005 was compiled by the Intelligence and Security Committee (ISC), an independent Parliamentary body whose role it is to examine the work of civilian intelligence agencies, in which the following were examined: the possibility that intelligence which could have prevented the attacks might have been overlooked; why the threat assessment level before the attacks was lowered and the effect thereof; and the lessons learnt as a result of the attacks (UK, 2006(b): 4). The report refers to the interaction between the respective agencies, pointing out that "Intelligence on terrorist activity in the UK, may come, for example from communications between terrorists intercepted by the GCHQ, from agents controlled by MI6 inside terrorist cells or networks overseas (connected back to the UK), from foreign liaison services, from physical surveillance by the Security Service or the police of terrorist or extremist activity in the UK, or from agents run by the police within those networks in the UK." (UK, 2006(b): 6). The report clearly acknowledges the limitations to intelligence, namely the impossibility of knowing everything, intercepting all communications, or within the process of prioritisation to always give the correct weight to every issue, within the overwhelming volume of intelligence (UK, 2006(b): 7). It is pointed out in the report that the IC was aware that the threat was bigger than the capacity to deal with it, hence strict prioritisation of intelligence targets (UK, 2006(b): 30). A major recommendation in the report is to increase coverage of terrorist threats not only overseas, but also domestically in the UK, by ensuring a regional presence of MI5 (UK, 2006(b): 35). A key lesson from the 7 July 2005 attacks is the value of close cooperation between MI5 and the police (UK, 2006(b): 36). At the same time it is important that police are not "removed from their local roots".

3.4.3. Review of the Intelligence on the London Terrorist Attacks on 7 July 2005

The report titled *Review of the Intelligence on the London Terrorist Attacks on 7 July 2005* followed the *Report into the London Terrorist Attacks on 7 July 2005*, with more focused attention on the fact that two of the 7 July 2005 bombers

featured in a previous investigation, codenamed Operation Crevice. Operation Crevice was a successful investigation which led to one of the longest terrorist trials in the UK, and in which five men were convicted for planning to explode a fertiliser bomb in the UK. At the time when MI5 was investigating the Operation Crevice suspects, they were in contact with two unidentified men- later identified as Mohammed Siddique Khan and Shazad Tanweer, two of the London (7 July 2005) bombers. The ISC investigated the question why, in view of the fact that MI5 came across these suspects, they were not able to prevent them from committing the attacks (UK, 2009(c): 3). The extent of Operation Crevice was huge with 45 000 man-hours devoted to monitoring and transcription, and 34 000 man-hours of surveillance, in addition to other investigative methods (UK, 2009(c): 9). In addition to the massive overload of work in the investigation, it became clear that an attack was imminent leading to arrests at a stage when MI5 would have preferred to gather more intelligence. Following up on intelligence gained from Operation Crevice, the police were successful through Operation Rhyme to arrest further suspects who planned coordinated attacks by parking limousines packed with gas canisters in underground parking areas and exploding them. It was planned to put radiological material in the devices to form crude “dirty bombs” (UK, 2009(c): 12). Numerous follow-up operations were launched, related and unrelated to the Crevice and Rhyme Operations, without uncovering new plots (UK, 2009(c): 14). The report shows that the IC did what they could within their constraints and with intelligence that was available at the time.

A solution to prevent the recurrence of suspects ‘getting lost’ in an investigation or are not prioritised, is the establishment of what is referred to as ‘legacy teams’, which must reflect on previous operations as well as on the suspects in those operations, and make a new assessment of what must be followed up. The advantage of this method has already becoming apparent in terms of adding to the knowledge of terrorists and in particular to analyse the way terrorists work; connections between operations and possible future targets for attack; and

improving the intelligence agencies' understanding about how best to deploy their resources during operations (UK, 2009(c): 46). Another initiative is to improve the storing and accessing of information, to ensure effective exploitation of intelligence, which assists investigators to better identify targets (which may be terrorists and their associates) or other persons who may lead to identifying terrorists from fragmentary information, analyse their activities, establish connections between people and help focusing limited resources (UK, 2009(c): 47). MI5 has also implemented the recommendation of establishing regional offices previously referred to. This has led to increased intelligence coverage, including an increase in local intelligence sources, faster response capabilities and better coordination with police investigations. The police also reacted by establishing an additional three counter-terrorist units with both an intelligence- and investigative capacity (UK, 2009(c): 52). The report underlines the importance of assistance that local communities and organisations can give in combating terrorism.

The UK has developed a particular strategy in order to counter international terrorism.

3.4.4. United Kingdom's Strategy for Countering International Terrorism

The *UK's Strategy for Countering International Terrorism*, developed in 2003, revised in 2006 and updated in 2009, is based on four principles referred to as 'PREVENT', 'PURSUE', 'PROTECT' and 'PREPARE' (UK, 2009(a): 13). In respect of intelligence and intelligence cooperation 'PURSUE' and 'PROTECT' are of particular importance. 'PURSUE' refers to the gathering of intelligence regarding the terrorist threat; disrupting terrorist activities through prosecution and other means; and international cooperation with partners and allies overseas to strengthen the intelligence effort and disrupt terrorists outside the UK. 'PROTECT' covers issues such as strengthening border control; working with the private sector to protect key utilities (referred to as the Critical National Infrastructure) and to protect against attacks by means of technological advances

and protection of persons going about their daily activities (UK, 2009(a): 14, 15). MI5, MI6, the GCHQ and the police forces are the main role-players in respect of these two pillars of 'PROTECT'. The UK provides extensive training and other assistance to foreign governments in order to build their capacity to counter terrorism. The Border Management Programme, aimed at amongst others, the improvement of intelligence sharing in support of border operations includes the issue of e-borders and the use of biometrics in identifying suspect travellers, initiatives which have been referred to in Chapter 5 (UK, 2009(a): 16). The Foreign and Commonwealth Office, in conjunction with the law enforcement and positive intelligence agencies, plays an important role in understanding and combating of radicalisation, supporting reform, sharing of intelligence, assisting governments in improving their counter-terrorism capabilities, organising joint counter-terrorism exercises and promoting joint action against known terrorists.

The manner in which intelligence on WMD was dealt with by civilian intelligence agencies and the government also initiated a review of intelligence processes in the UK, and is of importance to this study in view of the focus on international crimes such as the proliferation of WMD.

3.5. Report on the Review of Intelligence on Weapons of Mass Destruction

This inquiry is similar to the inquiry in the US regarding WMD. The Review Committee was tasked in February 2004 to investigate the intelligence coverage on the programmes on WMD in countries of concern; on the global trade in WMD; to investigate, with hindsight what was known about Iraqi WMD until March 2003; to evaluate discrepancies between the intelligence gathered, analysed and used before March 2003 and the findings of survey teams later-on; and to make recommendations on the future gathering, evaluation and use of intelligence (UK, 2004: 1). The Review Committee underlined the value of the information provided by the International Atomic Energy Agency (IAEA) and the

UN Special Commission (UNSCOM). It recommended that the contribution of such international organisations need to be built on for the future, in addition to the capacity of national intelligence sources. The Committee also recognised the need to create a virtual network of expertise on WMD. In particular the need to integrate the work of the Defence Intelligence Staff (DIS) with the rest of the intelligence community and to create channels for dissent with evaluations of the DIS was recognised.

The present model in the UK for dealing with crime intelligence in relation to organised crime needs to be analysed as it relates in some respects to the FBI in the US, but also has characteristics which are relevant as a benchmark for intelligence and intelligence cooperation on national level.

3.6. The Serious Organised Crime Agency

Before the establishment of SOCA the UK did not have the equivalent of the US FBI, in respect of either law enforcement or crime intelligence. The establishment of SOCA, through the *Serious Organised Crime Act, 2005,* reflects in various ways a dramatic transformation of and a total new approach in respect of crime intelligence and law enforcement in the UK, and is to a large extent a reaction to the multitude of intelligence agencies in the UK, such as MI5, MI6 and the GCHQ. The duplication of functions came about as a result of the fact that the respective agencies were established to address specific needs at the time of establishment. This led to a lack of sharing of information, as well as a lack of coordination between the respective agencies. The need for secrecy and fear of compromise also stifled any move to centralised databases, standardisation and interoperability of electronic communications system, all of which are requirements for effective sharing of information (Segell, 2007: 218). The mindset of what constitutes intelligence and analysis thereof has changed from the over-emphasis of secrecy towards "openness, transparency, civic consultation and participation in the political debate" (Segell, 2007: 219). SOCA had, for example

established by the end of 2008 mutually beneficial relationships with hundreds of businesses, trade associations and regulatory bodies (UK, 2009(b): 32). A major catalyst for the establishment of SOCA, is the ongoing transformation of the EU and its organisations, and the openness of borders in the EU, which necessitates closer cooperation between the respective countries of the EU to combat those crimes where jurisdiction is abused for impunity and crimes which are committed across international borders, such as the international crimes dealt with in this study. The limited counter-terrorism role of SOCA in respect of the financing of terrorism developed as a result of the fact that 60 percent of members of 'paramilitary organisations' in Northern Ireland have turned to organised crime (Segell, 2007: 220).

SOCA has been established in addition to the existing intelligence agencies as well as the existing police services and military intelligence units in the UK, but at the same time consolidated intelligence activities and law enforcement (Segell, 2007: 220). SOCA is described as UK's first non-police law enforcement body (Segell, 2007: 220). SOCA is also the UK's National Financial Intelligence Unit, which receives suspicious transactions reports. The National Criminal Intelligence Service (NCIS), the National Crime Squads and investigators of the Customs and Immigration Services were amalgamated into SOCA, which commenced in 2006 with a staff complement of 4 000, of which half were criminal investigators and half analysis and intelligence personnel. SOCA has 120 liaison officers, based in 40 countries around the world (Segell, 2007: 217). To appreciate the unique composition of SOCA, it is necessary to expand on some of the agencies which were integrated into SOCA. The NCIS housed the UK National Central Bureau of INTERPOL, and its 500 strong staff complement was drawn from the police, Customs and Excise and the Home Office. SOCA also acts as the gateway for UK law enforcement for a wide range of specialised services through INTERPOL, Europol and Schengen. In the period 2008/2009 SOCA acted as a gateway for 155 000 messages which generated some 27 000

cases of which 23 per cent were carried out on behalf of Association of Police Chiefs (ACPO) forces (UK, 2009(b): 32).

The NCIS was one of the first services in Europe to deal with crime intelligence on a national scale. The NCIS gathered intelligence on drug traffickers, money-launderers, organised criminal groups, paedophiles and soccer hooligans. It focused on the highest echelons of crime and assisted police and other agencies in the UK and elsewhere (Pike, 1997). The National Crime Squad (NCIS) was launched in 1998 by the amalgamation of six regional crime squads. The NCIS's investigative focus was on serious drug trafficking; illegal arms dealing; money-laundering; contract killing; counterfeit currency, kidnap and extortion. The High-Tech Crime Unit was part of the NCS and was a national law enforcement agency tasked to combat serious and organised cyber crime on national and international scale (Segell, 2007: 222).

To fulfil its national and international roles, SOCA has established Regional Intelligence Cells (RICs) in the UK and at the same time strengthened cooperation with Europol; the EU Joint Situation Centre; the Intelligence Division of the EU military staff; and the EU Satellite Centre also referred to in Chapter 3 (Segell, 2007: 220, 224). The international involvement of SOCA is of particular importance as it took over some of the liaison functions of the Foreign Office. SOCA is involved in the G8 countries' Lyon Group, responsible for the "improvement of cross-border sharing of intelligence information; to prevent and disrupt terrorist activity and prosecute terrorists; for effective use of advanced investigative techniques such as interception and undercover agents; an enhanced legal framework with states criminalising and prosecuting terrorist activities… tackling passport fraud; faster operational action to tackle attacks on computer networks; and faster cooperation in tackling Internet related crimes such as child pornography" (Segell, 2007: 224).

SOCA investigators closely cooperate with specialist prosecutors, who will remain answerable to the National Prosecution Service, and will be available when required to provide "comprehensive, practical and specialist advice to help shape investigations and develop strong and well-presented cases for prosecution". These prosecutors are expected to become involved in cases from an early stage and to work alongside investigators until conclusion of the prosecution "wherever it would make good operational sense" (Segell, 2007: 226). SOCA would differ from MI5 in that MI5 officers do not have powers of arrest. The intelligence mandate of SOCA is the same as that of traditional police forces, namely limited to the investigative powers of amongst others, surveillance, interception and use of covert human intelligence sources, as provided for in *RIPA*. SOCA officers have the multiple powers of police, immigration and customs, and is further supported through the use of the following powers: (Segell, 2007: 227).

— The power to prosecutors to make statutory deals for immunity or reduced sentences;
— a power to courts to make orders for a period up to 20 years to force criminals to provide bank statements, to ensure they have no crime-related earnings; and
— a power to courts to issue disclosure notices to force suspects to provide documents under threat of prosecution, but without the information being used for trial.

The personnel of SOCA include detectives, specialist civilian investigators, financial analysts and computer experts. SOCA is subdivided into four directorates, respectively responsible for intelligence (to gather, assess and use intelligence); enforcement (for an operational response to threats and basically investigating, or building court cases); intervention (to disrupt criminal activities through particularly the freezing and seizing of criminal assets) and corporate services, to support, facilitate and develop the capabilities of SOCA (Segell, 2007: 235). It is clear that SOCA is an innovative further step in the

transformation of intelligence and law enforcement in the UK and its success or not will certainly form the basis of further transformation. The problem has already been identified that the RICs referred to above, have been established with the aim to collect information from the communities in which potential terrorist extremists can receive support and sympathy, but despite the growth in numbers of the RICs there currently exists no nationwide database for the sharing of counter-terrorism intelligence. Instead, reliance is placed upon personal relationships and communications creating vulnerabilities to security. It had been proposed that in the longer run, the counter-terrorism role of SOCA could be extended from only terrorist financing to using its 'revolutionary' broad nationwide mandate to "build intelligence networks and investigative and disruptive capabilities with an international reach and presence" (Hindle, 2007: 40, 41). It has also been pointed out that the issue of independence or sovereignty of civilian and crime intelligence agencies is becoming increasingly irrelevant and potentially obstructive in the conduct of counter-terrorism investigations (Hindle, 2007, 39).

4. CONCLUSION

There are numerous common areas between the US and UK models of interagency intelligence cooperation. Firstly in terms of the policing model it is vital that policing should be intelligence-led. Secondly, there must be a mindset change from excessive secrecy to a community based intelligence system, involving the private sector as widely as possible. In both the US and the UK the systems to provide a wide local coverage of intelligence within communities such as immigrant communities where terrorists may found refuge, have the same shortcoming, namely the excessive or singular focus on intelligence regarding terrorism instead of an all-crimes approach as in some fusion centers in the US. The reasons for an all-crimes approach are logical - the fusion centers in the US and RICs in the UK are expensive to maintain on a national level. Although intelligence on terrorism needs such coverage, the main crime threats in many

communities are not terrorism, and their commitment and therefore the sustainability of these structures is dependant on the local needs to be effectively addressed through those structures. In addition it is clear that in many instances terrorists have reverted to common crimes and by focusing on intelligence on terrorism alone may defeat the purpose for which these structures were established.

The establishment of SOCA in the UK is evidence that it is sometimes important to integrate some structures rather than proliferating intelligence and law enforcement structures. The transformation of intelligence structures in the US post-11 September 2001 did not address the multitude of agencies with overlapping mandates. More intelligence structures were established and there was a serious debate on whether it was necessary to establish a domestic intelligence agency in the US, based on the MI5 model in the UK. This was decided against. The office of the DNI was established by statute on 17 December 2004, which is positive in terms of the coordination of intelligence. In addition the Department of Homeland Security was also established on 25 November 2002, eventually integrating border security, immigration, customs immigration and crime intelligence functions. The Department of Homeland Security in the US is a huge Department with multiple functions, but has a much wider focus than SOCA, which has organised crime as main focus. The establishment of SOCA in the UK also underlines the importance of having an intelligence capacity in law enforcement structures- also similar to the FBI in the UK. In respect of a separate domestic security or intelligence agency, it is regarded as useful, but might depend on the constitutional dispensation of a country. In the US, for example it is not regarded as conducive to the preservation of civil rights to have such a domestic civilian intelligence agency.

The essence of an effective intelligence system is to have at least one agency or institution which has access to all intelligence and to have a centralised database. In the UK the RICs weak point is that despite wide intelligence

coverage there is no such central database, forcing reliance for cooperation in respect of and sharing of intelligence, on personal relationships. Such centralisation is necessary in order to be able to 'connect the dots'. In this regard a number of phrases need to not become mere clichés, but principles of information and intelligence sharing and cooperation, namely 'a common intelligence environment', 'single information environment'; 'integration of all sources of intelligence'; 'joint operational planning'; 'integrated intelligence enterprise' and 'joint action'. Despite the events of 11 September 2001, the very clear recommendations of various Commissions of Inquiry and the fact that it had been identified as a major stumbling block even before 11 September 2001, interagency rivalry and interagency 'turf battles' remain a major stumbling block for interagency intelligence sharing and cooperation. The respective agencies must relinquish some authority (sometimes even referred to as 'sovereignty') for the sake of joint planning, but must retain operational responsibility. Independence of agencies, even police agencies, is regarded as irrelevant and 'destructive'. Another common problem in the US and the UK is that of capacity to deal with the intensive type of investigation required to follow up all leads on a national scale in view of what can often be described as an overload of intelligence. This factor necessitates proper methods of prioritisation of targets.

The most frustrating intelligence failure is to find that some intelligence targets have slipped the net and committed atrocities such as the London bombings. A best practice developed from this in the UK is the establishment of legacy teams to review closed investigations and to follow up some leads which were previously not prioritised, or which can be enriched with new information. Most important to successful intelligence cooperation seems not to be structures, but rather mindsets, such as the deeply imbedded intelligence principle of "need-to-know" which must be replaced by the principle of "need-to-share". In the new intelligence structures the notion of agencies to regard them as 'owners' of intelligence has no place. In Chapter 4, the factor of mistrust was pointed out as one of the major stumbling blocks which inhibit information sharing. To overcome

mistrust, it is important to establish a 'trusted information environment', through the vetting of personnel, securing and controlling access to databases especially central databases with applicable levels of access related to the levels of sensitivity, and securing communications lines.

Another important element for successful intelligence cooperation is leadership. All the necessary intelligence structures and policies could be in place in a country, but successful cooperation and sharing of information and intelligence to enhance day-to-day operations as well as longer term strategic goals, require constant effort and leadership. Interagency information and intelligence sharing should exist between all members of the positive IC and law enforcement. The notion that law enforcement is part of the broader IC must be nurtured. In the UK such cooperation also includes game wardens and local authorities. If an ideal or model interagency intelligence system should be devised, it should have the following elements:

— An office with overall power in respect of the whole IC, including law enforcement (crime) intelligence, like the DNI in the US.
— There should be a similar if not the same accountability or review system in respect of the activities of the whole IC.
— A comprehensive framework for intelligence should be established such as the NIM in the UK.
— There must be a national coordination mechanism on which all agencies are represented, such as the National Counter Terrorism Centre in the US and the Joint Terrorism Coordination Centre and the Joint Terrorism Analysis Centre in the UK.
— Policing must be community based and intelligence-led and information gathering should give the maximum coverage into communities, involving civil society. Fusion of intelligence should take place on the local as well as regional and national levels- in line with the examples of the RICs in the UK and the fusion centers in the US.

- Intelligence focus should not be limited to terrorism, but also serve local communities, by following an all-crimes approach.
- Law enforcement focusing on international and transnational crimes should function on a multi-disciplinary basis with powers of police, immigration and customs integrated into the same agency, as with SOCA.
- Cooperation should also take place between law enforcement and the prosecution, as in the UK and the US from an early stage of the investigations.
- Secure communications lines must be established as well as secure databases and security enhanced by vetting and controlled access to databases (create a trusted information network). Vetting is a slow process and might need to be improved.
- Duplication of intelligence structures with overlapping mandates must be avoided by integrating such structures into a single unit, as happened with SOCA.
- Policies to delineate the respective roles of the agencies in the positive IC and crime intelligence fields as well as to address attitudes in relation to intelligence must be in place.
- There must be an award system in place to award sharing of information or intelligence.

In the next chapter intelligence sharing and cooperation in respect of international crimes are analysed on the regional level within and between regional agencies and national and international organisations.