TABLE OF CONTENTS

CHAPTER 1
INTRODUCTION

CHAPTER 2
INTERNATIONAL CRIME AND INTELLIGENCE:
A CONCEPTUAL FRAMEWORK

CHAPTER 3

IMPERATIVES FOR INTELLIGENCE CO-OPERATION

CHAPTER 4
CHALLENGES FOR COOPERATION: CIVILIAN INTELLIGENCE AND LAW ENFORCEMENT

CHAPTER 5:
INTELLIGENCE METHODOLOGIES OF CRIME INTELLIGENCE AND POSITIVE INTELLIGENCE: COMMON GROUND

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

CHAPTER 7
MODELS FOR INTELLIGENCE COOPERATION ON THE REGIONAL LEVEL

CHAPTER 8
MODELS FOR INTELLIGENCE COOPERATION ON INTERNATIONAL LEVEL

CHAPTER 9
EVALUATION

CHAPTER 1
INTRODUCTION

1. IDENTIFICATION OF THE RESEARCH THEME

Within the Western context, intelligence collection during the Cold War primarily focused on the Soviet Union. Some of the major threats which need to be addressed presently are terrorism, transnational organised crime in all its manifestations and crimes related to weapons of mass destruction (WMD). In respect of methodology, the focus in many countries was on signals intelligence (SIGINT), rather than on human intelligence (HUMINT). The events of 11 September 2001 in the United States of America (US) were watershed events, exposing the weaknesses of a lack of intelligence-sharing both nationally and internationally and the over-reliance on SIGINT (Johnson & Wirtz, 2004: 33).

The adoption by international organisations of a large number of international instruments dealing with crimes ranging from terrorism, to corruption and war crimes, resulted into what is referred to as 'international criminal law' (Van den Wyngaert, 1996: ix). This study has been undertaken with reference to 'international crimes', meaning those crimes which countries need to enact in their national legislation under obligations emanating from international instruments. The term includes terrorism; transnational organised crime, including drug offences and money-laundering; war crimes; genocide; crimes against humanity; crimes relating to the proliferation of WMD; mercenary offences; crimes against the environment; piracy; and corruption.

The term 'international crime' as opposed to 'transnational crime' is preferred for purposes of this study, in view thereof that for instance, war crimes and crimes against humanity, committed during a civil war are regarded as international crimes, but are not necessarily transnational, in other words, cross-border, in

nature. Many international crimes, such as terrorism might be committed within the national context: Therefore the term 'international crime' or 'crimes' is more descriptive. The focus of this study is on international crimes with major security implications. The term 'international crime' as used in this study therefore comprehends transnational organised crime; terrorism crimes; crimes relating to the proliferation of WMD; war crimes, genocide and crimes against humanity; piracy and crimes relating to mercenary activities.

Where reference is made to transnational organised crime, it is done within the context of the *United Nations (UN) Convention against Transnational Organized Crime* and its three supplementary Protocols. Although there are separate international conventions dealing with drug offences (such as the *Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (1988)*), those crimes, committed within transnational context, are also covered by the *UN Convention against Transnational Organized Crime*.

The combating of terrorism differs from other international crimes, in the sense that exclusive military options, and covert actions, are sometimes opted for to combat terrorism, rather than the criminal law option. This in itself complicates global intelligence cooperation in respect of terrorism, in view of diverse political views; a lack of a universally accepted definition of terrorism; and the fact that political, religious and ideological motives are inherent to terrorist activities.

In combating transnational organised crime and in particular drug trafficking, there is already a high degree of international cooperation in respect of law enforcement, but which still needs to be much improved in respect of intelligence cooperation and sharing. In the US, covert actions or operations may be used by law enforcement in respect of terrorism as well as other crimes such as drug trafficking. Both terrorism and transnational organised crime are increasingly viewed as impacting on national security. In the past the two phenomena were, however, seen as distinct. There are numerous links between transnational

organised crime and terrorism. Combating terrorism and transnational organised crime cannot be separated from each other. By focusing on the crime element of terrorism, it can be detected in ways which are not possible otherwise (US, 2005(d): 76).

Special investigative techniques may be employed to investigate international crime, which techniques bear close resemblance to some civilian intelligence gathering techniques, such as the use of agents and informers. The biggest common factor between the respective functions of law enforcement, including crime intelligence, and civilian intelligence, is clandestine intelligence gathering.

This in itself provides a common basis for intelligence cooperation. These special investigative techniques include undercover operations and controlled delivery and surveillance, including electronic surveillance. Cooperation between civilian intelligence, law enforcement (crime) intelligence and even military intelligence in combating crime was first evident in counter-drug operations. It is clear that this cooperation should be extended to all international crimes.

In the post-Cold War era, targets of law enforcement and civilian intelligence began to merge. To remain relevant, the broader Intelligence Community (IC) must have the ability to provide intelligence to all customers who can make use of it. Good, actionable intelligence is a force multiplier (Vetter, 1995: 2, 11). The intelligence target for both law enforcement and civilian intelligence, grew to such an extent that intelligence cooperation became a necessity to provide adequate coverage (Clough, 2004: 607). Intelligence cooperation is essential in technology transfer regimes, sanctions monitoring, the pursuit of potential war criminals, but most important regarding global terrorism and WMD (Clough, 2004: 608).

The failure of the respective law enforcement and intelligence agencies in the US to share available information timely is regarded as cause for a lack of advance knowledge and ability to prevent the 11 September 2001 terrorist attacks in

Washington, D.C., Pennsylvania and New York (US, 2001: 3). The lessons learnt from the Madrid train bombings prior to the Spanish elections in 2004, are that the three methodologies of intelligence analysis, namely: trends and patterns, frequency and probability, must be integrated. Furthermore, the success of intelligence analysis lies in the structure of each intelligence agency, and its relations with other government and non-governmental entities (Segell, 2005: 235).

In view of the international nature of international crime, there is a need for improved cooperation between positive intelligence (which includes both military and civilian intelligence) and law enforcement agencies. This need is valid both on the national and international level (Wilkinson, 2006: 205). Such cooperation is hampered and challenged by various factors, such as sovereignty between nations, the differences in methodologies of respectively law enforcement (crime intelligence) and positive intelligence, their legal and constitutional mandates and functions. Furthermore, some states provide a safe haven to criminals, and their civilian intelligence and law enforcement institutions are corrupted or at least infiltrated by criminal elements or manipulated by such elements by means of terror (narco-terrorism) on political, executive and judicial level.

National governments are willing to allow other governments' intelligence services and police only limited access to their secret intelligence. This is to protect sources of information, as a result of a lack of trust from fear of action against the government, and of fear to reveal weaknesses in their intelligence system (Wilkinson, 2006: 175). Intelligence is sometimes not releasable to any other nation, for reasons of national interest (Clough, 2004: 605). Alternatively there could be a general breakdown or lack of order or stability in a country, making cooperation with that country impossible. The methodology of civilian intelligence agencies in respect of their traditional role is in many instances not acceptable to law enforcement in terms of human rights standards, and legal requirements for admissibility of evidence.

Cooperation between positive intelligence and law enforcement (crime intelligence) could realise the primary objective of any intelligence agency to be efficient, namely, to prevent actions such as terrorism from developing beyond its incipient stage (Wilkinson, 2006: 73). Cooperation between law enforcement (crime intelligence) and positive intelligence (military and civilian intelligence) could be mutually beneficial. Police, in enforcing the law and their contact in combating crime within all levels of the community give them an "unrivalled bank" of information from which contact information can be developed (Wilkinson, 2006: 73). Police in many countries do have sophisticated intelligence services, gathering, analysing and using crime intelligence. Specialist anti-terrorist units seem to be a necessity (Wilkinson, 2006: 77). The same is probably valid in respect of other forms of international crime.

The view is held that serious intelligence cooperation is reserved for bilateral and trilateral level and not within regional, for example, European Union (EU), level. This is especially true of sharing raw intelligence data. The sharing of analyses and assessments on such regional level is, however, deemed important to elicit action from governments, where action is required (Wilkinson, 2006: 175).

Rivalry and duplication of functions between various intelligence agencies nationally is another challenge (Wilkinson, 2006: 73). Reference is made to "walls of separation", between law enforcement and civilian intelligence, within the US context, to prevent the use of intelligence techniques against citizens and legal residents of the US without obtaining court orders (US, 2001: 10).

It is predicted that intelligence relationships will continue to proliferate adding benefits of liaison, but increasing the possibility of compromise (Clough, 2004: 612).

It is clear that the particular international crimes, such as piracy, terrorism and crimes related to the proliferation of WMD pose specific challenges for cooperation. Intelligence within the UN similarly poses its own challenges.

2. STUDY OBJECTIVES

The main objective of the study is to identify ways of improving cooperation between law enforcement (crime intelligence) and positive intelligence (civilian and military intelligence), in combating international crime, on the following levels:

— At national level, namely between the respective law enforcement agencies and positive intelligence agencies within a state.
— On regional level, between particular regional organisations and their member states.
— On international level, between member states and particular international organisations and their member states, as well as between such organisations and regional organisations.

A secondary objective is to identify and analyse the respective challenges which inhibit intelligence cooperation between law enforcement and positive intelligence in combating international crime. With intelligence cooperation is meant broad cooperation and not only intelligence sharing. The challenges, and how they are dealt with, will be analysed on national, regional and international levels, also through the use of selected case studies.

In this study, these challenges are identified and analysed on the national level, with reference to particular case studies, notably the US, and the United Kingdom (UK). On national level the cooperation between the respective agencies in the countries involved in combating international crime through intelligence sharing and cooperation are assessed.

The intelligence fusion concept as it is being applied in the US, as well as the new approach to transnational crime as it manifests in the UK are analysed. Brief reference is made to relevant practices in other countries, such as Canada and the Netherlands. The fusion model is aimed at an even broader intelligence sharing within the IC, inclusive of law enforcement (crime intelligence), and military and civilian intelligence on the one hand, and information within the civil society, on the other. Attention is in particular given to the different objectives of crime intelligence and civilian intelligence, and the different methodologies employed. The commonalities are highlighted in order to find common ground for cooperation between law enforcement (crime intelligence) and positive intelligence agencies in combating international crime.

The countries referred to here have been selected in view of their particular experiences in combating international crime; and official inquiries launched after 11 September 2001 in those countries, with the mandate to investigate intelligence failures or problems. These inquiries revealed specific weaknesses relating to intelligence cooperation and sharing and led to wide-ranging proposals and initiatives taken in order to address the identified deficiencies.

On regional level, the example of cooperation between law enforcement and positive intelligence (military and civilian intelligence) within the EU and the Association of South East Asian Nations (ASEAN) are analysed, including the ASEAN Chiefs of Police (ASEANAPOL). In respect of the EU the Berne Group, the Counter-Terrorist Group, and Europol are studied and analysed.

Recent developments on the African continent are analysed, in particular the various law enforcement cooperation initiatives, and positive intelligence cooperation. The establishment of a Continental Early Warning Centre of the African Union (AU), and the AU centre to coordinate information on terrorism in Algiers, Algeria, are analysed. The Committee for Intelligence and Security Systems in Africa (CISSA) is another example of intelligence cooperation on

regional level, serving as platform also for broader international intelligence cooperation.

On the international level the examples of the International Criminal Police Organization (ICPO)-INTERPOL, commonly referred to as INTERPOL, and the UN are discussed and analysed. INTERPOL had to face challenges in playing an increasing role in combating terrorism, in view of the political nature of terrorism and the fact that the INTERPOL Constitution prohibits the participation by the organisation in any activities relating to politics (Article 3). Recently the Secretary-General of INTERPOL stated that the UK, amidst continuing terrorist threats, is totally under-utilising the INTERPOL database of 11 000 suspected terrorists (Dodd, Norton-Taylor, 2007).

Relationships between INTERPOL and ASEANAPOL are also investigated, in view of the historic agreement recently concluded between ASEANAPOL and INTERPOL.

The UN performs functions in respect of peace support operations, weapons monitoring, (Clough, 2004: 609), the monitoring of compliance with UN Security Council arms embargoes and obligatory sanctions relating to terrorism. The manner in which the UN, as an organisation consisting of Member States inclusive of most countries in the world, deals with intelligence, is important as a case study, in view of the challenge to balance interests of the collective as opposed to a single Member State – a problem which needs to be addressed by any organisation on international level.

The aim of the study is therefore to analyse these challenges and to identify means to improve cooperation both on national level, regional level and international level. Models in this respect, both in terms of structures and process have been studied, in order to make recommendations on how the cooperation between law enforcement (crime intelligence) and positive intelligence could be

improved. Best practices are identified. Possible solutions to improve intelligence cooperation on international, regional and national level are investigated, to determine models which could be applied. Ways of improving intelligence cooperation in a broad sense, namely not limited to intelligence sharing are proposed. One of the inhibiting factors is the admissibility of intelligence in courts of law.

A further secondary objective has been to compare the intelligence gathering techniques employed by law enforcement (crime intelligence), such as undercover operations, controlled delivery and surveillance, to the techniques employed by positive intelligence. Coercive intelligence operations are not restricted to the military and, without reference to any particular country, could include satellite reconnaissance, psychological operations/disinformation, proxy invasion, interdiction, assassination, industrial espionage, false-flag operations, covert ownership of assets, information system penetration and destruction, raids, break-ins, blackmail and entrapment, sabotage, electronic countermeasures, and *coups* support (Reismann & Baker, 1992: 11- 13). Many of the above actions imply actions which are legally untenable and unacceptable to courts and law enforcement. Nevertheless, covert action is allowed and regulated, with parliamentary oversight in many democracies. It is called the ultimate paradox to allow covert actions in a democracy (Treverton, 1987: 222). The use of covert action by positive intelligence as a possible obstacle in the way of cooperation between law enforcement and positive intelligence is investigated in this study. The Central Intelligence Agency's (CIA) covert actions during the 1960's and 1970's are examples in this regard, exposed in the recently released so-called "Family Jewels" Dossier (US, 2007(c)).

The 11 September 2001 events in the US are regarded as a watershed which served as a driver for closer intelligence cooperation between law enforcement (crime intelligence) and civilian intelligence on all levels described above. This study therefore primarily focused on the period between 11 September 2001 up

to the end of 2007. Some more recent developments regarded as of importance to the study has, however, also been included.

During the post-Cold War era, intelligence services were redirected to a large extent to focus on terrorism, transnational organised crime and WMD, in addition to their more traditional role relating to intelligence gathering on national interest issues. Within international organisations such as INTERPOL and the UN, the focus also shifted to these crimes. Although the issue of intelligence sharing was topical within INTERPOL, Europol and on national level, the critical value and need therefore was acutely underlined by the 11 September 2001 events and led to numerous initiatives on the various levels to enhance intelligence sharing and cooperation.

3. LITERATURE SURVEY

The Council of Europe expresses the opinion that the convergence of security intelligence, meaning positive intelligence (military and civilian intelligence) and crime intelligence is problematic and "interlinking of networks will not be achieved without difficulty, if it is ever achieved at all." (De Koster, 2005: 39).

.

Numerous sources confirm the difficulties of intelligence sharing and cooperation. In addition, challenges to intelligence cooperation or factors inhibiting intelligence cooperation, such as mistrust, are dealt with separately in various sources, or only challenges to cooperation in respect of a particular type of intelligence, such as strategic intelligence, or challenges to intelligence cooperation only in respect of a particular international crime, such as terrorism, are discussed (Clough, 2004) (Canada, (No date): par 3.2.) (Walsh, 2006) (Ryan, 2006: 120-146).

There is a need for a comprehensive study in which all possible such challenges are determined and in which comprehensive proposals are made to address those challenges.

International organisations, law enforcement and the IC over a long period of time tended to deal with international crimes separately. An example is the development of international instruments on terrorism. As terrorist threats permutated from the hijacking of airplanes to bombings in public places, destruction of fixed platforms at sea, to the latest threat, namely that of possible access to and criminal use by terrorists of nuclear material, international organisations developed *ad hoc* international instruments in respect of each threat (UN, 2007(a)). After adopting 13 such counter-terrorism instruments to ensure maritime and aviation safety; to suppress nuclear terrorism and terrorist bombings and the financing of terrorism; to protect diplomats against violence and to criminalise hostage-taking, the UN structures have still been unable to complete the drafting of a comprehensive convention on terrorism.

In a similar fashion, the respective international crimes have been addressed in separate international and regional instruments with a huge overlap in respect of a number of areas of cooperation relating to mutual legal assistance; extradition; intelligence sharing and cooperation; technical assistance and assistance with special investigative techniques in law enforcement (Van den Wyngaert, 1996).

On national level there are in numerous instances a proliferation of law enforcement and intelligence structures, each with a limited mandate in respect of a particular crime or threat, also leading to a silo approach in relation to intelligence.

From the myriad of international instruments there is a need to identify common provisions in order to develop general principles for and obligations in respect of intelligence cooperation covering international crimes in general.

The adoption of the *UN Convention against Transnational Organized Crime* and its supplementary Protocols relating to trafficking in persons, trafficking in

migrants and trafficking in firearms heralded a new era of addressing international crime in a more holistic fashion. On an operational level, the development of units or capacities to address at least organised crime in a comprehensive manner is a trend that followed suit (Canada, (No date) (Das & Kratcoski, 1999).

Intelligence failures led to the institution of various commissions of inquiry in respectively the US and the UK, to establish the reasons for such failures and to address the same. In each instance this was done with reference only to a particular crime, such as terrorism or intelligence relating to WMD and within the context of a particular country with its unique composition of law enforcement and intelligence structures (UK, 2004) (US, 2003(c)) (US, 2004(b)) (US, 2005(c)) (US, 2008(d)) (Segell, 2005)). The bombings which took place in London, during 2005, led to further reviews of intelligence activities of both law enforcement and intelligence agencies in the UK, which are of importance with reference to interagency relationships (UK, 2006(b)) (UK, 2009(c)). The practice of rendition by the US led to a review of this practice in the UK, which review indicates important principles to protect human rights in intelligence cooperation (UK, 2007(a)). The said practice of rendition by the US also led to a report by the Special Rapporteur to the UN on the promotion and protection of human rights and fundamental freedoms while countering terrorism. This report proposes 35 good practices on legal and institutional frameworks for intelligence services and their oversight (UN, 2010).

Comprehensive plans, structures or strategies have been developed to address the particular failure within the particular country, with reference to a particular international crime, for example the *National Criminal Intelligence Sharing Plan* (US, 2003(a)); the *National Intelligence Strategy of the United States of America* (2005(b); the *National Strategy for Information Sharing: Successes and Challenges in Improving Terrorism-Related Information Sharing* (US, 2007(a); United States Intelligence Community: Information Sharing Strategy (US,

2008(a); Department of Homeland Security Information Sharing Strategy (US, 2008(b); *Department of Defence Information Sharing Strategy* (US, 2007(b); the *National Security Strategy of the United Kingdom: Security in an Interdependent World* (UK, 2008(a); the *United Kingdom Strategy for Countering International Terrorism* (UK, 2009(a)).

Logically such plans, structures or strategies will not all be applicable to other countries. However, there are best practices and strategies proposed in the various reports, which could be used universally. There was therefore a need to identify such best practices and strategies.

Only recently, studies pertaining to the convergence of certain crimes, such as transnational organised crime and terrorism identified common focus areas, which could lead to a holistic approach to both transnational organised crime and terrorism (De Koster, 2005). There was a clear need to investigate whether those focus areas could not also be used on an intelligence level to address all or most other international crimes.

In respect of special investigative techniques, namely undercover operations and controlled deliveries; and surveillance, including electronic surveillance, a compilation has been made by means of a questionnaire, of such techniques in Member States of the EU and a number of other countries (De Koster, 2005). These special investigative techniques are largely intelligence-based (use of surveillance, informants and agents). The research in this regard showed wide-ranging terminology and practices in the various laws and legal systems. In order to enhance international intelligence cooperation in this regard, a common understanding needed to be developed of the respective techniques. There was therefore a need in this study to develop, from the available laws, common terminology.

The available literature focuses respectively on the national level (US, 2001) (US, 2003(a)) (US, 2005(d)) (Vervaele, 2005) (Wilkinson, 2006) (UK, 2004); the regional level (Walsh, 2006) (Ryan, 2006); or the international level (Deflem, 2004, 2006) (Wilkinson, 2006), of intelligence cooperation. The main advantage of this study is that by describing and analysing all three levels in the same study, a novel approach could be followed in order to make proposals on how to improve intelligence sharing and cooperation on all levels.

Various reports of the UN, such as that of international commissions of inquiry into Darfur (UN, 2005(b)) and the fact-finding mission on the Gaza conflict ((UN, 2009(c)) provide insight into the investigation of war crimes, genocide and crimes against humanity. Manuals drafted by international tribunals, such as the *Best Practices Manual for the Investigation and Prosecution of Sexual Violence Crimes in Situations of Armed Conflict: Lessons from the International Criminal Tribunal for Rwanda* (ICTR, 2008) and the *Manual on Developed Practices of the International Tribunal for Yugoslavia* (ICTY-UNICRI, 2009) provide valuable guidelines on how to deal with information, intelligence and witnesses in investigations into war crimes, genocide and crimes against humanity.

Manuals and codes of practice in the UK and the US on intelligence practices are available, such as the *Guidelines on the National Intelligence Model* (ACPO, 2005); *Covert Human Intelligence Source Code of Practice* (UK, 2002(a)); *Covert Surveillance Code of Practice* (UK, 2002(b)); Interception of *Communications Code of Practice* (UK, 2002(c))*; Acquisition and Disclosure of Communications Data Code of Practice* (UK, 2007(b); *Investigation of Protected Electronic Information Code of Practice* (UK, 2007(c); The Attorney General's *Guidelines on Federal Bureau of Investigation Undercover Operations* (US, 2008(b); *Fusion Centre Guidelines* (US, 2006(c); and the *Attorney General's Guidelines for Domestic FBI Operations* (US, 2008(e)).

Information on the activities, mandates, and functions of the respective law enforcement and intelligence agencies, international organisations such as the UN and INTERPOL and regional organisations such as ASEAN, ASEANAPOL, and the AU are available on the Internet, especially on the home websites of these organisations.

This study was aimed at issues which are not covered in the available literature, namely to comprehensively identify and analyse challenges or blockages to intelligence cooperation on national, regional and international level; to make proposals to address such challenges; to identify from the various international instruments the common provisions relating to intelligence and law enforcement cooperation and obligations in that regard, in order to develop principles for intelligence cooperation; to develop common terminology relating to special investigative techniques; and to determine whether the intelligence focus areas developed from the convergence of terrorism and organised crime can be used in respect of other international crimes.

4. IDENTIFICATION AND DEMARCATION OF THE RESEARCH PROBLEM

Within the context of international crime, the study aims at identifying and analysing the challenges to cooperation between law enforcement (crime intelligence) and positive intelligence and to make recommendations in order to improve such cooperation. The study focuses on international crimes with major security implications, namely terrorism; transnational organised crime, including drug offences and money-laundering; war crimes; crimes relating to the proliferation of WMD and protection of nuclear material; mercenary offences; crimes against humanity; piracy; and corruption. The motivation for this selection is that especially transnational organised crime; terrorism, and crimes related to the proliferation of WMD, are regarded as serious threats to the security of

states. It is also clear that the intelligence and investigation methods required to combat these crimes have much in common.

The basic research question is: What can be done nationally and internationally to improve cooperation between crime intelligence and positive intelligence? Inquiries into intelligence failures revealed that a lack of cooperation between crime intelligence and positive intelligence contributed to such failures and that improved cooperation between crime intelligence and positive intelligence can be mutually beneficial to prevent and combat crime.

Secondary research questions emanating from this are:

— What are the challenges, blockages or factors inhibiting or preventing cooperation between law enforcement (crime intelligence) and positive (military and civilian) intelligence? The identification and analysis of particular challenges or blockages to intelligence cooperation will enhance the finding of solutions to remove such challenges or blockages, or mitigating their negative effects on intelligence cooperation.

— What has the recent response (post-11 September 2001), to these challenges been on national (interagency), regional and international levels in respect of intelligence cooperation and sharing? Following post-11 September 2001 resolutions were adopted by the UN Security Council, with an emphasis on complying with international obligations regarding cooperation to combat terrorism and crimes related to the proliferation of weapons of mass destruction. Countries such as the US and the UK responded on an unprecedented scale in respect of intelligence policies, structures and methodology.

— Are there best practices which on their own or in combination could be used to benchmark solutions for improved cooperation between crime intelligence and positive intelligence? The identification of best practices and determination of their applicability can be used to formulate solutions to improve intelligence cooperation on different levels.

— How can the sharing of intelligence, including "raw intelligence", be improved on operational level? The sharing of "raw intelligence" seldom takes place, except amongst the most trusted parties, mostly on bilateral level. For operational reasons "raw intelligence" is often required timeously to respond to a threat and it is therefore important to find ways to improve the sharing of raw intelligence on operational level.

This study is based on the following assumptions:

— Although the events of 11 September 2001 have led to increased emphasis on intelligence cooperation at the various levels, certain factors such as sovereignty and mistrust are still preventing more effective cooperation between crime intelligence agencies and positive intelligence agencies.
— Broad intelligence cooperation and sharing in respect of covert action and covert operations are highly unlikely.
— Intelligence cooperation needs to be very focused in terms of methodology, mainly clandestine intelligence gathering methods, especially human intelligence, within the context of special investigative techniques of controlled deliveries; undercover operations; and surveillance, including electronic surveillance.
— By operating in an incremental fashion, and on a project basis, trust can be built between the respective actors in order to promote future intelligence sharing.

5. METHODOLOGY

The approach to the study is descriptive and analytical. Given the aim of the study, namely to identify and develop guidelines and methods to improve cooperation between crime intelligence and positive intelligence in combating international crime, the theoretical approach to the study is based on a conceptual framework and analysis of international crime and intelligence

(Johnson & Wirtz, 2004). International crimes are largely defined in international instruments, but on a political level the definitional issue remains relevant in that there still is no universally accepted definition of terrorism and even of organised crime. The respective international instruments will be utilised as a common basis in this regard. Whilst it was realised that on international level intelligence sharing is mostly on the strategic level, the study was aimed at identifying methods and a framework for cooperation in the broadest sense, between crime intelligence and positive intelligence, and on how to develop confidence to share raw intelligence material in order to combat international crime effectively (Clough, 2004) (Walsh, 2006).

The primary sources which have been utilised include the US *National Criminal Intelligence Sharing Plan*, setting out solutions and approaches to improve the ability of the US to develop and share crime intelligence (US, 2003(a): 3); the *Report of the National Commission on Terrorist Attacks on the US*, which have been studied against the background of recent criticism regarding the recommendations of the report itself, and the manner in which the recommendations were actually implemented (US, 2004(b)); the report on the review of intelligence on WMD (UK, 2004); various reports to the US Congress on intelligence sharing and other intelligence issues (US, 2001) (US, 2003(b)) (US,2003(c)); the *National Intelligence Model* developed in the UK, establishing the concept of intelligence–led policing (ACPO, 2005); and the *Fusion Centre Guidelines* developed to enhance information sharing in the widest possible manner (US, 2006(c)). The above primary sources all deal with intelligence failures and deficiencies and propose remedial actions. These proposals have been described and analysed and from that a generally applicable framework for improving intelligence cooperation has been developed.

In respect of international crime, all the relevant international instruments on terrorism, organised crime and drugs are available electronically (United Nations Office for Drugs and Crime). Other relevant international instruments have been

compiled by Van Wyngaert (1996). The regional counter-terrorism instruments have been compiled by the UN (2001).

A compilation of the legislation of countries in the EU, the US and Canada pertaining to special investigative techniques to investigate terrorism provides a basis for analysing these techniques as understood in these countries. It has been used to develop common definitions of the respective techniques (De Koster, 2005).

An important secondary source was the research on intelligence analysis done by Shelley *et al*, (US, 2005(d)). In this source recognition is given to the problem that intelligence analysts are in effect overwhelmed by the sheer volume of intelligence. Intelligence methods, which relate to intelligence sharing and cooperation are analysed to determine the general application thereof in respect of the combating of all international crimes.

Other important secondary sources include the evaluation done by Ryan (2006) on criminal (*sic*) intelligence in the EU; the research of Deflem (2004, 2006) on international police cooperation, and that of Gerspacher (2002; 2005) on police cooperation institutions responding to transnational (cross-border) crime.

In respect of the role of intelligence within the UN, important secondary sources were Dorn (1999), Heide & Perreault (2004), Carment and Rudner (2006), and Champagne (2006).

6. STRUCTURE OF THE RESEARCH

Chapter 1: **Introduction**

This chapter introduces and outlines the study objectives, the need for the study, the structure thereof and the research problems that are addressed.

Chapter 2: **International crime and intelligence: A conceptual framework**

In this chapter the concepts used within the context of this study are explained. Concepts such as international crime, transnational organised crime, intelligence, civilian intelligence, human intelligence, domestic intelligence, foreign intelligence, military intelligence, signals intelligence, technical intelligence, crime intelligence, strategic intelligence and terrorism, are defined for purposes of the study. The importance of intelligence cooperation is specifically also discussed.

Chapter 3: **Imperatives for intelligence cooperation**

A short historical background on intelligence cooperation is provided and the watershed events such as the effect of the post-Cold War era and the 11 September 2001 events are discussed. The international obligations in the various conventions and resolutions of the UN Security Council; the African Union (AU); the Southern African Development Community (SADC) and the ASEAN pertaining to international information sharing and cooperation in respect of special investigative techniques are discussed in this chapter. Drivers for intelligence cooperation and sharing such as globalisation, the value for money concept, and the enrichment of intelligence, are discussed.

Chapter 4: **Challenges for intelligence/law enforcement cooperation**

The challenges for cooperation between law enforcement and civilian intelligence are identified and discussed in this chapter. Main challenges which have been identified are sovereignty; jurisdiction; lack of standards for communication and information technology; technical advances; secrecy and fear of compromise;

mistrust; the difference in focus and structure between law enforcement and positive intelligence; states which have no effective government; corruption in governments; and the rise of private intelligence and private security.

.

The different oversight mechanisms for law enforcement and positive (military and civilian) intelligence are also described.

Chapter 5: **Methodologies of law enforcement and positive intelligence**

The methodology of respectively law enforcement (special investigative techniques), and positive intelligence practices are analysed. The common areas, upon which cooperation between law enforcement and positive intelligence could be based, are identified.

Chapter 6: **Models for cooperation on national (interagency level)**

This chapter includes a number of case studies on national level. Firstly a case-study of the US post-11 September 2001. This includes an analysis of the 9/11 Commission, the *National Criminal Intelligence Sharing Plan*, the *Fusion Centre Guidelines* and how the 9/11 Commission's recommendations have been implemented.

In respect of the case study of the UK, the changing roles and functions of intelligence agencies enabling them to be able to combat terrorism and organised crime are analysed, including the role of MI5, the National Crime Intelligence Service, the Crime Squads and the recent establishment of the Serious Organised Crime Agency (SOCA).

Chapter 7: **Models for cooperation on regional level**

The models presented by intelligence cooperation within Europol, ASEANAPOL and the African Centre for the Study and Research of Terrorism (ACSRT), which is intended as an Early Warning Centre on terrorism, are analysed in this chapter, as well as the role of CISSA on the African Continent, linking with intelligence agencies globally.

Chapter 8: **Models for cooperation on international level**

In this chapter the models presented within INTERPOL and the UN are analysed.

Chapter 9: **Evaluation**

This chapter summarises the study; tests the main assumptions of the study, and presents the main findings and recommendations of the study. Recommendations on how intelligence cooperation on the national, regional and international level could be improved are made.

CHAPTER 2

INTERNATIONAL CRIME AND INTELLIGENCE: A CONCEPTUAL FRAMEWORK

1. INTRODUCTION

In this chapter, concepts such as international crime, transnational organised crime, intelligence, civilian intelligence, human intelligence, domestic intelligence, foreign intelligence, military intelligence, signals intelligence, technical intelligence, crime intelligence/criminal intelligence and strategic intelligence are defined within the context of, and for purposes of the study. In respect of many concepts there are no universally accepted definitions, making it even more important to outline what is understood in respect of such concepts. A proper definition of the respective phenomena regarded as international crimes is critical for legal regulation thereof and legal responses thereto. It is stated that without precise definition, ambiguities are created that allow terrorists and organised crime members to "slip through the cracks", and states may take advantage of uncertainties to expand room for maneuver in terms of targets and methods used against targets, in order to pursue other unrelated ends (Orlova & Moore, 2005: 61). In view of the importance of intelligence cooperation as focus of this study, concepts relating to intelligence cooperation are explained.

2. INTERNATIONAL CRIME

The term "international crime" had evolved over a period of time, initially referring to crimes by states. Crimes by states are now referred to as "serious breaches of obligations owed to the international community as a whole" (Amnesty International, 2001: Introduction: 2). Crime intelligence focuses on crimes

committed by persons or groups, whilst civilian intelligence also focuses on breaches of international law by states. A distinction is made between those crimes that reached the status of becoming part of customary international law, as *ius cogens* ("the compelling law"), and crimes over which universal jurisdiction needs to be established in terms of obligations stemming from conventions. In respect of crimes reaching the status of *ius cogens* all states are under an obligation to establish and exercise universal jurisdiction (Bassiouni, 1996: 65). Under universal jurisdiction is understood the ability to investigate or prosecute crimes committed outside the state's territory which are not linked to that state by the nationality of the suspect, or of the victim or by harm to the state's own national interest (Amnesty International, 2001: Introduction: 1). The term international crime is popularly used, "sometimes loosely", by scholars, governments and courts. (Amnesty International, 2001: Introduction: 2). There has been skepticism about the term 'international criminal law' or a discipline by that name. The counter-argument is that in recent years so many 'instruments' (dealing with the various aspects of international criminal law) "have been drafted that it has become very difficult to find one's way in the labyrinth of international criminal law treaties" (Van den Wyngaert, 1996: ix).

Following the terrorist events of 11 September 2001, in the US, "additional status" and impetus were given to the existing counter-terrorism instruments in terms of binding Chapter 7 of the United Nations Charter resolutions taken by the UN Security Council, such as Resolution 1373/2001, of 28 September 2001. This Resolution calls on states to become parties to the respective conventions and protocols. Some of these Conventions, such as the *International Convention for the Suppression of Terrorist Bombings, 1997,* require at least an extended or extraterritorial jurisdiction. This extraterritorial jurisdiction is not really universal in the sense that it is still linked to offences committed in the territory of the state, vessels flying the flag of the state, aircraft operated by the government of the state, committed by a national or stateless person who has his or her habitual residence in the territory of that state, or if the victim is a national of the state, the

offence was committed against a state or government facility of the state, or to compel that state to do or not to do something. (UN, 2001(a): 103, 104, Article 6) Extraterritorial jurisdiction in respect of the predicate offences mentioned in the *UN Convention against Transnational Organized Crime* is also limited.

In this study the term 'international crime' is used as a collective for those crimes which need to be established in national laws of states in terms of obligations under international law. For purposes of this study it is irrelevant whether those obligations emanate from *ius cogens* or instruments such as international conventions or protocols. The jurisdictional issue, namely whether a particular international crime had been enacted in the national law of a particular country is, however, of importance, as it impacts on cooperation and providing safe havens for criminals in countries which have not enacted the legislative framework required by international law.

In respect of some international crimes, there is truly universal jurisdiction, in the sense that those crimes may be prosecuted in national courts, or in international courts or tribunals, such as the International Criminal Court (ICC), established by the *Rome Statute of the International Criminal Court.* Crimes which may be prosecuted in the ICC are war crimes, crimes against humanity, and genocide.

Although international instruments have been adopted in respect of international crimes, defining those crimes and requiring the enactment of those crimes in the national laws of States Parties to those conventions, by institutions such as the UN, not all Member States of the UN are parties to those conventions. In many instances even states who are parties to such conventions have not yet enacted the required offences or provided through legislation for the required jurisdiction.

International crimes include war crimes, genocide and crimes against humanity, transnational organised crime, terrorist crimes, mercenary crimes, piracy, corruption, crimes relating to the proliferation of WMD and environmental crimes.

This study is focused on crimes which relate to or may impact on the security of states, and therefore include all the abovementioned crimes, with the exception of environmental crimes.

2.1. War crimes, genocide and crimes against humanity

This category of crimes is clearly defined in international law, with the adoption of the *Rome Statute of the International Criminal Court* on 17 July 1998 (UN, 1999-2003). The *Statute* establishes the ICC, permanently seated in The Hague, but which may sit elsewhere, where provided for in national legislation. The States Parties to the *Rome Statute of the International Criminal Court* are also obliged to criminalise in their national laws the crimes in the *Rome Statute of the International Criminal Court* and to establish jurisdiction in their own courts in respect of the crimes provided for. States Parties must also adopt measures in their national law to ensure cooperation with the ICC in respect of investigation and prosecution, the tracing, handing over and transit of suspects who have allegedly committed crimes under the *Rome Statute*.

In terms of the *Rome Statute* the jurisdiction of the ICC shall be limited to "the most serious crimes of concern to the international community as a whole" namely the crime of genocide, crimes against humanity, war crimes, and the crime of aggression (UN, 1999 -2003: Article 5).

In respect of the crime of aggression, there is not yet an agreed upon definition and the *Rome Statute* provides that the ICC shall exercise jurisdiction over the crime once a provision is adopted defining the crime (UN, 1999-2003: Article 5(2)). A definition of such crime has stirred considerable debate under the States Parties to the *Rome Statute*. The development of such definition is work in progress by a special working group established by the Assembly of the States Parties in 2002. The main issues focused on by the special working group are under which circumstances the ICC may exercise jurisdiction over such crime

and whether there should be a requirement that an outside body such as the UN Security Council must make a determination of a state act of aggression before the ICC may exercise jurisdiction over the crime. The special working group focused on three elements of the crime, namely the leadership requirement, the individual's conduct, and the state act of aggression (Coalition for the International Criminal Court, 2007:1). In view of the fact that the international law is still in the process of developing aggression as an international crime, no specific attention will be given to aggression as an international crime in this study, although intelligence on aggression by states is of importance to civilian and military intelligence.

Crimes such as terrorism and drug trafficking are not included in the jurisdiction of the ICC. It is foreseen that such a step might in future follow if the States Parties to the *Rome Statute* could reach an agreement on that (UN, 2002).

The *Rome Statute* defines genocide as any of the following acts committed with intent to destroy, in whole or in part, a national, ethnical, racial or religious group, as such: (UN, 1999-2003: Article 6)

(a) Killing members of the group;
(b) Causing serious bodily or mental harm to members of the group;
(c) Deliberately inflicting on the group conditions of life calculated to bring about its physical destruction in whole or in part;
(d) Imposing measures intended to prevent births within the group;
(e) Forcibly transferring children of the group to another group.

The *Rome Statute* defines crimes against humanity as any of the following acts when committed as part of a widespread or systematic attack directed against any civilian population, with knowledge of the attack: (UN, 1999-2003: Article 7)

(a) Murder;
(b) Extermination;
(c) Enslavement;
(d) Deportation or forcible transfer of population;
(e) Imprisonment or other severe deprivation of physical liberty in violation of fundamental rules of international law;
(f) Torture;
(g) Rape, sexual slavery, enforced prostitution, forced pregnancy, enforced sterilization, or any other form of sexual violence of comparable gravity;
(h) Persecution against any identifiable group or collectivity on political, racial, national, ethnic, cultural, religious, gender as defined in paragraph 3, or other grounds that are universally recognized as impermissible under international law, in connection with any act referred to in this paragraph or any crime within the jurisdiction of the Court;
(i) Enforced disappearance of persons;
(j) The crime of apartheid;
(k) Other inhumane acts of a similar character intentionally causing great suffering, or serious injury to body or to mental or physical health.

Various terms used in the definition, namely 'attacks directed against any civilian population', 'extermination', 'enslavement', 'deportation', 'torture', 'forced pregnancy', 'persecution', 'the crime of apartheid' and 'forced disappearance of persons' are defined in the *Rome Statute* (UN, 1999-2003: Article 7(2)).

The Rome Statute defines 'war crimes' particularly when committed as a plan or policy or part of a large-scale commission of such crimes, elaborately with reference to: (UN, 1999-2003: Article 8)

(a) Grave breaches of the Geneva Conventions of 12 August 1949;

(b) Other serious violations of the laws and customs applicable in international armed conflict within the established framework of international law;

(c) In the case of an armed conflict not of an international character, serious violations of Article 3 common to the four Geneva Conventions of 12 August 1949, namely;

(d) Paragraph 2 (c) applies to armed conflicts not of an international character and thus does not apply to situations of internal disturbances and tensions, such as riots, isolated and sporadic acts of violence or other acts of a similar nature;

(e) Other serious violations of the laws and customs applicable in armed conflicts not of an international character, within the established framework of international law, namely, any of the following acts….

(f) Paragraph 2 (e) applies to armed conflicts not of an international character and thus does not apply to situations of internal disturbances and tensions, such as riots, isolated and sporadic acts of violence or other acts of a similar nature. It applies to armed conflicts that take place in the territory of a State when there is protracted armed conflict between governmental authorities and organized armed groups or between such groups.

The definition of war crimes is much more elaborate, and the above is an extract, as it is not deemed necessary to include the full definition in the text (UN, 1999-2003: Article 8).

Although there are already 105 States Parties to the *Rome Statute*, some very important countries are not States Parties, such the Peoples' Republic of China, the US, and the Russian Federation.

The next international crime of particular relevance for the security of any state and which is described hereunder, is international terrorism.

2.2. International terrorism

International terrorism is often claimed to be one of the most serious challenges facing the international community (Orlova & Moore, 2005: 1).

There is not yet a comprehensive international instrument dealing with terrorism. At present there are 30 instruments, 16 universal (13 instruments and 3 recent amendments) and 14 regional, pertaining to the subject of international terrorism. The topics of the 13 instruments referred to, include offences in relation to aircraft, civil aviation, airports, crimes against protected persons, including diplomatic personnel, hostage taking, crimes in respect of the protection of nuclear material and acts of nuclear terrorism, crimes against the safety of maritime navigation, crimes committed on fixed platforms, and crimes involving plastic explosives, terrorist bombings, and terrorist financing. These instruments can be viewed as *ad hoc* interventions by the international community against various forms of terrorism used by the perpetrators through the years and in response to particular instances or series of events of terrorism, such as hijacking of aircraft or ships, hostage taking or bombings (UN, 2006: 19).

The 13 universal instruments on terrorism are as follows: (UN, 2007(a))

- 1963 *Convention on Offences and Certain other Acts Committed on Board Aircraft*;
- 1970 *Convention for the Suppression of Unlawful Seizure of Aircraft*;
- 1971 *Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation*;
- 1973 *Convention on the Prevention and Punishment of Crimes Against Internationally Protected Persons*;
- 1979 *International Convention against the Taking of Hostages*;
- 1980 *Convention on the Physical Protection of Nuclear Material*;
- 1988 *Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation, supplementary to the Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation (Extends and supplements the Montreal Convention on Air Safety (Airport Protocol)*;
- 1988 *Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation (Maritime Convention) and the Protocol thereto-Protocol to the Convention for the Suppression of Unlawful Actions against the Safety of Maritime Navigation*;
- 1988 *Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms Located on the Continental Shelf and 2005 Protocol thereto*;
- 1991 *Convention on the Marking of Plastic Explosives for the Purpose of Detection (Plastic Explosives Convention)*;
- 1997 *International Convention for the Suppression of Terrorist Bombings (Terrorist Bombing Convention)*;
- 1999 *International Convention for the Suppression of the Financing of Terrorism (Terrorism Financing Convention)*;
- 2005 *International Convention for the Suppression of Acts of Nuclear Terrorism (Nuclear Terrorism Convention)*.

The General Assembly of the UN established an *Ad Hoc* Committee tasked to draft a *Comprehensive Convention on International Terrorism*. The *Ad Hoc* Committee progressed to the point where a consolidated draft comprehensive convention had been produced (UN, 2005(a): 7). The draft *Comprehensive Convention on International Terrorism* could not yet be finalised, due to a number of political issues that are highly contentious, and on which consensus could not yet be reached. The first issue is that of motive, and whether it should be an element of a definition of terrorism. Motive relates to the inducement, cause or reason why a thing is done (Orlova & Moore. 2005: 276). This further relates in particular to the question whether peoples' struggles against foreign occupation, aggression, colonialism and hegemony aimed at liberation and self-determination in accordance with the principles of international law shall be excluded in the convention as terrorist crimes. This proposed exclusion is based on the recognition of the legitimacy of such struggles by various UN General Assembly resolutions (Orlova & Moore, 2005: 277). Various recent UN resolutions, however, reaffirmed that no terrorist act can be justified in any circumstances (UN, 2008(b): 2).

The proponents of the exclusion of such struggles from the scope of the draft *Comprehensive Convention on International Terrorism* argued that the requirement that the struggle must be "in accordance with the principles of international law", provided a safeguard against abuse (Orlova & Moore, 2005: 277). One of the counter-arguments is that the International Humanitarian Law (IHL) applies to all combatants and that blurring the distinction between combatants and civilians is unacceptable (Orlova & Moore, 2005: 278).

Understandably this debate is a lively one also in respect of legislation on national level. The definition of 'terrorist act' in the Canadian legislation (Clause 83.01(1)(b)(i)(A)) had as required element a political, religious or ideological motive. The Superior Court of Justice found that there is no compelling benefit or justification for such motive requirement. Jurisdictions such as Australia, New

Zealand and South Africa have similar 'motive' requirements in their counter-terrorism statutes (Canada. 2006: paragraphs 69, 80).

The second issue in dispute is that of 'state terrorism', which effectively stalled the negotiations on the draft *Comprehensive Convention on International Terrorism*. The dispute is basically between the Western nations and the Organisation of the Islamic Conference (OIC). The Western nations argued that there is no need to include crimes committed by a state's military forces as they fall under other corpora of international law such as the IHL or human rights law. The OIC's proposal is to provide a back-up to cover such crimes. At the moment the result of the abovementioned disputes is that the negotiations have stalled (Orlova & Moore. 2005: 280, 281). There are new proposals on the table in a bid to resolve this impasse, but it is not clear whether consensus in this regard might be reached soon (UN, 2007(b): 7, 8).

The following 'offence' is provided for in the draft *Comprehensive Convention on International Terrorism*: (UN, 2005(a): 9, Article 2)

> Any person commits an offence within the meaning of the present Convention if that person, by any means, unlawfully and intentionally causes:
>
> (a) Death or serious bodily injury to any person; or
>
> (b) Serious damage to public or private property, including a place of public use, a State or government facility, a public transportation system, an infrastructure facility, or to the environment; or
>
> (c) Damage to property, places, facilities or systems referred to in paragraph 1(b) of the present article resulting in or likely to result in major economic loss.

This definition of the offence in international law is, however, not legally binding, in view of the fact that the Convention had not been concluded or adopted yet. It

is regarded as an 'operational' definition, but criticised as being too wide in scope (Orlova & Moore, 2005: 272). A person who, for example, merely expresses sympathy for the aims of a terrorist group, could commit an offence under the proposed definition (Orlova & Moore, 2005: 273).

The offences which states are required to enact in national legislation in terms of the obligations in the 13 international instruments adopted by the international community in response to particular manifestations of terrorism, are therefore the most definitive crimes which are 'universally' accepted. Not all states are yet States Parties to these instruments, but a huge majority of states are States Parties thereto.

A general definition describing the offence of terrorism which is favored is the definition of 'terrorist activity' in the Canadian Criminal Code, save for the clause relating to motive being deleted. This definition provides that terrorist activity includes an act or omission that is committed in whole or in part with the intention of intimidating the public, or a segment of the public, with regard to its security, including its economic security, or compelling a person, government or a domestic or an international organisation to do or refrain from doing any act, whether the public or the person, government or organisation is in or outside (Canada or for that matter any country in respect of which the definition is applied) (section 83.01(1)(ii)) and:

> that intentionally-
>
> (A) Causes death or serious bodily harm to a person by the use of violence,
>
> (B) Endangers a person's life;
>
> (C) Causes a serious risk to the health, or safety of the public or any segment of the public;
>
> (D) Causes substantial property damage, whether to public or private property, if causing such damage is likely to result in the conduct or harm referred to in

any of the clauses (A) to (C); or

(E) Causes serious interference with or serious disruption of an essential service, facility or system, whether public or private, other than as a result of advocacy, protest, dissent or stoppage of work that is not intended to result in the harm referred to in clauses (A) to (C).

A conspiracy, attempt or threat to commit an act or omission described above is also criminalised. Acts or omissions committed during an armed struggle in accordance with customary international law or conventional international law, or the exercise of official duties by military forces of a state are, however, excluded (Canada, 2006(b): 6, 7).

Transnational organised crime, like terrorism, enjoys attention at the highest international level as an international crime which needs to be addressed by means of international cooperation.

2.3. Transnational organised crime

In order to analyse the concept of transnational organised crime, the phenomenon organised crime needs to be described. There is no universally accepted definition of organised crime. (Symeonido-Kastanidou, 2007: 83).

Even the *UN Convention against Transnational Organized Crime* (UN: 2004(a)) does not contain a definition of organised crime as such. The *UN Convention against Transnational Organized Crime* defines 'organized criminal group' as a structured group of three or more persons, existing over a period of time and acting in concert with the aim of committing one or more serious crimes or offences established in accordance with the *UN Convention against Transnational Organized Crime* in order to obtain directly or indirectly, a financial

or other material benefit. 'Structured group' is defined as a group that is not randomly formed for the immediate commission of an offence and that does not need to have formally defined roles for its members, continuity of its membership or a developed structure. It defines a serious offence as an offence punishable by a maximum deprivation of liberty of at least four years. Within the context of the *UN Convention against Transnational Organized Crime* organised crime boils down to the commission of a serious offence involving an organised criminal group.

There are literally dozens of definitions on organised crime. The following definition of organised crime, which is also in consonance with the *UN Convention against Transnational Organized Crime*, is supported:

> Organised crime is the planned commission of criminal offences determined by the pursuit of profit and power which, individually or as a whole, are of considerable importance and involve more than two persons, each with his/her own assigned tasks, who collaborate for a prolonged or indefinite period of time-
>
> (a) by using commercial or business-like structures,
> (b) by using force or other means of intimidation; or
> (c) by exerting influence on politics, the media, public administration, judicial authorities or the business sector.

This definition originates from the German Bűndeskriminalampt (BKA) (Von Lampe, 2005).

The *UN Convention against Transnational Organized Crime* is clear on what 'transnational' means. It states that an offence is transnational in nature if it is committed in more than one state; if it is committed in one state, but a substantial part of its preparation, planning, direction, or control takes place in another state; if it is committed in one state, but involves an organised criminal group that

engages in criminal activities in more than one state; or if it is committed in one state, but has substantial effects in another state (UN, 2004(a): Article 3(2)).

The following characteristics of transnational organised crime are relevant to motivate its inclusion in this study, namely transnational criminal organisations operate as enterprises that merge corporate and criminal cultures and have developed into sophisticated transnational business generating huge profits. Their resources rival those of multinational corporations and their disregard for holidays, working hours, borders and legal systems gives them an edge over national law enforcement efforts. Such organisations threaten national security and economic growth, jeopardise the political and economic stability of states, threaten domestic and global economics, and alter the fabric of society (Gerspacher, 2002: 1, 2).

Transnational organised crime, as defined above, encompasses a wide variety of cross-border crimes, such as human trafficking, money-laundering, trafficking in drugs, firearms, explosives, illegal conventional arms trade, trafficking in migrants, illegal trade in protected species of fauna and flora. In respect of each of these categories, there are legal obligations in international instruments in respect of cooperation among states, and enactment of appropriate crimes in their national legislation

Another category of international crimes of direct concern from a security point of view is ‘mercenary crimes’, which includes acts such as *coup d’etats.*

2.4. Mercenary crimes

There is only one global instrument dedicated to addressing mercenary and mercenary-related activities, and one regional convention within the African region, placing obligations on States Parties to act against mercenary activities.

2.4.1. *International Convention against the Recruitment, Use, Financing, and Training of Mercenaries*

This global Convention was adopted on 4 December 1989, but has been ratified or acceded to by only 30 countries. It provides that States Parties shall take steps to legislate against mercenary activities, including recruitment and financing of mercenary activities; cooperation to combat mercenary activities; arrest of suspected mercenaries; and extradition where applicable. The Convention has numerous gaps and ambiguities and is silent on the issue of private military companies. Despite the fact that the UN is continuing to foster the ratification of, or accession to the Convention, the UN is seeking support for a process towards an additional protocol to the Convention to address newer forms of mercenarism such as the activities of private military and security companies (UN, 2008(e): 5).

The *International Convention against the Recruitment, Use, Financing, and Training of Mercenaries* defines a 'mercenary' as any person who is specially recruited locally or abroad in order to fight in an armed conflict, is motivated to take part in the hostilities by the desire for private gain and, is promised, by or on behalf of a party to the conflict, material compensation substantially in excess of that promised or paid to combatants of similar rank and functions in the armed forces of that party (International Committee of the Red Cross, 1989: Article 1).

In situations other than in an armed conflict, a mercenary is defined as any person motivated by the desire for significant private gain and prompted by the promise or payment of material compensation; who is recruited locally or abroad, for the purpose of participating in a concerted act of violence aimed at overthrowing a government or otherwise undermining the constitutional order of a state; or undermining the territorial integrity of a state (International Committee of the Red Cross, 1989: Article 1).

In respect of both scenario's it is further required, to fall within the ambit of the definition of a mercenary, that a person is neither a national nor a resident of the state against which such an act is directed; has not been sent by a state on official duty; and is not a member of the armed forces of the state on whose territory the act is undertaken (International Committee of the Red Cross, 1989: Article 1).

It is clear that the above Convention, through the requirements that a person sent 'on official duty' or, being a member of the armed forces, are effectively excluded from being a 'mercenary' creates a loophole for governments to employ mercenaries through private military and private security companies, who are contracted by the armed forces, and performs duty alongside members of the armed forces. An example in case is the rise of the private military and security companies acting in support of or sometimes as an integral part of government forces. This development is described as the privatisation or corporatisation of war, with the deployment of thousands of private military or private security personnel in Iraq in situations where they actively participated in hostilities, under immunities granted to them (Scahil, 2007: Chapter 19).

2.4.2 Organization of African Unity (OAU) Convention for the Elimination of Mercenarism in Africa

This Convention was adopted at Libreville on 3 July 1977 (AU, 1977). It came into force on 22 April 1985, following a slow rate of ratification of, or accession to, the Convention. To date only 24 Member States of the African Union have ratified the Convention. The contents of the Convention is very similar to that of the *International Convention against the Recruitment, Use, Financing and Training of Mercenaries.* Without detailing the contents of the OAU Convention, it should be mentioned that, following the Equatorial Guinea *coup* attempt, the African Union's Peace and Security Council mandated and requested: "the necessary steps to find a global solution to the phenomenon of mercenary activities on the Continent

through the harmonization of existing legislation and measures within the context of a review of the *OAU Convention on the Elimination of Mercenarism in Africa"* (AU, 2004(b)).

Both the *International Convention against the Recruitment, Use, Financing and Training of Mercenaries and the OAU Convention on the Elimination of Mercenarism in Africa* have therefore been identified for review and improvement in order to address emerging developments such as the "privatisation of war" and the widespread use by countries of private military and private security companies in conflicts, acting as combatants for private gain and are actually extensions or proxy forces of the armed forces of those countries. Some movement has already taken place in this regard, with the adoption by 17 states on 17 September 2008 of the *Montreux Document on Pertinent International Humanitarian Legal Obligations and Good Practices for States related to Operations of Private Military and Security Companies during Armed Conflict* (UN, 2008(d)).

An international crime that has been the first such crime to be recognised as requiring international cooperation to combat, is piracy, which has emerged in a modern form as important to address as ever.

2.5. Piracy

This is one of the few international crimes of which a generally accepted definition exists. The *United Nations Convention on the Law of the Sea* (UNCLOS), provides in Article 101, that piracy consists of any of the following acts: (UN, 1982: Article 101):

(a) any illegal acts of violence or detention, or any act of depredation, committed for private ends by the crew or the passengers of a private ship or a private aircraft, and directed:
    (i) on the high seas, against another ship or aircraft, or

against persons or property on board such ship or aircraft;

(ii) against a ship, aircraft, persons or property in a place outside the jurisdiction of any State;

(b) any act of voluntary participation in the operation of a ship or of an aircraft with knowledge of facts making it a pirate ship or aircraft;

(c) any act of inciting or of intentionally facilitating an act described in subparagraph (a) or (b).

Although this is one of the oldest international crimes, it is as relevant as ever, as there is a convergence of piracy and terrorism. There is also an overlap between the crime of piracy and the acts provided for in Article 3 of the *Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation*, which is regarded as one of the international counter-terrorism instruments. Piracy, can, in terms of UNCLOS only be committed on the high seas, whereas the *Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation* is not restricted to the high seas.

Linked with high-technology, and one of the latest threats relating to terrorism, is the issue of WMD. This issue received the attention of commissions of inquiry, both in the UK and US investigating intelligence failures related to a perceived threat of WMD posed by Iraq (UK., 2004) (US, 2005(c) (US, 2008(c)).

2.6. Crimes relating to weapons of mass destruction

Nuclear, biological and chemical weapons are regarded as WMD: “Designed to terrify as well as destroy, they have the potential to kill thousands and thousands of people in a single attack, and their effects may persist in the environment and in our bodies, in some cases indefinitely” (Sweden, 2006: 22).

A number of international instruments deal with WMD, by placing obligations on states to prevent the proliferation of WMD, including the development, production and stockpiling thereof. The main instruments in this regard are the following: (Sweden, 2006: 34)

— *Treaty on the Non-Proliferation of Nuclear Weapons (NPT)* - in force since 1970, joined by 189 Parties (UN, 2000). The NPT represents the only binding commitment in a multilateral treaty to the goal of disarmament by the nuclear-weapon states. There is, however, no universal comprehensive prohibition on the use of nuclear weapons in either customary or international humanitarian law. The principal judicial organ of the UN, namely the International Court of Justice (ICJ), on 8 July 1996, gave an advisory opinion about the 'Legality of the threat of the use of nuclear weapons'. The 14 judges of the ICJ concluded unanimously that the principles and rules of international humanitarian law applied to the use of nuclear weapons. They added that the use of nuclear weapons would generally be contrary to the principles of international humanitarian law (ICRC, 2003), (ICJ, 2006: 266, 267).

  The opinion, however, stated an exception that in an extreme circumstance of self-defence in which the state's very survival may be at stake, the use of nuclear weapons may be permissible. This exception must still be viewed against the general principles of the IHL relating to proportionality; necessity; the existence of an armed attack; the lack of any steps by the UN Security Council; use of weapons indiscriminately of civilian and military targets; causing wide-spread and permanent damage to the environment; unnecessary and aggravating suffering of combatants; and affecting other states not involved in the conflict.

— *Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on their Destruction (BTWC)* - in force since 1975, with 155 States Parties which have ratified or acceded to the Convention. It bans the development,

production, stockpiling, acquiring, retention and use of microbial or other biological agents or toxins. It also bans weapons or equipment or means of delivery designed to use such agents or toxins for hostile purposes or in armed conflict. The Convention requires States Parties to take measures to give effect to the Convention (OPBW, 2005: Article (IV)).

— *Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on Their Destruction (CWC)* - in force since 1997, with 177 States Parties. The CWC bans the development, production, stockpiling, transfer and use of chemical weapons (OPCW, 2005).

According to customary international humanitarian law that is binding on all states and on all parties to an armed conflict, the use of biological and chemical weapons is prohibited (ICRC, 2003). Furthermore, employing poison or poisoned weapons or poisonous or other gasses or all analogous liquids, materials and devices are regarded as 'war crimes' (UN, 1999-2003: Article 8(2)(b)(vii) and (viii)).

The combating of the proliferation of WMD is closely linked to the missile delivery systems that could be used to deliver WMD. Without venturing into the definition of WMD, the Committee for the Review of Weapons of Mass Destruction regarded missiles with a range greater than 150 kilometers and related major parts, and repair and production facilities as WMD (UK, 2004: 4). The Committee of Privy Counsellors chaired by Lord Butler were appointed by the UK prime minister to review the accuracy of intelligence on Iraqi WMD up to March 2003 and in particular discrepancies between intelligence available before the Iraqi war and the findings survey made after the war (UK, 2004).

The above instruments were, however, drafted with the primary objective of preventing the proliferation of WMD among states, and save for possibly the CWC, they are not suitable to deal with non-state actors. After the 11 September

2001 events, as well as the revelation in 2003 of the existence of a private network of suppliers of sensitive nuclear technologies, led by the Pakistani scientist Abdul Qadeer Khan, it was realised that the focus should be widened to include non-state actors as recipients, as well as suppliers of sensitive goods and technologies (Frantz & Collins, 2007: xiii, xiv). The UN Security Council opted to utilise Chapter VII of the UN Charter and adopted Resolution 1540 of 2004. Such a resolution is binding upon all Member States of the UN. The adoption of the Resolution is viewed as a controversial step in respect of a general threat as opposed to a specific threat in a specific situation (Ahlström, 2007: 460, 461). Operative paragraph 1 of the Resolution provides that Member States shall not provide support to non-state actors to develop, acquire, manufacture, possess, transport, transfer, or use nuclear, bacteriological or chemical (NBC) weapons and their means of delivery. In terms of operative paragraph 2 of the Resolution, Member States of the UN, are obliged to adopt and enforce effective domestic law that would prohibit the activities mentioned above.

In terms of operative paragraph 3 of the Resolution, Member States are also required to establish and maintain effective accounting systems, physical protection measures, border controls, law enforcement measures, and national export controls that would also cover transshipment. These elaborate measures could seem unrealistic and affects the implementation of the Resolution, as is clear from the poor response from Member States on reporting progress with the implementation thereof (Ahlström, 2007: 466-469). Only one third of UN Member States have never reported on the implementation of the Resolution (Ahlström, 2007: 437). In practice, the most common international crime where intelligence cooperation would be required relating to WMD would be in respect of contravention of the control measures which Member States need to adopt in respect of WMD.

Most UN Member States have export control legislation in place and have adopted national lists of controlled items (including technologies), such lists are

not uniform and some Member States control goods and technologies not listed in any control list (catch-all controls) (Ahlström, 2007: 471). Only a limited number of Member States control transport, transfer of technologies, end-user, transfer, transshipment or re-export of dual-use items.

It is clear from the above that, in respect of numerous international crimes, there is a lack of universally accepted definitions, despite the existence of numerous international instruments. War crimes, genocide and crimes against humanity are well defined, in international law, with reference to the *Rome Statute of the International Criminal Court***.** A number of the most important countries are, however, not party to the *Rome Statute*. In respect of terrorism, the drafting of a *Draft Comprehensive Convention on Terrorism* has virtually stalled. Specific forms of terrorism, such as bombings, hijacking of aircraft and ships or interference with the safe navigation thereof, hostage-taking, attacks on diplomatic personnel, and even acts of nuclear terrorism are quite well defined in what can be referred to as the main counter-terrorism instruments. Defining terrorism as such is, however, a political dilemma, which affects the adoption of national legislation in order to enforce the relevant international instruments.

Transnational organised crime is not defined, in international law, but by using existing definitions of ‘organized criminal group’ and ‘transnational’ in the *United Nations Convention against Transnational Organized Crime***,** it is possible to draft effective national legislation to combat transnational organised crime. Especially in respect of mercenary offences, international law needs to be reviewed and updated to effectively address the extensive use of private military and private security companies in armed conflicts in a combat role, often participating as combatants during armed hostilities. The crime of piracy, as one of the oldest international crimes is well defined in international law. Crimes related to WMD are required in terms of UN Security Council Resolution 1540 to be adopted by UN Member States in their national legislation, but the implementation thereof is

difficult and controversial in view of the manner in which the powers of the UN Security Council are used to 'legislate' in international law.

It is also necessary to describe what is understood within the context of this study under the term 'combating of international crime', as 'intelligence and intelligence cooperation'- is the focus of this study and also key elements to the successful combating of international crime.

3. COMBATING OF INTERNATIONAL CRIME

The following responses are possible in combating international crimes:

— **Law enforcement response.** Effective law enforcement requires an appropriate legal response to international obligations in providing for the required crimes, legal powers such as criminal and civil asset forfeiture, special investigative tools or techniques, as well as the freezing of assets, deportation, extradition and international assistance in criminal matters. The usual response to crime in law enforcement context is a reactive response, namely the investigation of crimes already committed and the prosecution, arrest, trial and punishment of the offenders. The preferable option, however, would be to prevent those crimes from being committed in the first place, something which is possible by means of timeous intelligence in combination with appropriate preventive action (Wilkinson, 2006: 77-79). The bulk of the responsibility for combating international crime rests with police services, but law enforcement includes the totality of law enforcement, including local police agencies, justice, immigration, customs and revenue services. Intelligence support and cooperation is important in respect of both the investigation and prevention of crime. In most countries formal processes in respect of mutual legal assistance are required to use measures such as surveillance, including electronic surveillance of communications, or other special investigative techniques, such as undercover operations in the investigation of crime, whether already committed or in the

incipient phase. Many special investigative tools/techniques, such as controlled deliveries, whether performed nationally or across international borders require continuous physical and electronic surveillance in order to be successful.

— Military response. The international crimes relating to the security of countries, as described in this chapter are all of such a nature, that a military option might be the only possible response in the circumstances (US, 2001: 16). The terms 'global war on terror' and 'war on drugs', are often used, in describing responses to terrorism and drug trafficking. Especially in respect of war crimes and crimes such as genocide and crimes against humanity, military intervention in the form of peacekeeping and peace enforcement operations mandated by the UN Security Council are required (US, 2001: 3). Military responses to international crimes may range from an all-out military response, such as Russia's aerial bombing on Grozny to crush the separatist Chechen movement at a huge cost to civilian life or the use of the military in supporting civil power, such as in Northern Ireland (Wilkinson, 2006: 70-72). The US military response to the Taliban terrorist threat in Afghanistan is another example of a military response to crime (US, 2001: 30). Military assistance, is often indispensable, such as for interdicting aircraft or ships involved in piracy or arms or drug trafficking. However, the use of military force or covert actions to interdict drug production and shipments within the territorial borders of other countries cannot be advocated as it can have significant drawbacks and damaging effects on other important interests (US, 2001: 9).

— Intelligence response. High quality intelligence is required to prevent crimes such as terrorism and to bring criminals to justice. Although police services themselves normally have intelligence capabilities, they share the tasks of gathering, collating and analysing intelligence with domestic and foreign intelligence services and technical agencies responsible for SIGINT and other sources (Wilkinson, 2006: 73). What is referred to as 'covert action' in US literature and in NATO countries, is called 'dry affairs', 'wet affairs', 'dirty tricks' 'black operations' or 'covert operations' in some countries- including even assassination (Jansen van Rensburg, 2005: 22). Covert action may further

range from propaganda to political interventions in the political process of the target nation, the use of economic measures against a state, the instigation of a *coup* in another country, support of paramilitary actions, secret participation in combat, and especially within the context of terrorism, the much criticised use of extralegal rendition (Lowenthal, 2006: 162-165). Covert action by nature is highly controversial and different opinions exist as to whether it indeed could be regarded as part of intelligence (Shulsky & Schmitt, 2002: 96). The use of covert action to combat crime remains a controversial issue.

— **Combined response.** In some instances combined responses of law enforcement, intelligence and military have been used, not only to combat drug trafficking, but also war crimes and terrorism. In respect of terrorism 'rendition' (in effect abduction of suspects against the laws of a country, and against international law) has been performed by law enforcement and intelligence agencies in various countries ((Wilkinson, 2006: 164). The Mossad, Israel's Secret Intelligence Service, abducted a Second World War Nazi war criminal, Adolf Eichmann from Argentina to stand trial in Israel (Eisenberg, Dan & Landau, 1978: 25-40). In the 'war on drugs' the head of state of Panama, General Manuel Noriega was captured by the US military and Drug Enforcement Agency (DEA) in Panama to stand trial in Miami. This happened during an invasion of Panama and Noriega evading the US forces in his country for 22 days. He was convicted of drug trafficking, money-laundering and racketeering and sentenced to 40 years imprisonment (US, 2001: 25, 26). Such responses are only possible in countries where the courts allow jurisdiction to be established in this manner, such as the US (the Ker-Frisbie-doctrine) (US, 2001: 27).

The intelligence response is one of the most important responses to international crime, and consequently the following definition of key importance for this study, is 'intelligence', which term is analysed hereunder.

4. INTELLIGENCE: A CONCEPTUAL FRAMEWORK

The term 'intelligence' will firstly be analysed and described within different contexts, and then the expressions 'combating of international crime' and 'intelligence cooperation' will be analysed.

4.1. Meaning

'Intelligence' in the broadest sense is described as a 'process', as 'a product' and as 'organisation' (Johnson & Wirtz, 2004: 1). 'Intelligence' could also refer to certain kinds of information or activities (Shulsky & Schmitt, 2002: xi, 2).

The different meanings depend on the context within which it is used. One of the uses of 'intelligence' is to refer to the IC, namely the national agencies responsible for security, or to units within the IC, which perform intelligence functions (Cleary, 2006: 7). "'Intelligence' in government is based on the particular set of organizations with that name: The 'intelligence services' or (sometimes) 'intelligence communities'. Intelligence activity is what they do, and intelligence knowledge what they produce." (Herman, 1999: 2). In the quest for an appropriate definition of intelligence, it is clear that the dimension in which the term is used, influences the description thereof. For example, intelligence has been defined within the CIA, (a US civilian foreign intelligence agency) as follows: "Intelligence is secret, state activity to understand or influence foreign entities." (Warner, 2003: 7).

4.2. Dimensions of intelligence

There are three different dimensions of intelligence, namely foreign, military and domestic intelligence (US, 2006(b): 5).

Foreign intelligence means that which is collected covertly and overseas, and is provided to policymakers to inform national security decisions and actions (US, 2006(b): 4).

Military intelligence means that which is collected, analysed, disseminated, and possibly acted upon by defence entities (including the intelligence elements) and the combat support agencies and is related to another foreign power's capabilities to attack a state's national interests militarily (US, 2006(b): 5).

Domestic intelligence relates to threats against a government's ability to govern, or against its existence, and which emanates from individuals or groups within the borders of the country. The aims of such groups or individuals could be to overthrow the government by illegal means, the use of violence to change government policies, in other words, for political purposes, or the exclusion from participation in politics or government members of a particular ethnic, racial, or religious group. The perception of such threat may vary from country to country depending on the system of government and level of democracy in the country involved. Domestic intelligence may include foreign links or elements, such as individuals or groups acting as, on behalf of, or at the direction of a hostile foreign power or share and pursue common objectives of a hostile foreign power, with or without any ties to such hostile foreign power (Shulsky & Schmitt, 2002: 4). The definition of 'domestic intelligence' in the South African *National Strategic Intelligence Act 39 of 1994*, for example, includes "intelligence on any internal activity, factor or development which is detrimental to the national stability of the Republic, as well as threats or potential threats to the constitutional order of the Republic and the safety and well-being of its people."

The term civilian intelligence refers to that part of the IC focused on providing accurate, verifiable intelligence to civilian leaders so they can make appropriate political decisions (Bradberry, 2006: 1). Foreign and domestic civilian intelligence

exist to uncover threats, and estimate and warn about the likelihood of their materialising and analising their effect (Cave, 2002: 10).

A further distinction can be made between positive and crime intelligence.
'Positive intelligence' is used as a term inclusive of all intelligence, except counter-intelligence and 'security (crime) intelligence'. In this study 'positive intelligence' will be used to describe all intelligence exclusive of counter-intelligence and law enforcement intelligence. The product derived from positive intelligence "may be considered as domestic or foreign, in terms of purpose, scope or substance" (Cave, 2002: 13).

'Security intelligence' refers to specialised operational intelligence concerning criminal and illegal activities on both national and international scale such as smuggling, counterfeiting and murder (Kent, 1966, 3, 210). It is further described as the intelligence behind the police function and the knowledge and the activity which defensive police forces must have in order to take specific action against individual criminals (Kent, 1966: 209 -210; US, 2006(b): 7). From a law enforcement perspective, intelligence is defined as information that has been subjected to a defined evaluation and risk assessment process in order to assist with police decision-making (ACPO, 2005: 13).

Some information is defined within a law enforcement context as pieces of raw, unanalysed data that identifies persons, evidence, events, or illustrates processes that indicate the incidence of a criminal event or witnesses or evidence of a criminal event: Information is collected as the currency that produces intelligence. Consequently 'law enforcement intelligence' is defined as the product of an analytic process that provides an integrated perspective to disparate information about crime, crime trends, crime and security threats and conditions associated with criminality (Carter, 2004: 9). Sometimes 'law enforcement intelligence' is referred to as 'criminal intelligence' or 'crime intelligence' (US, 2003(a)).

This definition of 'security intelligence' coincides with the definition of 'law enforcement', 'criminal intelligence' or 'crime intelligence', referred to hereunder. 'Criminal intelligence' is gathered overtly or clandestinely and domestically as evidence to support a prosecution of a criminal act or to learn more of a criminal enterprise (US, 2006(b): 4). There is, however, much communality in the respective definitions, whether it is used in the traditional intelligence environment or within the law enforcement environment. Of particular importance is the place and meaning of information in relation to intelligence. Information should not be equated to intelligence (Warner, 2003: 3). The intelligence activity in respect of police functions is often described as 'crime intelligence' (Cave, 2002: 15). The traditional police functions are the prevention of crime, crime detection and investigation (including collection of information and evidence to ensure a successful prosecution in a court of law), and policing actions in respect of public safety and public order. In this study the term 'law enforcement intelligence', 'criminal intelligence' and 'crime intelligence' are used interchangeably as different terminology is used in the respective countries for the same concept.

Information which could be collected for 'crime' intelligence analysis is informant information, surveillance, travel records, CCVTV videotapes, banking transactions, undercover information, pen-register/trap and trace) (communications-related information), documentary evidence, forensic evidence, communications intercepts (wiretaps) (Carter, 2004: 10). Just as information and intelligence should be distinguished from each other, there is also a difference between 'information sharing' and 'intelligence sharing'. Of importance is that intelligence is both 'a process' and 'an end-product', or both 'an activity' and 'a product of that activity' (Warner, 2003: 4). Within the law enforcement environment reference is made to 'source assets', which include victims and witnesses, communities and members of the public, crime-stoppers, prisoners,

forensic information, undercover operatives, surveillance products, and covert human intelligence sources (CHIS) (ACPO, 2005: 32).

4.3. Intelligence as a process

The intelligence cycle refers to the developing of raw information into intelligence products for use in decision-making and formulating policies or actions. The cycle is characterised by the following steps, namely planning and direction; collection of raw data; analysis; dissemination and evaluation. The focus here will primarily be on collection and analysis (US, 2003(a): 3).

4.3.1. Collection

In order to understand the intelligence process, it is necessary to explore the sources of intelligence, also referred to as 'collection disciplines' (Lowenthal, 2006: 89-104). The following are sources of intelligence:

4.3.1.1. Open source intelligence

The most available and easily obtainable source of intelligence is open source intelligence (OSINT). OSINT includes the traditional publicly available sources such as newspapers, books and magazines, as well as the huge expansion of online available sources (Clark, 2004: 66). Online sources, such as commercial databases which are available on subscription, also qualify as OSINT. Online sources are the most commonly used open sources. Most of the online sources are available from the World Wide Web: "The rapid expansion of global information networks provides analysts with large volumes of information that were previously unavailable" (Clark, 2004: 68) - to such an extent that the analyst encounters information overload. Many OSINT sources remain available only in hard copy, obtainable from libraries, commercial database, and from scientists and business people. Valuable sources include telephone books monographs,

journals, patents and technical literature. Classified 'in-house' literature which erroneously lands in libraries or otherwise in the public domain, are regarded as OSINT, but referred to as 'gray literature' (Clark, 2004: 69).

4.3.1.2. Human intelligence

Human intelligence (HUMINT) focuses on people. It includes police informers, recruited sometimes amongst criminals, prison inmates, through police interaction with the community, plea bargains, or sentence reduction, paid informers and neighbourhood watches (Settle, 1995: 28, 38, 68, 149, 153).

It can furthermore consist of liaison relationships between intelligence organisations with other intelligence organisations and law enforcement groups, émigrés and defectors, and clandestine sources such as classical spies, moles or agents. HUMINT is usually the best method in dealing with illicit networks (Clark, 2004: 70-76).

4.3.1.3. Signals intelligence

Signals intelligence (SIGINT) can be broken down into five components, namely communications intelligence (COMINT); electronics intelligence (ELINT); radar intelligence; (RADINT); laser intelligence (LASINT); and non-imaging infrared (Richelson, 1989: 167). COMINT is the interception, processing and reporting of an opponent's communications. Communications includes voice and data communications, facsimile, Internet messages, and any other deliberate transmission of information. COMINT is collected by aircraft, and satellites, overt ground-based sites, a limited number of seaborne collectors, and some covert and clandestine sites. The most common COMINT is surveillance of telephone communications, through 'normal' telephone tap. Some instruments can convey room conversations when the telephone is on its cradle. Telephone conversations can also be intercepted in bulk by COMINT equipment if the

equipment is properly positioned to collect micro-wave point-to-point transmissions from the company's trunk lines. Unencrypted cellular networks can also be intercepted, and remote acoustic monitoring techniques can also be used (Clark, 2004: 76, 79).

4.3.1.4. Technical Intelligence

In respect of 'technical intelligence' or 'specialised technical collection' the most important for law enforcement is biometrics, namely the use of a person's physical characteristics or personal traits for human recognition. Digitised fingerprints and voiceprints, iris and retinal scans, hand geometry and keystroke dynamics are becoming increasingly important both in the investigation of crime and functions such as controlling access to facilities and at border crossing points (Clark, 2004: 93) (Baker, 2007).

4.3.2. Processing/collation and analysis

Evaluating the information's validity and reliability, collation entails the sorting, combining and categorising and arranging data so that relationships can be determined. Analysis connects information in a logical and meaningful manner to produce an intelligence report that contains valid judgments based on analysed information. The process which separates information from intelligence is the process of analysis (Ryan, 2006: 16). A way to distinguish between data, information and intelligence, is the extent to which value has been added to the raw data collected through overt or clandestine means. "Information is collected as 'raw' until its sources have been evaluated, the information is combined or corroborated by other sources, and analytical and due diligence methodologies are applied to ascertain the information's value." (US, 2006(b): 2). There are different methodologies of analysis. Two of these are trends and patterns; and frequency. After the Madrid bombings, of 2004, which took place exactly 911 days after the 9/11 or 11 September 2001 terrorist attacks in the US, it was

suggested that to achieve successful analysis, there must be a determination of the probability of an event based on the risk of latent threat and target vulnerability. This is something which is well-known in analysis, but "experts tend to be quite inept at assigning even roughly correct probabilities to their predictions." (Segell, 2005: 239, 230).

4.4. Intelligence as a product

It has been mentioned above that intelligence is both an activity and a product. The production of intelligence falls into one of five categories, namely: (Ryan, 2006: 17, 18, 19)

— **Warning intelligence**- when the risk of crisis is sufficiently high, policymakers are issued with a warning.

— **Current intelligence or daily reportage**- refers to daily briefings that brings policymakers up to date and make short term predictions.

— **Basic intelligence**- this is the compilation of encyclopedic, in-depth data on various countries or subjects.

— **Estimative or predictive intelligence**- of which National Intelligence Estimates, informal research papers and policy-related judgments in briefings and memoranda are examples.

— **Raw intelligence**- material taken directly from collectors and given to policymakers- it is unevaluated, may be misleading, lacking context and should be marked as non-analysed information upon distribution. The distinction between raw intelligence and intelligence as a product of analysis is most important in respect of cooperation, as the sharing of information (raw data) and sharing intelligence (analysed information) are two distinctly different tasks in the interagency bargaining process (Ryan, 2006: 27).

4.5. Strategic intelligence and tactical intelligence

Strategic intelligence deals with long-range/long term issues. In this case possible scenarios are developed and intelligence takes a long-term, analytical view. For strategic intelligence more sophisticated and analytical techniques are required and are more complicated than those used for tactical intelligence. Strategic intelligence can be further described as a mechanism to predict threats to a nation's stability and security, of military, political environmental or societal nature (Clough, 2004: 602). It may comprise information and response: The collection, analysis and dissemination of information about global conditions, especially potential threats to a nation's security, and based on this information, the use of secret intelligence agencies to help protect the nation against harm abroad (Johnson, 1991: 46). Strategic intelligence may, also relate to domestic conditions and is not confined to 'global' or 'foreign' conditions (Cave, 2002: 11).

Tactical intelligence on the other hand, deals with issues that require immediate action. The intelligence process is fast on the tactical level, as a quick synthesis of data is necessary to support ongoing tactical operations. Additional collection often needs to be done intelligently in a short time. This type of synthesis is called 'fusion' and is aimed at using all available data sources to develop a more complex picture of a complex event, usually with a short deadline. Fusion is common in intelligence support to law enforcement (Clark, 2004: 156, 157).

4.6. The focus of intelligence

Intelligence can focus on the domestic level on political dissent as a security threat; on the foreign level at threats posed by hostile foreign powers, which may be of a military nature or aimed at a nation's fundamental system of government; or it can focus on economic or nontraditional issues such as environmental issues (Shulsky & Schmitt, 2002: 4-6). The 'new priorities' on which intelligence focuses, are terrorism; proliferation of WMD; narcotics; economics; health and

environment; peacekeeping operations; 'information operations', vaguely described as 'the use of computer technology to wage war'; and dominant battlefield awareness (Lowenthal, 2006: 236-252).

Intelligence relating to peacekeeping operations (PKI) is regarded as a new form of intelligence that emphasises open sources of information, multilateral sharing of intelligence at all levels, the use of intelligence to ensure force protection, and interoperability and communality with coalition partners (Carment & Rudner, 2006: 1). The challenges facing PKI are increasingly intertwined with questions of arms control, commercial interests, international crime and ethnic conflict (Aid, 2006: 43).

Central to this study, is the meaning given to the term 'intelligence cooperation'.

5. INTELLIGENCE COOPERATION

Intelligence cooperation, involves the following: (Lander, 2004: 491-492)

— Sharing of intelligence based assessments;
— sharing of assessed, but single-source reporting;
— sharing of pre-emptive intelligence, such as precise reporting of plans or intentions, backed by operational cooperation;
— sharing of the raw intelligence product; and
— operational cooperation, which may involve surveillance; joint agent handling; sharing of linguists; exchanges of technical know-how and equipment; common training; and sharing of analytical staff.

Operational intelligence cooperation includes collection of intelligence, for example the UKUSA agreement, between the UK, the US, Canada, Australia and New Zealand, in terms of which signals collection efforts are divided between the different signatories (Lefebvre, 2003: 530).

In respect of analysis of intelligence, international organisations are important, for example, Europol employs 100 intelligence analysts (Europol, 2006: 15).

International intelligence cooperation can take place at various levels, referred to as the 'agencies' involved and 'granularity'. Granularity refers to complete visibility of the source and product which provides the greatest detail, but carries the most risk; exposing all or part of the raw product, without exposing the source; sharing only a summary of the data; sharing just analysis of the data; and sharing policy conclusions resulting from the intelligence (Clough, 2004: 603).

Intelligence cooperation may take place on local, national and international level, each with its own challenges and modalities. The above areas of cooperation are mentioned within the context of international intelligence cooperation, but could be equally applicable to intelligence cooperation on local, national and regional level. Just as intelligence can be described institutionally, as a process and as a product, intelligence cooperation can be expressed along the same lines.

The types of intelligence of particular interest within the context of intelligence cooperation include travel patterns, profiling of mail and courier services, including analyses of bills-of-lading cross referenced with crime databases; shared illicit nodes linked to fraudulent documents; arms suppliers, financial experts (whose expertise is abused for money-laundering and terrorist financing), drug traffickers and other criminal enterprises; the use of communications networks for criminal purposes; technical and personnel support overlapping between criminal enterprises and groups; abuse of information technology for criminal purposes; use of corruption; suspicious financial transactions, money-laundering and terrorist funding (US, 2005(d): 44-58).

5.1. Models of intelligence cooperation

There are a number of cooperation models in the form of strategies and plans developed for the IC, as well as, for example, crime intelligence and military intelligence. An analysis of these models reveals that, although the focus is the improvement of information or intelligence sharing, the models include measures aimed at improving the whole intelligence process. Examples of national models of intelligence cooperation mainly relating to national intelligence cooperation are:

— The *National Criminal Intelligence Sharing Plan* (US, 2003(a)).
— *Fusion Centre Guidelines: Developing and Sharing Information and Intelligence in a New Era* (US, 2006(c), 2006).
— The (UK) *National Intelligence Model* (ACPO, 2005).
— *Department of Defence Information Sharing Strategy* (US, 2007(b)).
— *Department of Homeland Security Information Sharing Strategy*. (US, 2008(b)).
— *US Intelligence Community Information Sharing Strategy* (US, 2008(a)).

5.2. Products of intelligence cooperation

The combating of international crime is greatly enhanced by the products of international cooperation, especially in the law enforcement environment. In this regard the different notices circulated by INTERPOL can be mentioned, alerting police services globally to persons wanted for extradition in respect of crimes; collecting information about a person's identity or activities in relation to a crime; providing warnings and crime intelligence in respect of persons who have committed a crime and are likely to repeat these crimes in another country; and providing warnings about potential threats from disguised weapons, parcel bombs and other dangerous materials; suspected groups or individuals who are targets in respect of sanctions of the UN against Al-Qaida and the Taliban. INTERPOL also carries lists of wanted persons in a number of countries.

INTERPOL also provides the MIND/FIND mobile service regarding access to databases containing millions of records of criminal information on individuals and property submitted by Member States. This includes a database of passports, identity cards and visas reported stolen or lost by countries all over the world. There is also a database of stolen vehicles. All these databases can now be accessed on a mobile instrument by law enforcement officers (INTERPOL, 2008(j)).

Within the EU, an *Organised Crime Threat Assessment (OCTA)* and *EU Terrorism Situation and Trend Report* were produced by Europol (Europol, 2006: 5) (Europol, 2007(a)) (Europol, 2007(b)).

5.3. Institutions for intelligence cooperation

Institutionally, intelligence cooperation relates to the intelligence interaction and assistance between the agencies respectively responsibly for military, positive and civilian intelligence. Most notable are the fusion centres established in the US, on different levels, integrating intelligence from a wide variety of role-players, including civil society. Following the events of 11 September 2001, the Office of the Director of National Intelligence (DNI) was established in the US, to ensure overall coordination of intelligence. International organisations such as INTERPOL, Europol and ASEANAPOL originated from a need to collect, analyse and distribute information relating to law enforcement.

International organisations exclusively focused on intelligence cooperation have been established on a formal and informal level, such as the Club of Berne in Europe; the Kilowatt Group, including South Africa and Israel; the NATO Special Committee and the Egmont Group of Financial Intelligence Units; and within the African Region, the Committee of Intelligence and Security Services of Africa (CISSA) (Lefebvre, 2003: 530-532) (AU, 2005(b): 12). The AU also established the Continental Early Warning System, focused on security issues and conflict

resolution in Africa, including issues such as arms proliferation and arms trafficking, land-mines, mercenarism and terrorism (AU, 2008).

6. CONCLUSION

In this chapter, the international crimes relating to not only the security of individuals, but also the security of states and in some instances global security, namely war crimes, genocide and crimes against humanity; international terrorism, transnational organised crime, mercenary crimes, piracy; and crimes relating to the proliferation of WMD were described, with reference to the relevant international instruments and principles of international law. In respect of numerous international crimes, there is a lack of universally accepted definitions, despite the existence of numerous international instruments, only war crimes; genocide and crimes against humanity; and piracy are well defined in international law. The drafting of effective national legislation to implement international instruments on transnational organised crime and terrorism, is possible, within the context of existing international instruments, despite the need, in respect of terrorism to define the term in the *Draft Comprehensive Convention on Terrorism.*

International and regional instruments on mercenary activities have been identified in the UN and AU for review to effectively address the extensive use of private military and private security companies in armed conflicts in a combat role. Consequently few countries have effective legislation to act against mercenary activities. Crimes related to WMD are required in terms of UN Security Council Resolution 1540 to be adopted by UN Member States in their national legislation, but the implementation thereof is difficult and controversial in view of the manner in which the powers of the UN Security Council are used to 'legislate' in international law.

The implementation of the various international instruments and consequently cooperation in combating international crime on all levels, including intelligence cooperation, is hampered by this lack of proper definitions as well as the fact that many countries are still not party to many of the key international instruments; or have not ratified or implemented them.

A conceptual framework of the term 'intelligence' is also provided, describing the different meanings of 'intelligence' as well as the dimensions of intelligence, namely foreign, military and domestic intelligence. The terms 'security intelligence' and positive intelligence are also described in relation to law enforcement/crime intelligence. Particular attention is paid to intelligence as a process, with reference to collection of intelligence and the sources of intelligence, as well as an analysis of intelligence. In respect of intelligence as a product, the categories of intelligence products are described, namely warning intelligence, current intelligence, basic intelligence and raw intelligence.

The focus of intelligence is also described, referring to 'new' intelligence priorities, such as terrorism, peacekeeping intelligence and intelligence on WMD. Lastly, the key term to this study, namely 'intelligence cooperation' is analysed and described with reference to models of intelligence cooperation, products of intelligence cooperation and institutions for intelligence cooperation.

In conclusion, it is clear that the international legal framework in respect of key international crimes needs to be improved, especially in relation to defining crimes such as terrorism and mercenary crimes. However, international law is not amended easily, whilst it is important to combat international crime in every possible way, especially in respect of improving intelligence cooperation. It would therefore be more expedient in the shorter term to look at practical and operational means to improve the situation.

In the next chapter a historical background to intelligence cooperation is provided, as well as a description of international obligations in respect of intelligence cooperation. This is an important factor to determine whether intelligence cooperation could be improved through further obligations in respect of cooperation, and when the challenges for intelligence cooperation are analysed to assess the effectiveness of international obligations in respect of intelligence cooperation.

CHAPTER 3
IMPERATIVES FOR INTELLIGENCE CO-OPERATION

1. INTRODUCTION

In this chapter, a short overview is provided of the change in the focus and priorities of intelligence with reference to the periods following the end of the Cold War and the watershed events of 11 September 2001, respectively.

The international obligations in the various conventions and resolutions of the UN Security Council; the AU; SADC and ASEAN pertaining to international information sharing and cooperation in respect of special investigative techniques, are furthermore discussed in this chapter. Drivers for intelligence cooperation and intelligence sharing, such as globalisation, the value-for-money concept, and the enrichment of intelligence, are discussed. The focus of intelligence during the post-Cold War era is dealt with first.

2. THE CHANGE IN INTELLIGENCE FOCUS IN THE POST-COLD WAR ERA

The intelligence focus during the Cold War era was mainly a military one between the Western and Soviet power blocs. A major intelligence failure in the US was insufficient intelligence warning of the impending collapse of the Soviet Union: “What is clear is that an agency that had spent the last 40 years primarily on trying to discern the intentions of the Soviet Union and its leaders had overestimated the strength of the Soviet economy” (Green, 2005: 37). One of the post-Cold War failures relating to Iraq’s WMD, is ascribed to institutional bias of

collectors to share operational information with analysts (Green, 2005: 45). The intelligence strategy of the US reflects the trend in the change in priorities, to the combating of terrorism and to prevent and counter the spread of WMD, for example in the *National Intelligence Strategy of the United States of America* (US, 2005(b)). In addition to refocused strategic objectives various institutional or 'enterprise objectives' are also stated, such as the optimisation of collection capabilities, improved access to intelligence by the IC and customers, and to establish new and strengthen existing foreign intelligence relationships (US, 2005(b): 4, 5). There is furthermore a strong move towards an 'integrated intelligence enterprise' with a new information sharing model where, for instance the generally accepted, but outdated 'need-to-know principle' is substituted by the principle of 'responsibility to provide', reflected in the *United States Intelligence Community: Information Sharing Strategy* (US, 2008(a): 7, 9).

In the post-Cold War era the IC had to re-establish itself in respect of new focus areas. Rimington, a previous Director General of the British Security Service reflected upon the 'certainties of the Cold War and the state of flux' in which intelligence agencies were finding themselves thereafter (Rimington, 1994). Throughout the post-Cold War period the IC seems to have been searching for a reason to exist (Green, 2005: 47).

Way before the 11 September 2001 events, terrorism and proliferation matters were identified as a substitute for the void left by the end of the Cold War (Rimington, 1994). In the US there were indicators that the intelligence system was at cross-roads before 2001, with numerous deficiencies, identified (Hulnick, 1999: 1), and the future role of intelligence in respect of drug trafficking, organised crime, terrorism and crimes related to WMD already then laid out (Hulnick, 1999: Chapter 6).

Failures by the IC to prevent and manage conflicts in the post-Cold War era, such as that in Somalia, Bosnia and the genocide in Rwanda, highlighted the

critical need for strengthening prevention mechanisms such as Early Warning Systems which could support early action. Numerous governmental and non-governmental bodies consequently became involved in early warning (Wane, 2008: 4). The example of the AU will be dealt with later on in this chapter. The post-11 September 2001, developments in the US set the scene for more focused intelligence cooperation, especially intelligence and information sharing.

3. THE EFFECT OF 11 SEPTEMBER 2001 EVENTS ON THE FOCUS OF INTELLIGENCE

The events of 11 September 2001, as well as the intelligence failures in respect of WMD in Iraq, played a major part in the focus of the IC on terrorism and WMD. Few single events in history had such a major impact on intelligence cooperation and sharing on all levels, as the 11 September 2001 events.

Transatlantic intelligence and security cooperation expanded considerably after both the 11 September 2001 events and the bomb attack in Madrid 911 days thereafter. Additional Airborne Warning and Control System (AWACS) aircraft (used to perform airborne surveillance, and command, control and communications functions for both tactical and air defence forces), were provided by Europe to assist with the protection of the US, which allowed the US to release American aircraft for duty elsewhere. Europol was designated as a central point for data exchange between European law enforcement agencies and the US (Aldridge, 2004: 731).

Although the 11 September events led to huge internal improvements in intelligence cooperation and sharing in the US, the most important paradigm shift emanated from the realisation that the US needs partners in a protracted war on terrorism with a global reach. Furthermore, it was realised that the Achilles heel of US intelligence, despite its technological capabilities regarding imagery and interception, is the need for the country to be assisted by smaller intelligence

agencies with HUMINT capabilities. The US even experienced a lack of interpreters in foreign languages (Reveron, 2006: 454). The US realised it could provide training and other assistance to foreign agencies, in exchange for HUMINT, intelligence sharing or being allowed to use foreign territory for surveillance, rather than having to develop HUMINT capabilities (Reveron, 2006: 455).

In South-East Asia the 11 September 2001 events marked the passage of the post-Cold War era. Before those events the regional security issues were dominated by domestic instability with spill-over potential such as in Indonesia, the South China Sea crisis and various territorial disputes in the region (Acharya, 2003: 1). After the 11 September 2001 events, the threat of international terrorism became the focus of security attention, although the other threats did not disappear. South-East Asia has been termed as the 'second front' in the global war on terror (Acharya, 2003: 2, 3). The US engagement in South-East Asia had been marginal and uncertain prior to the 11 September 2001 events. The region now enjoys a higher priority in US strategic thinking, although the "US re-engagement in South-East Asia is not comparable to that in India, Pakistan or in Central Asia" (Acharya, 2003: 5).

Recognition of new threats in terms of crime in the region is not limited to terrorism. During the opening of a regional police chiefs meeting (ASEANAPOL), it was mentioned that "a new form of war with non-conventional threats such as terrorism, the illegal trade in narcotics, trade in human beings, crimes connected with money-laundering and other forms of transnational crime" requires the creation of security through intelligence exchange. This observation was made with reference to the post-Cold War era, and following the 11 September 2001 events and the Bali bombing (Bali News, 2005).

The global response to the 11 September 2001 events is reflected in national counter-terrorism legislation adopted in numerous countries, various resolutions

of the UN Security Council and the global strengthening of measures to combat terrorism.

On an institutional level, law enforcement agencies acquired extensive overseas missions whilst intelligence agencies also focus on illegal activities abroad, despite the fact that law enforcement and intelligence communities operated in "fundamentally dissimilar manners retaining different legal authorities, internal modes of organisation, and governing paradigms" (US, 2001: 2).

It is important to determine the nature of international obligations for intelligence cooperation, as well as other, more practical imperatives, drivers or incentives for intelligence cooperation. In this regard global obligations are most important and are dealt with next.

4. INTERNATIONAL OBLIGATIONS: INTELLIGENCE COOPERATION

Universal obligations form the highest order of international obligations, namely those obligations which are generally applicable to basically all states or at least all the Member States of the UN.

4.1. Universal obligations

The first category of obligations consists of resolutions of the UN Security Council, which are of a binding nature.

4.1.1. United Nations

Resolution 1373/2001 of the UN Security Council was adopted within days of the 11 September 2001 events. It *inter alia* calls upon all states to find ways of

intensifying and accelerating the exchange of operational information, in particular information regarding the following: (UN, 2001(b): 3)

— Actions or movements of terrorist persons or networks;
— forged or falsified travel documents;
— traffic in arms, explosives or sensitive materials;
— use of communications technologies by terrorist groups; and
— the threat posed by the possession of WMD by terrorist groups.

The Resolution furthermore calls for the exchange of information in accordance with international and domestic law and to cooperate on administrative and judicial matters to prevent the commission of terrorist acts, and to cooperate through bilateral and multilateral arrangements to prevent and suppress terrorist acts and to take action against the perpetrators of such acts (UN, 2001(b): 3).

Resolution 1540(2004) of the UN Security Council which deals with measures to prevent the proliferation of WMD, is not specific in respect of information exchange, but calls upon states to promote cooperation on nonproliferation so as to address the threat posed by proliferation of nuclear, chemical or biological weapons and their means of delivery and to take 'cooperative action' to prevent illicit trafficking in nuclear, chemical or biological weapons, their means of delivery and related materials (UN, 2004(b): 4). The language in respect of intelligence cooperation in the two Resolutions is rather weak, and by simply 'calling' upon States does not seem to place a specific obligation on States.

There are, however, in numerous counter-terrorism instruments more strongly worded obligations in respect of the exchange of information on the relevant terrorist crimes, for example:

— Obligating the exchange of information and coordinating the taking of administrative and other measures as appropriate to prevent the commission of the crimes mentioned in the respective Conventions (*UN: Convention on the Prevention and Punishment of Crimes against*

Internationally Protected Persons, including Diplomatic Agents, (UN, 2001(a): 32, Article 4(b)); *International Convention against the Taking of Hostages*, (UN, 2001(a): 40, Article 4(b)); *Convention for the Suppression of Unlawful Acts Against the Safety of Maritime Navigation*, (UN, 2001(a): 77, Article 13(b); *International Convention for the Suppression of Terrorist Bombings*, (UN, 2001(a): 109, Article 15(b)).

— Obligating the establishment and maintenance of channels of communication between the competent agencies and services to facilitate the secure and rapid exchange of information concerning all aspects of offences in the relevant Convention (*International Convention for the Suppression of the Financing of Terrorism* (UN, 2001(a): 127, Article 18(3)(a)).

— Obligating cooperation between States on the offences in the relevant Convention concerning the identity, whereabouts and activities of persons in respect of whom a reasonable suspicion exists that they are involved in the relevant terrorist financing offences; as well as the movement of funds relating to the commission of such offences (*International Convention for the Suppression of the Financing of Terrorism*, (UN, 2001(a): 127, Article 18(3)(b).

On a practical enforcement level, the UN Security Council has established committees to promote and ensure compliance with sanctions imposed on individuals and entities identified to be connected to Al-Qaida and the Taliban and associates (UN, 2008(i) (j)).

The obligations in respect of international cooperation in relation to intelligence are much more explicit in the *UN Convention against Transnational Organized Crime*, which requires the establishment in Member States of a financial intelligence unit to serve as a national centre for the collection, analysis, and dissemination of information regarding potential money-laundering. States are required to ensure that administrative, regulatory, law enforcement and ‘other

authorities' have the ability to 'cooperate and exchange information at the national and international level' (UN, 2004(a): 9: Article 7(1)(b)).

The said Convention envisages joint investigative bodies (in other words between states) regulated by bilateral or multilateral agreements or on a case-by-case basis (UN, 2004(a): Article 19). The Convention not only obliges states to allow in their national laws for the use of special investigative techniques such as electronic or other forms of surveillance and undercover operations, and controlled deliveries, but also to enter into agreements to execute such techniques within the context of international cooperation or allow it on a case-by-case basis (UN, 2004(a): Article 20).

States Parties are also obliged to take appropriate measures to encourage persons who participate or who have participated in organised criminal groups to cooperate with law enforcement authorities by supplying information useful to the authorities on matters such as the identity, nature, composition, structure, location or activities of organised criminal groups, links, including international links with other organised criminal groups, and offences that organised criminal groups have committed or may commit (UN, 2004(a): Article 26).

The *Rome Statute of the International Criminal Court*, obliges States Parties to comply with requests of the ICC to provide the identification and whereabouts of persons or the location of items; the taking of evidence and production of evidence; including expert opinions and reports necessary to the Court; the questioning of any person being investigated or prosecuted; the examination of places or sites including the exhumation and investigation of grave sites; the execution of searches and seizures; and the identification, tracing and freezing or seizure of proceeds, property and assets and instrumentalities of crimes for the purpose of eventual forfeiture (UN, 1999 – 2003: Article 93).

States may protect national security information from being disclosed as a result of requests for information by the Court to the State. A mechanism is provided for in the *Rome Statute of the International Criminal Court* to resolve in a cooperative manner disputes following the expression of an opinion by a state that information must be withheld as a result of the opinion of the state that the information constitutes national security information. These steps include the modification of the request by the Court; seeking ways of obtaining the information from another source or in a different form and an agreement on conditions under which the assistance could be provided including, among other things, summaries or redactions, limitations on disclosure, use of *in camera* or *ex parte* proceedings, or other protective measures permissible under the Statute and the Rules of Procedure and Evidence (UN, 1999 – 2003: Article 72(5).

The *Rome Statute of the International Criminal Court* obliges the Court to ensure the confidentiality of documents and information, except as required for the investigation and proceedings described in the request (UN, 1999 – 2003: Article 93(8)(2)). In respect of police cooperation, INTERPOL plays the most important role and the nature of the legal framework thereof is of particular importance.

4.1.2. International Criminal Police Organization

ICPO-INTERPOL, was established in 1956 (Van Den Wyngaert, 1996: 249). In general, international police organisations are designed to facilitate interstate communication, providing networks of information sharing between states and "to serve as clearinghouses for gathering of information, analysis and reporting of finished intelligence" (Gerspacher, 2002: x).

INTERPOL functions in terms of a Constitution to which Members voluntarily subscribe. Such a model does not require ratification by the states involved, as is the case with international instruments such as agreements between states or an international convention. The lack of a ratification process is believed to impair

INTERPOL by not commanding less commitment from Member States as if a convention were in place. Membership of INTERPOL is not well-defined. It is not clear whether members are police units, the entire law enforcement community at the national level of a state or 'yet another population'. The matter is left for the interpretation of individual Member States, which may cause Member States to escape their obligations. On the other hand this 'uncertainty' results in the organisation being flexible and adaptive (Gerspacher, 2002: 45, 46). According to the Constitution of INTERPOL, any country may delegate as a Member to INTERPOL any official police body whose functions come within the framework of activities of the Organisation (INTERPOL, 2007(a): Article 4). There may be more than one delegate from a country, but only one delegation head representing the country (INTERPOL, 2007(a): Article 7).

The INTERPOL Constitution itself is silent on the issue of intelligence cooperation and even information exchange. It simply states that the General Secretariat of INTERPOL shall amongst others: (INTERPOL, 2007(a): Article 26)

(b) Serve as an international centre in the fight against ordinary crime;
(c) Serve as a technical and information centre;
(d) Maintain contact with national and international authorities.

The General Assembly of INTERPOL is, however, empowered to adopt resolutions and make recommendations to Member States on matters with which INTERPOL is competent to deal and to examine and approve any agreements to be made with other organisations (INTERPOL, 2007(a): Article 8). The Annual General Assembly generates resolutions to draw up policies regarding the Member States. Although there is no obligation on Member States to follow the guidelines for information exchange, most Member States in practice do follow it. The INTERPOL Standard Operating Policies and Procedures (SOPP) are prepared by the INTERPOL Working Group and set out the framework for

Member State cooperation. The policies are only recommendations and not binding (Ryan, 2006: 107). Strict rules have been laid down for the processing of information for police cooperation. In view of the strict rules to regulate the access to and transfer of information, cooperation agreements are necessary between INTERPOL and international organisations. This has led to numerous cooperation agreements concluded by INTERPOL, for example with the following: (INTERPOL, 2008(a))

— The International Commission on Missing Persons;
— the International Atomic Energy Agency;
— the International Maritime Organisation;
— the Office of the prosecutor of the International Criminal Court;
— the World Intellectual Property Organisation;
— the Special Court for Sierra Leone;
— the Convention on International Trade in Endangered Species of Wild Fauna and Flora (CITES) Secretariat;
— the Council of Europe;
— Europol;
— The UN; and
— The World Customs Organisation.

The agreement with Europol, in addition to the exchange of information, provides for the exchange of liaison officers (INTERPOL, 2001: Article 4).

For some time, the Constitution of INTERPOL has been perceived to inhibit intelligence and other police cooperation through INTERPOL in order to combat terrorism. The Constitution of INTERPOL prohibits INTERPOL from investigating political matters, whilst a political motive often is an element of terrorist activities (Wilkinson, 2006: 165). It is, however, notable that INTERPOL is recently playing an increasingly important role in combating terrorism. The opinion is held that this is the result of UN sanctioned obligations, such as the lists of Al-Qaida and

Taliban terrorists published by the Resolution 1267 Committee, and the fact that the 13 counter-terrorism instruments (UN, 2008(c)) (UN, 2008(i)(j)) reflect a common understanding of the well-known terrorism offences such as hijacking, terrorist bombings, terrorist financing, hostage-taking, without the need to define the concept of terrorism in a politically controversial fashion. International cooperation through INTERPOL and its "Member Agencies" can be based on a 'common ground' surrounding terrorism by treating it as a depoliticised crime (Deflem, 2006: 249). The General Assembly of INTERPOL condemned the 11 September 2001 events simply as 'a crime against humanity', thereby de-politicising terrorism to enable better global cooperation to combat terrorism (Deflem, 2004:230).

The next layer of cooperation is on the regional level, where the legal basis of cooperation within the EU, AU and South-East Asian regions is analysed.

4.2. Regional obligations for intelligence cooperation

Regional intelligence cooperation is very important as the states within a region usually experience the same threats and have common economic, military and security interests.

4.2.1. The European Union intelligence community

Europol, the Joint Situation Centre (SitCen), the EU Satellite Centre (EUSC) and the Intelligence Division of the EU Military Staff (INTDIV) are regarded as "information agencies providing intelligence reports to the decision-making institutions of the EU, such as the EU Council and the Secretary General/High Representative" (Herzberger, 2007: 52). Europol coordinates information sharing within the EU, whilst SitCen monitors the security situation both in and outside the borders of the EU. The EU Commission has proposed a policy of better

exchange of information between the law enforcement authorities of EU Member States and intelligence-led law enforcement (Herzberger, 2007: 54).

There are seconded officers from the national intelligence and security services stationed in Brussels to inform the EU Council and Commission about the activities of those services and to remain appraised of initiatives such as information sharing (Herzberger, 2007: 59). A Counter-Terrorism Coordinator is located in the EU Council Secretariat. A Counter Terrorism Group (CTG) outside the EU structure, consisting of the heads of all national intelligence and security services of the EU Member States has been established to improve international cooperation, including common threat assessments on terrorism. It serves as a useful forum on operational level for multilateral cooperation and to pick up trends in counter-terrorism policy (Herzberger, 2007: 61). The CTG had its origin in the Berne Group or Club of Berne which established working groups for combating both organised crime and terrorism. The Berne Group is not based on a formal charter and operates outside the institutions of the EU. There appears not to be a formal commitment or expectation of cooperation in the Berne Group (Walsh, 2006: 631). For purposes of this chapter it is not discussed in further detail, as the focus here is more on formal relations and obligations. Although civilian intelligence and military intelligence are dealt with separately by respectively the SitCen and INTDIV, both forms of intelligence are integrated in reports through the Single Intelligence Analysis Capacity (SIAC) before submission to intelligence customers (Herzberger, 2007: 70).

4.2.2. European Police Office

Europol was established in 1995 through the *Europol Convention*, concluded under the auspices of the EU (Europol, 2008(a)). The principal tasks of Europol are the facilitation of the exchange of information between Member States; to obtain, collate and analyse information and intelligence; to notify the competent authorities of Member States through national units, of information concerning

them and of any connections identified between criminal offences; to aid investigations in the Member States by forwarding information to national units in Member States; to maintain a computerised system of collected information containing data in accordance with the Convention; to participate in a support capacity in joint investigation teams; and to ask the competent authorities of the Member States concerned to conduct or coordinate investigations in specific cases (Europol, 2008(a): Article 3). Europol began operations in 1999 (Walsh, 2006: 632).

There is an obligation on Member States to consider and deal with any request from Europol to initiate, conduct or coordinate investigations in specific cases. Member States must inform Europol whether such investigation is being initiated and must provide reasons for not complying with a request. The only circumstances in which a Member State is not obliged to provide reasons for non-compliance with a request is if providing such reasons would harm essential national security interests; or would jeopardise the success of investigations under way or the safety of individuals (Europol, 2008(a): Article 3b).

Member States are required to designate a national unit to carry out the tasks determined in the Convention. Save for a specific agreement with the Member State involved, communication between Europol and the Member State is restricted to the national unit. National units are tasked in terms of the Convention to take the initiative to provide the information and intelligence necessary for Europol to perform its tasks. National units must furthermore respond to Europol's requests for information, intelligence and advice; update information and intelligence; evaluate information and intelligence in accordance with national laws for the competent authorities and transmit such information and intelligence to them; issue requests for advice, information or intelligence to Europol; and supply information to Europol for storage in its computerised system (Europol, 2008(a): Article 4). Each national unit must second at least one liaison officer to Europol (Europol, 2008(a): Article 5). The secondment of police officers

and officials is regarded as most effective in building a network of informal international cooperation (Wilkinson, 2006: 165). The contacts and personal relationships with other liaison officers greatly facilitate the exchange of intelligence or information. They act as 'hubs of facilitators' and provide informal networks of intelligence sharing (Hertzberger, 2007: 75).

In line with the strict regime of data protection and privacy which characterises the European Union, the Europol Convention lays down strict rules as to the contents and details of data that may be kept by Europol; and the purpose for which it may be kept. In addition to certain personal data, such as the identifying of particulars of individuals, Europol may keep data of: (Europol, 2008(a): Article 8)

— Criminal offences, alleged crimes and when and where they were committed;
— means which were or may be used to commit the crimes;
— departments handling the case and their filing references;
— suspected membership of a criminal organisation; and
— convictions, where they relate to criminal offences for which Europol is competent.

Individuals have a right of access to data relating to them or to have such data checked, and may make a request in that regard to the competent authority. The competent authority must convey it to Europol to deal with it within three months.

The law of the relevant country applies to such a request. Europol may refuse an application if such refusal is necessary to: (Europol, 2008(a): Article 19(3))

— Enable Europol to fulfill its duties properly;
— protect security and public order in the Member States or to prevent crime; and
— protect the rights and freedoms of third parties.

Considerations which it follows cannot be overridden by the interests of the person concerned by the communication of the information.

On the practical level, it seems as if Europol experiences a lack of resources to act as a European clearing-house for crime intelligence. Europol states that it would be more capable to fulfill such a role if it has more resources, such as more analysts (Herzberger, 2007: 80). Europol is increasingly fulfilling a more strategic role, impacting on the policy level, although its main customer remains the national police forces in the EU. It is not excluded that Europol strives towards being the criminal intelligence centre for the EU (Herzberger, 2007: 81).

A region where huge development occurred in respect of developing an infrastructure for intelligence and law enforcement cooperation, is Africa, with a leading role played by the AU and related sub-regional structures.

4.2.3. The African Union

The *Constitutive Act of the AU* and the *Protocol relating to the Establishment of the Peace and Security Council (PSC) of the AU* gives the AU the power to create the structures and processes in order to establish a comprehensive peace and security architecture for the African Continent. This architecture includes the PSC, the Panel of the Wise, the African Standby Force, and the Continental Early Warning System (Wane, AU, 2008: 3).

The PSC shall, among others, take all necessary steps to anticipate and prevent disputes and conflicts, as well as policies that may lead to genocide and crimes against humanity; ensure the implementation of AU and other relevant instruments on terrorism; and harmonise and coordinate efforts at regional and continental levels to combat international terrorism. To this end a Continental Early Warning System shall be established using a situation room which serves as an observation and monitoring centre to collect and analyse data. The

Continental Early Warning Centre is supported by regional early warning centres, also provided for in the said Protocol (Wane, AU, 2008: 3).

The *AU Non-Aggression and Common Defence Pact*, regards technological assistance of any kind, intelligence and training to another State for use in committing acts of aggression against other Member States of the AU as 'aggression', which is forbidden in terms of the Pact. In terms of the Pact, State Parties of the AU undertake to intensify collaboration and cooperation in all respects relating to combating international terrorism and any other form of organised transnational crime (AU. 2005(a): Article 5). These Parties also undertake to cooperate and enhance their military and intelligence capabilities through cooperation (AU. 2005(a): Article 7). The Pact furthermore provides for the establishment of the ACSRT to centralise, collect and disseminate information; studies, and analysis on terrorism and terrorist groups; provide training programs; and assist Member States to develop expertise and strategies for the prevention and combating of terrorism. The Parties to the Pact are obliged to support and actively participate in the activities of the Centre (AU. 2005(a): Article 13).

The role of the PSC of the AU as implementing agency in respect of the combating and prevention of terrorism is further elaborated upon in the *AU Protocol to the OAU Convention on the Combating and Prevention of Terrorism*. The PSC must harmonise and coordinate continental efforts in the prevention and combating of terrorism, and must establish operating procedures for information gathering, processing and dissemination; establish mechanisms to facilitate information exchange among States Parties on patterns and trends in terrorist acts and the activities of terrorist groups and on successful practices in combating terrorism; and establish an information network with national, regional and international focal points on terrorism (AU. 2004(a): Article 4).

The Commission of the AU is also charged with an oversight and facilitation role in the prevention and combating of international terrorism. The Commissioner in charge of Peace and Security, assisted by a unit established within the PSC and Security Council of the Commission and the ACSRT, shall amongst others, provide technical assistance on legal and law enforcement matters relating to combating the financing of terrorism; develop and maintain a database on issues relating to terrorism, including experts and technical assistance available; maintain contacts with regional and international organisations and other entities dealing with issues of terrorism; and provide advice and recommendations to Member States on how to secure technical and financial assistance in the implementation of continental and international measures against terrorism (AU. 2004(a): Article 5).

The Assembly of the AU endorsed the establishment of CISSA, in Abuja, Nigeria on 26 August 2004. The Assembly agreed that CISSA should collaborate with the AU and all its organs and directed that an Intelligence and Security Committee located in the Office of the Chairperson of the AU Commission shall be created for that purpose. The said Office shall be the recipient of reports from the CISSA Secretariat or other CISSA structures (AU, 2005(a)). At the fifth annual conference of CISSA, held in May 2008 in Cape Town, it was reported that a number of milestones had been reached in respect of the governance, executive and administrative structures, including the operationalisation of the secretariat of CISSA. The organisation has, in addition to some pre- and post-election analyses, developed a Continental Threat Assessment which was updated annually and which identified key intelligence priorities. Furthermore an Africa-wide secure communications system between the CISSA headquarters and Member States' services to facilitate intelligence exchange and interaction was established (Kasrils, 2008: 4).

Within the AU context, the *OAU Convention on the Prevention and Combating of Terrorism* is very specific on the areas of cooperation required in terms of

information exchange amongst the States Parties to the Convention. States Parties undertake in terms of the Convention to strengthen the exchange of information regarding the following: (AU. 1999: Article 5)

- Acts and crimes committed by terrorist groups, their leaders and elements, their headquarters and training camps, their means of sources and funding and acquisition of arms, their types of arms, ammunition and explosives used, and other means in their possession;
- the communication and propaganda methods and techniques used by the terrorist groups, the behaviour of these groups, the movement of the leaders and elements, as well as travel documents;

Also any information that may-

- lead to the arrest of any person charged with a terrorist act against the interest of a State Party or against its nationals, or attempted to commit such an act or participated in it as accomplice or an instigator; or
- lead to the seizure and confiscation of any type of arms, ammunition, explosives, devices or funds or other instrumentalities of crime used to commit a terrorist act or intended for that purpose.

The Convention demands the preservation of confidentiality of exchanged information and that the providing of such information to a third state party is subject to the consent of the state party which provided the information. The Convention also provides for cooperation in research and development of expertise and exchange thereof; technical assistance and joint training

programmes to improve scientific, technical and operational capacities to combat terrorism.

4.2.4. Southern African Region: Southern African Development Community

SADC is developing a regional early warning system, which is described as being "integrated in the intelligence community and based on classified information". Despite this description, it is clear that intelligence to be used will be primarily open-source based (Wane, AU, 2008: 7). This apparent contradiction illustrates some confusion between warning intelligence and early warning. Early warning entails a focus on destabilisation within states in respect of which the collection of intelligence is predominantly a domestic issue. The restraints upon the AU and SADC in this regard would be the same as that of the UN which is precluded from engaging in techniques that employ secrecy or stealth- in effect 'spying' on Member States (Hough, 2004: 27). The Regional Early Warning System is based in Gaborone, Botswana, and is supported by a National Early Warning Centre in each of the Member States of SADC. SADC is in the process of establishing a situation room and recruiting analysts (Wane, AU, 2008: 6). The Regional Early Warning Centres are supposed to play a complementary role in the implementation of the *AU Protocol to the OAU Convention on the Combating and Prevention of Terrorism*. To this end Member States must, *inter alia* establish contact points on terrorism in the region and establish modalities for sharing of information on the activities of the perpetrators of terrorist acts (AU. 2004(a): Article 6). In the SADC *Strategic Indicative Plan for the Organ on Politics, Defence and Security Cooperation (SIPO)*, intelligence cooperation in the form of the exchange of intelligence through the development of a common database on cross-border crime is mentioned as a "strategy/objective" (SADC, 2001: 34). Most of the international crimes mentioned in this study are mentioned amongst challenges for the SADC region, which challenges include "Efficient communications systems backed by a reliable criminal intelligence network" (SADC, 2001: 77).

Of particular importance in the SADC sub-region, is the mechanism for police cooperation, the Southern African Regional Police Chiefs Cooperation Organisation (SARPCCO), established on 1 August 1995. This organisation consists of the police chiefs of most Southern African countries who are Member States of SADC, namely Angola; Botswana; Democratic Republic of the Congo; Lesotho; Malawi; Mauritius; Mozambique; Namibia; South Africa; Swaziland; Tanzania; Zambia; and Zimbabwe. SARPCCO had been established by a simple decision by its members and the adoption of a Constitution which regulates its functions, aims and objectives. This Constitution is not in the form of an international agreement which requires ratification by the legislatures of the Members' Countries. This means that cooperation within SARPCCO at its inception was based on voluntary cooperation rather than international obligations. The major objectives of SARPCCO are: (INTERPOL, 2008(c))

- To prepare and disseminate relevant information on criminal activities as may be necessary to benefit members to contain crime in the region;
- to carry out regular reviews of joint crime management strategies in view of changing national and regional needs and priorities; and
- to ensure efficient operation and management of criminal records and efficient joint monitoring of cross-border crime taking full advantage of the relevant facilities available through INTERPOL.

The Regional Bureau in Harare, Zimbabwe serves as permanent secretariat for SARPCCO. The Secretariat of SARPPCO and the INTERPOL Regional Bureau thus act as one, utilising the same premises, office equipment and facilities. The SARPCCO Constitution is, however, reinforced by a binding multilateral international agreement requiring ratification. The *Agreement in respect of Co-operation and Mutual Assistance in the Field of Crime Combating* provides for,

inter alia the regular exchange of information; the planning, coordination and execution of joint cross-border operations, including undercover operations; and the controlled delivery of illegal substances or any other objects (RSA. 1997: Article 5(1)). This agreement was signed in Harare, Zimbabwe, on 30 September 1997 (INTERPOL, 2008(c)).

Notable successes had been achieved with cross-border operations aimed at drugs and vehicle theft carried out under the auspices of SARPCCO. Huge successes have been obtained in respect of regional cooperation to combat the proliferation of small arms and light weapons. Intelligence-driven operations to locate, gather and destroy arms caches which are the remnants of civil wars were executed in Mozambique *(Operations Rachel)*; Angola and Namibia *(Operation Mandume)*; and the Democratic Republic of the Congo *(Operation Fifi)*. During these operations, hundreds of tons of weapons (including arms caches, seized, captured, obsolete or redundant firearms) have been destroyed, decreasing the number of firearms available to criminal elements or rebel groups, limiting the move of firearms from one country to another in the region and limiting the use of firearms in crime (SaferAfrica, 2006: 24-26) (Rhodes, 2007).

In the South-East Asian Region security and defence cooperation evolved in intelligence and law enforcement cooperation, which must be noted to understand the global network of intelligence and law enforcement cooperation. This will subsequently be discussed.

4.2.5. Association of South-East Asian Nations

Five countries, namely Indonesia, Malaysia, Philippines, Singapore and Thailand established the ASEAN on 8 August 1967. The organisation was joined by Brunei Darussalam in 1984; Vietnam in 1995; Lao Peoples' Democratic Republic and Myanmar in 1997 and Cambodia in 1999. One of the pillars of ASEAN is the Security Community. It has Components for political development, conflict

prevention, and post-conflict peace building (ASEAN, 2008(a)). There is a practice of secret annual meetings of intelligence agencies of the ASEAN countries with intelligence sharing increasing over the years. As far back as 1976, "an agreement for an exchange of information, of views and intelligence among the countries in Southeast Asia for the past four years" was confirmed. Intelligence sharing amongst the ASEAN Member States has over the years become more extensive (Acharya, 1991: 165, 166).

Within the broader region, outstanding operational co-operation was evident between the Indonesian Authorities and the Australian Federal Police (AFP) in *Operation Alliance,* the joint investigation into the Bali bombings of 12 October 2002. The AFP was able to respond immediately by coordinating the multi-national police response team in areas such as technical intelligence, intelligence assessment, bomb scene investigation, disaster victim identification and forensic evidence (McFarlane, 2005: 305). After the 11 September events, a trilateral agreement was signed between Malaysia, Indonesia and the Philippines. The agreement provides for anti-terrorism exercises as well as combined operations to hunt suspected terrorists, the setting up of hotlines and sharing air passenger lists, aimed at speeding intelligence exchange between these countries (Acharya, 2003: 13).

ASEAN undertook a number of actions to combat terrorism, such as: (Asia Pacific Economic Cooperation, 2003: 2, 4)

— Improving cooperation amongst the Member States' law enforcement agencies in combating terrorism and sharing best practices;
— enhancing intelligence exchange with the emphasis on terrorists and terrorist organisations, their movement and funding, and any other information needed to protect lives, property and security of modes of travel;

- strengthening cooperation between the ASEAN Ministerial meeting on Transnational Crime and other relevant bodies in ASEAN in countering and preventing all forms of terrorist acts;
- developing regional capacity building programmes to improve the capabilities of Member States to investigate, detect, monitor and report on terrorist acts; and
- immigration authorities of Member States have agreed to assist and coordinate with other law enforcement authorities in the region to deter cross-border terrorism by establishing intelligence units to address trafficking in persons and terrorism.

ASEAN adopted a *Work Programme to Implement the ASEAN Plan of Action to Combat Transnational Crime* (ASEAN, 2002). The action-steps on illicit drug trafficking, trafficking in persons, piracy, robbery at sea, arms smuggling, money-laundering, terrorism, international economic crime and cyber crime have the following common features: (ASEAN, 2002)

- Conducting typology studies on trends and *modus operandi* in respect of the mentioned crimes;
- maximising the use of modern information and communications technology to facilitate the exchange of data on criminal methodologies, arrests, legal documents and requests for assistance;
- regular joint regional training;
- establishing directories of focal points in respect of, amongst others, law enforcement, in the respective countries and institutions;
- considering the developing of multilateral and bilateral legal arrangements to facilitate the apprehension, investigation, prosecution, extradition and various forms of mutual legal assistance such as the exchange of witnesses, sharing of evidence, enquiry into and seizure and forfeiture of the proceeds of crime;
- promoting the efficient networking of relevant national agencies and organisations in the ASEAN countries.

— promoting cooperation and intelligence exchange with the UN International Maritime Organisation, INTERPOL, Europol, and customs and immigration authorities;
— enhancing cooperation and coordination in law enforcement and intelligence sharing; and
— the establishment of financial intelligence and investigative units.

The law enforcement community in the ASEAN region has also organised itself in an effective structure for regional cooperation, called ASEANAPOL, discussed hereunder.

4.2.6. Association of South-East Asian Chiefs of Police

ASEANAPOL was established in 1981 to minimise criminality in the South-East Asian Region, through cooperation within the ambit of the ASEAN organisation. It has established three *ad hoc* commissions to deal with illicit drug trafficking, mutual assistance in criminal matters, terrorism, arms smuggling, economic and financial crimes, credit card fraud, extradition and arrangements for handing over criminal offenders and fugitives (ASEANAPOL, No date).

ASEANAPOL has also established its own database to enable Member States to exchange information and enhance access to INTERPOL databases. During 2007, ASEANAPOL and INTERPOL concluded a historic agreement. The agreement means that information stored in the electronic ASEANAPOL databasis system will be accessible to law enforcement agencies worldwide through INTERPOL's secure global police communications system called I-24/7. Any searches made of the ASEANAPOL database system will automatically run against INTERPOL's Stolen and Lost Travel Document and Stolen Motor Vehicle databases. INTERPOL has never before agreed to share these databases with another regional or international entity on a real-time basis (INTERPOL, 2007(b)).

At its 2008 conference ASEANAPOL Members recommitted themselves to enhance coordination and cooperation through intelligence sharing for: (ASEAN, 2008(b))

— The identification, tracing, freezing, forfeiture and confiscation of assets derived from proceeds of drug trafficking;
— the prevention and suppression of terrorism, including information on terrorists, terrorist organisations and their *modus operandi* and activities; and
— combating arms smuggling, human trafficking and fraud.

4.2.7. Association of South-East Asian Regional Forum

The ASEAN Regional Forum (ARF) draws together 23 countries with an interest in the region's security, including the 10 members of ASEAN. The ARF's Members include the US, the Russian Federation, Australia, Canada and the EU. It has adopted measures aimed at cutting off funds for terrorism (Australia, 2008).

There are numerous other international agreements of a multilateral and bilateral nature. For a better understanding of the nature of international intelligence cooperation, reference is made to some of these agreements.

5. OTHER INTERNATIONAL AGREEMENTS ON INTELLIGENCE COOPERATION

It is stated that police and intelligence cooperation is the best at bilateral level (Wilkinson, 2006: 165). After 11 September 2001, various intelligence reforms focused on internal intelligence sharing and cooperation. In addition there is a realisation that critical intelligence can be gained by improving bilateral intelligence sharing outside of the US IC (Reveron, 2006: 453).

The following is probably the *crux* of intelligence cooperation in practice: "The best intelligence sources do not necessarily come from the biggest and most highly developed U.S. allies…the most effective, efficient division of effort recognises the strengths of partners better suited — by culture, geography, and experience — to target terrorists in a particular region." (Reveron, 2006: 456). It is significant that after the 11 September events, the US not only strengthened its relations with its traditional allies, Canada, the UK, Australia and other North Atlantic Treaty Organisation (NATO) allies, but also established new alliances and renewed some existing alliances. In the latter category are countries such as Saudi Arabia, Jordan, Pakistan, Yemen and Russia (Reveron, 2006: 463 – 465).

Of interest is 'hopeful dialogue' with 'non-traditional allies', China and 'rogue states', such as Libya, Syria, Iran and Sudan (Reveron, 2006: 466).

Since 11 September, the US has worked with the EU, G-8 and other international organisations to provide 'frontline' countries such as Pakistan, Afghanistan and Indonesia with financial support and training needed to combat terrorism with the concomitant advantage of expanded intelligence sharing (Reveron, 2006: 467). Most information sharing within the EU consists of bilateral or multilateral contacts between Member States. Both in respect of terrorism and other law enforcement fields the national-to-national contacts "make up more of the intelligence flow than is popularly believed" (Herzberger, 2007: 62). Even from a cost-benefit analysis of intelligence services, intelligence sharing on a bilateral basis yields much better results than sharing multilaterally. National intelligence services continue to report better results from national-to-national sharing (Herzberger, 2007: 101).

Extensive cooperation agreements have been concluded, for example between the US and Canada, where a *32-point Action Plan* had been agreed upon for better border control. This plan (point 25) provides for integrated intelligence: "Establish joint teams to analyse and disseminate information and intelligence,

and produce threat and intelligence assessments. Initiate discussions regarding a Canadian presence in the US Foreign Terrorist Tracking Task Force" (Canada, 2007).

It is accepted that many intelligence cooperation agreements and much cooperation on intelligence is not in the public domain. Reference is made to "a patchwork of bilateral and multilateral agreements of all kinds and all degrees of intimacy. The patchwork is unusual in its secrecy…". Significant cooperation between European countries has been kept secret (Villadsen, 2007: 4). There is also a plethora of bilateral agreements between international organisations, for example, between INTERPOL and ASEANAPOL, between INTERPOL and the World Customs Union, between ASEAN and Canada. These loose-standing agreements emphasise the role of international and regional institutions such as Europol and INTERPOL. Some 21 bilateral agreements between governments mention INTERPOL, or give a role to INTERPOL in implementing the agreements (INTERPOL, 2008(a)).

Though more multilateral than bilateral in nature, the cooperation agreement between the UK and the US, in which also Australia and Canada are sharing, is the SIGINT agreement referred to as the UKUSA agreement. The cooperation between the countries involved is said to be so complete that inputs of individual countries into joint intelligence products become indistinguishable (Aldrich, 2004: 737).

There are also many other agreements between international and regional organisations and individual states, which can be regarded as bilateral in nature. Examples of such agreements with INTERPOL have been mentioned. ASEAN – Canada *also made a Joint Declaration for Cooperation to Combat International Terrorism*. The exchange of information on the organisation, activities, and movement of terrorists and counter-terrorism measures is included in the declaration (ASEAN, 2006).

Having analysed the nature of the legal framework and obligations in respect of intelligence cooperation, it is necessary to set out the drivers of or factors positively influencing intelligence cooperation.

6. DRIVERS OF INTELLIGENCE COOPERATION

Formal and informal agreements on intelligence cooperation are therefore valuable tools to overcome mistrust in intelligence cooperation (Walsh, 2006: 630). 'Drivers' of intelligence cooperation refer to the factors that necessitate or stimulate intelligence cooperation. The term 'incentives' to intelligence cooperation could be used in the same sense as 'drivers'. Within the EU, the increased free movement of people has led to reduced national controls on cross-border activities and created a demand for sharing of intelligence about terrorism and other criminal activities. The free circulation of goods, capital and people within the EU also created threats such as opportunities for trafficking of contraband of all kinds; an increase in money-laundering; and terrorist financing stimulated by a common currency. Easy movement across national borders to some extent creates safe havens as a result of different criminal jurisdictions in the respective countries requiring formal processes such as extradition, before prosecution can be instituted (Walsh, 2006: 626).

Global and regional efforts and cooperation against transnational crime and terrorism is a major driver for intelligence and information sharing and other intelligence cooperation (McFarlane, 2005: 304). Intelligence failures such as the 11 September 2001 events and those relating to proliferation of WMD led to commissions of enquiry and shaped the present extensive policies in the US on information and intelligence sharing. On the other hand an intelligence failure where a particular agency is suspected of compromising vital sources could seriously hamper further cooperation (Wilkinson, 2006: 165).

Intelligence successes resulting from cooperation and intelligence sharing promote even more cooperation and intelligence sharing. It is said that it is utility that drives intelligence collaboration (Lander, 2004: 484).

The present global security environment is characterised by common intelligence threats from the proliferation of advanced conventional weapons and WMD, terrorism, drug trafficking, organised crime and economic crime. These threats demand immediate intelligence attention on a continuous basis. Intelligence institutions in various countries including the UK, US and Russia were subject to a decade of reductions in spending, whilst being faced with an increased range of potential military roles and intelligence targets. This has driven most nations to cooperation as a *modus operandi* (Clough, 2004: 611).

Furthermore, the volume of available intelligence is simply too much for a single intelligence agency to handle. Politicians increasingly demand better intelligence to deal with the mentioned threats, whilst intelligence budgets are subject to budget cuts. Improved intelligence cooperation and combining resources is a logic outcome of these circumstances. In regions such as Europe, increased defence cooperation necessitates increased intelligence cooperation (Villadsen, 2007: 11). The demand from the public and the media to effectively combat terrorism is an example of public pressure, though not necessarily focused on increased intelligence cooperation, as society is constantly also demanding more openness and transparency (Herzberger, 2007: 98).

Open sources of intelligence, commercial technologies and the so-called 'privatisation of intelligence' also encourage intelligence cooperation. The advantages of joint databases for rapid electronic dissemination of information may aid states in pursuing cooperation. Joint databases can be continuously updated rather than annually or periodically. This allows equal access to information and enhances analysts' ability to cooperate (Villadsen, 2007, 11,12).

States normally enter into formal and informal forms of intelligence cooperation in order to enhance their intelligence capability. The drivers of intelligence cooperation are further described as internal demands of a public, political or professional nature; external pressure such as a shift in intelligence power affecting a state; and uncertainty, hugely as a result of factors such as globalisation. Globalisation has led to expansion of interests by states into unknown areas (Fagersten, 2007: 16-21). EU Member States such as Poland and Slovenia for example gain valuable intelligence on terrorism from the EU SitCen which they would otherwise only be able to collect through costly and lengthy exercises (Herzberger, 2007: 73).

Policy decisions in many regions and countries implementing intelligence-led policing demands an increase in intelligence cooperation, as such cooperation is crucial in intelligence-led law enforcement (Hertzberger, 2007: 97, 98).

Improved intelligence cooperation on a regional level, such as in the EU, provides real added intelligence value, motivating further sharing and cooperation: “Thus improved European intelligence cooperation would be a positive self-fulfilling prophecy “ (Herzberger, 2007: 97).

After the 11 September events numerous strategies and policies have been adopted in the US, which underline the importance of intelligence cooperation and intelligence and information sharing. In respect of law enforcement and policing the following important policies have been adopted:

— *Intelligence-led policing, the New Intelligence Architechture* (US, 2005(a)).
— *Fusion Centre Guidelines- Developing and Sharing Information in a New Era* (US, 2006(c)).
— *The National Criminal Intelligence Sharing Plan* (US, 2003(a)).

In respect of the broader IC the following policies were adopted in the US:

— *The National Intelligence Strategy of the United States of America* (US, 2005(b)).
— *United States Intelligence Community: Information Sharing Strategy* (US, 2008(a)).
— *Department of Defense Information Sharing Strategy* (US, 2007(b)).

7. CONCLUSION

The new focus of and reason for existence of intelligence services in the post-Cold War era, is described with reference to new international threats of a transnational nature. The common threat of international terrorism after the 11 September 2001 events provided a renewed focus on intelligence sharing and intelligence cooperation. International obligations for intelligence cooperation in respect of international crime have been described on international and regional level in this chapter. There is a growing tendency on the international as well as the regional level to require intelligence cooperation in respect of intelligence and information sharing as well as on operational level by cooperating in the execution of undercover operations and electronic surveillance of communications. This is true in respect of all international crimes dealt with in this study. Mechanisms have been established such as in the UN Security Council to promote and ensure intelligence and operational and other cooperation in combating terrorism in particular.

Closer cooperation is clearly manifesting on regional level, whether within the EU, the African, Southern African, or ASEAN regions. It is important to note that in all cases there are at least on policing level, close links between the respective regions and INTERPOL, strengthened by formal cooperation agreements. INTERPOL is furthermore linked with individual countries and law enforcement agencies from Member States have easy access to the databases of INTERPOL. In respect of crime intelligence cooperation, INTERPOL is the one common link that completes the intelligence mechanism on the global level, with linkages to

the UN, customs and other organisations. In this regard it is notable that the INTERPOL arrangement is based on a Constitution, which, from an International Law point of view, is less enforceable, as it is dependant on voluntary cooperation rather than enforceable obligations. This factor, however, makes INTERPOL flexible and adaptable.

Although international obligations and efforts to promote international intelligence cooperation is an important factor for such cooperation, it is submitted that other factors, such as the needs of individual countries; shared crime threats such as terrorism; piracy and organised crime; economic factors; and the sheer advantages (utility) of cooperation are even more important drivers of intelligence cooperation. The volume of intelligence, cost of technology and inadequate HUMINT capabilities are drivers of intelligence cooperation on a *quid pro quo* basis: training and assistance in exchange for intelligence sharing or use of territory for surveillance purposes. The most cost-effective and closest intelligence cooperation is on bilateral basis between states.

Despite international obligations sometimes enforced through structures such as those of the UN Security Council, international instruments, resolutions of international organisations and multilateral and bilateral agreements, there is clearly scope for improvement of intelligence cooperation on the international level and this cooperation remains a challenge. Global intelligence cooperation remains not only a challenge, but an ideal which seems to be very far in the future or perhaps impossible. In the next chapter the factors which inhibit, complicate or sometimes even preclude intelligence cooperation, are discussed.

CHAPTER 4
CHALLENGES FOR COOPERATION: CIVILIAN INTELLIGENCE AND LAW ENFORCEMENT

1. INTRODUCTION

In view of the imperatives for intelligence cooperation on all levels, the question arises what the challenges are for intelligence cooperation, or which factors inhibit or in some instances prevent intelligence cooperation. Intelligence cooperation as a concept is described as 'somewhat oximoronic', because intelligence activities are so closely related to national security and sovereignty. Fagersten is of the view that: "Lack of trust, the need for secrecy, cultural conflicts and divergent interests are thought to render intelligence cooperation complicated on bilateral level and nearly impossible to achieve on multinational level." (Fagersten, 2007: 3).

The challenges for cooperation between law enforcement and civilian intelligence are identified and discussed in this chapter. The main challenges which have been identified are sovereignty; jurisdiction; lack of standards for communication and information technology; technical advances; secrecy and fear of compromise; mistrust; the difference in focus and structure between law enforcement and positive intelligence; states which have no effective government; corruption in governments; and the rise of private intelligence and private security. The test for the degree of actual intelligence cooperation can be found in the following: (Fagersten, 2007: 3)

— The 'scope' of intelligence cooperation, in other words whether cooperation extends to functions such as tasking, collection, analysis and dissemination performed by joint structures; and
— the 'depth' of intelligence cooperation, in other words, how much cooperation is executed jointly within those functions and not only sharing of what was performed separately.

The different oversight mechanisms for law enforcement and positive (military and civilian) intelligence will also be described. The first challenge to intelligence cooperation is sovereignty.

2. SOVEREIGNTY

Sovereignty affects intelligence cooperation in a number of ways, ranging from the inability of some states to control or to exercise power in terms of law enforcement to the relationship between international organisations and states as members of such organisations, and the effect of the own national interest of each state which usually supersedes other interests. It is therefore important to understand the meaning or meanings of the term and to analyse the manner in which it affects such cooperation.

2.1. Meaning of the term 'sovereignty'

Sovereignty is one of the most important factors which negatively affect intelligence cooperation on the international level. The term 'sovereignty' has a changing character in international law and may hold different meanings, for example, for Jurisprudence and Political Science. At least 13 different overlapping meanings of sovereignty are described, amongst others: (Nagan & Hammer 2004: 2, 3)

— Sovereignty as a personalised monarch;
— sovereignty as a symbol of absolute, unlimited control or power; and

— sovereignty as a symbol of political legitimacy or of political authority or jurisdictional competence to make and/or apply law or as a symbol of basic governance competencies.

Political authority is reflected in law- from a basic law or constitution to other laws. Following religious strife in Europe, the *Treaty of Westphalia* (1648) laid the juridical foundations of sovereign independence for the European nation-state (Nagan & Hammer, 2004: 9). The diverse basic conceptions about sovereignty might, if not clearly understood, "generate conflict with tragic and far-reaching consequences to world order" (Nagan & Hammer, 2004: 11). Traditionally national sovereignty entails a rejection of any form of centralised international authority, which accounts for some resistance against international intelligence cooperation. The different contexts in which the word can be used are further described as follows: (Fagersten, 2007: 12)

— 'International legal sovereignty' refers to aspects of international recognition;
— 'Westphalian sovereignty' is the principle of non-interference in the domestic affairs of a state, in other words, it "excludes external actors from a specific territory's internal authority structures";
— 'domestic authority' reflects the structural formation of authority in a state and the ability to exercise effective control over the state; and
— 'interdependence sovereignty' that relates to the power to regulate the flow of information, people, goods and capital within and across the borders of the state involved.

When states bind themselves by contract or convention to reduce their sovereignty by allowing an external authority (another state) to possibly influence their policy through intelligence provided to them, it may lead to an enhancement of another form of sovereignty, such as interdependence sovereignty to improve policing for example, or at least gain in terms of intelligence capacity (Fagersten, 2007: 13). In order to properly analyse

sovereignty within the context of intelligence cooperation, it is necessary to define the concept 'state'.

2.2. The meaning of 'state', and effect of 'failed states' and 'dysfunctional states' on intelligence cooperation

In terms of the *Montevideo Convention on the Rights and Duties of States (1933)* a state, as person in international law, should possess a permanent population, a defined territory, a government and the capacity to enter into relationships with other governments. (Organisation of American States, 1933: Article 1).

An important pre-condition for the existence of a state is that of control and specifically how authority is constituted. Membership of states of regional and international organisations such as the AU and the UN may lead to these states relinquishing some autonomy in exchange for benefits of membership (Nagan & Hammer, 2004: 18). A state's sovereign character may change as a result of a practical distribution of power to become, for example, a failed state. Sovereignty may also be abused, which after the Second World War led to the doctrine that the leaders of aggressor states could be accountable directly to the international community for criminal conduct (Nagan & Hammer, 2004: 27). The *Rome Statute of the International Criminal Court* secures sovereignty, especially of smaller sovereign states by providing for criminal responsibility (outlawing) of individuals for crimes that threaten the peace, security and well-being of the world and acts of aggression that target the territorial integrity and political independence of the sovereign state (Nagan & Hammer, 2004: 32).

The US national security doctrine developed after the 11 September 2001 events challenges sovereignty, self-defence, the use of force and the issue of intervention. The most controversial elements of this doctrine were the claims to pre-emptive intervention, the idea of the illegitimacy of so-called 'rogue states', as well as the doctrine of 'regime change'. The new security doctrine is based on the

notion that conventional strategies of deterrence are of little value in case of an enemy which is a non-state actor protected by rogue foreign states, and able to deploy WMD and mass murder (Nagan & Hammer, 2004: 35). The security doctrine of the US after 11 September 2001 is recognition of the abuse of the sovereignty concept by 'rogue' or 'failed states' (Nagan & Hammer, 2004: 36). Numerous factors can be taken into account in order to determine whether a state is a failed state and even to rank such states according to the degree of failure thereof. Such factors are demographic pressures; refugees and displaced persons; group grievance; human flight; uneven development; economy; delegitimisation of a state; public service; human rights; security apparatus; factionalised elites; and external intervention (Foreign Policy, 2008).

The issue of failed or dysfunctional states has a profound effect on intelligence cooperation on the international level in respect of the international crimes which are the subject of this study. This is most notable recently in respect of terrorism and piracy. Wherever a state becomes dysfunctional, it provides a safe haven for criminals who take advantage of the situation and who, through corruption and fear in many instances become a *de facto* power in a failed or dysfunctional state. This can take many forms: clear support of the criminals (such as with terrorism); turning a blind eye (as with narcotics trafficking); a corrupt relationship through which both government officials and the criminals benefit; or a total lawless society where the strongest rule by force. In respect of war crimes, the disruption caused by the conflict and military rule makes intelligence cooperation to investigate war crimes during an ongoing conflict extremely difficult.

Somalia is regarded as a text-book example of a failed state. It has been without any government (and thus could not have been regarded as a state for the period 1991 to 2000) (Kreijen, 2004: 331). During 2008 the International Maritime Bureau reported 92 ships attacked and 36 hijacked off the coast of Somalia and Yemen. Although there is a Transitional Federal Government in Somalia, which has requested the international community to assist with the combating of piracy

along the Somali coastline, the UN Security Council noted concern about the lack of capacity, the lack of domestic legislation and clarity on how to dispose of pirates after they have been captured, as hindering more robust international action against pirates in that region (UN, 2008(a): 2). The UN Security Council approved the necessary action on land and in the air to combat piracy in the area. The UN Security Council also called on countries to create a centre in the region to coordinate information relevant to piracy and armed robbery at sea off the coast of Somalia, *inter alia* to investigate and prosecute piracy in the region (UN, 2008(a): 3).

Al-Qaida, the Taliban and Lashkar-Al Taiba have established themselves as 'states' within states and are alleged to have a free reign in the Federally Administered Tribal Regions of Pakistan (Boot, 2008). Effective action by the Pakistani security forces has been lacking and it is alleged that the *Jihadist* groups have long-standing relationships with the Pakistani Inter-Services Intelligence Agency (Boot: 2008). This state of affairs led to some 40 US unmanned aerial vehicle (UAV) attacks performed by the CIA in about one year's time against Al-Qaida targets in Pakistan, without prior notice to the Pakistani authorities. Pakistan has been forced to an extent by the US after the 11 September events to cooperate with the US in the war against terror (US, 2004(b): 331). Pakistan is, however, unable to exercise sovereignty over West Pakistan which has become a safe haven for Al-Qaida terrorists. During his election campaign, the now US president Obama repeatedly stated that : "if the United States had credible information about hideouts of al-Qaeda fighters in the mountains of north-west Pakistan, and if it became clear that the Pakistanis were doing nothing against these fighters, then he, as president, would order air strikes, and more, to destroy these hideouts" (HSDailyWire.com, 2009).

A further such attack was indeed performed after Obama became president. Such attacks, when performed unilaterally have a negative effect in terms of respect for the sovereignty of Pakistan and may eventually be damaging to

intelligence and other cooperation between the US and Pakistan. States that are dysfunctional or benefit in one way or the other from lawlessness undermine effective international, regional and national intelligence cooperation. This category includes states where official corruption assists the internationalisation of organised crime and drug trafficking, and countries that exercise a *laissez-faire* policy with respect to law enforcement and financial regulation that attracts criminals and terrorists. These countries are referred to as 'spoilers' (Johnston, 1998: 4). In the *Report of the National Commission on Terrorist Attacks upon the United States,* the observation is made in respect of Afghanistan under the Taliban, that it was not a case of a state sponsoring terrorists, but a state sponsored by terrorists (US, 2004(b): 183).

Nagan and Hammer suggests some typologies of different states in the international system that implicate the abuse of the sovereignty idea, namely failed states; anarchic states; genocidal states; homicidal states; rogue states; drug influenced states; organised crime-influenced states; authoritarian states; garrison or national security states; and totalitarian states (2004: 36-39). In respect of drugs, narco-terrorism is of particular importance. The term is ambiguous as it refers to both the type of campaigns that drug traffickers, cartels such as Pablo Escobar in Colombia, and the mafia, use against anti-narcotics police; as well as the participation by terrorist groups in taxing, providing security for or otherwise aiding and abetting drug trafficking in an effort to further or fund terrorist activities. The campaigns that drug traffickers sometimes resort to include terrorist methods such as the use of car bombs, assassinations and kidnappings. (Björnehed, 2004: 306). A challenge for intelligence cooperation is the tendency to view the narcotics trade separately from terrorism. It is clear that there is cooperation in many instances between terrorism and drug traffickers. An example is in Afghanistan where heroin production blossomed even after the military action against the country in 2001 (Björnehed, 2004: 309).

Another effect of organised crime on states is corruption. Corruption is regarded as possibly the most substantial obstruction to transnational law enforcement and intelligence cooperation. This is a problem often experienced in what is called emerging markets. Examples in this regard are unsuccessful counter-narcotics efforts between the US and Mexican authorities undermined by high-profile corruption scandals on the Mexican side: Mexican government, police and military units struggle with corruption and links to drug cartels and immigrant smugglers. There are real fears that intelligence and information sharing may end up in the hands of organised criminal syndicates (Sunnucks, 2006). It is alleged that Mexican towns and cities along the US border are often rife with corruption and dominated by organised crime and violent drug cartels (Sunnucks, 2006). Another example of the negative effects of corruption is the unsuccessful US action against organised crime and nuclear smuggling undermined by corruption within the Russian Ministry of the Interior and Federal Security Service (Johnston, 1998: 2). Mere perceptions of corruption may lead to intelligence not being shared when intelligence institutions would rather err on the side of caution (Ryan, 2006: 208).

Smaller countries are suspicious of closer cooperation with powerful countries such as the US, for fear of being ‘junior partners’. This is more acute where investigations are to take place in the country of the ‘junior partner’. Being former adversaries such as Russia and the US, or countries known for their national pride towards what they regarded as US imperialism, also complicate intelligence cooperation. There is a fear that US capabilities, sources of intelligence and intelligence collection methods may be compromised to partners. Closely related to the principle of sovereignty is national interest, which usually will override many other considerations. Cooperation and wide-ranging sharing of intelligence may lead to a reduction in sovereignty (Johnston, 1998: 3). Close intelligence relationships disclose the respective parties to each others failings and weaknesses (Clough, 2004: 605, 606).

States display huge resistance to multilateral pooling of intelligence, especially very sensitive data for security concerns and wider concerns about sovereignty (Aldrich, 2004: 737). Some states experience constitutional problems to share intelligence, for example, Germany (Aldrich, 2004: 741). The emphasis of sovereignty over sharing of intelligence is regarded as a hampering factor in European intelligence cooperation. Intelligence sharing is to a large extent based on imagery collection and analysis, using the Western Europe Satellite Centre, based on commercial technology which limits the need to share highly classified information (Villadsen, 2007: 10). Closely related to sovereignty is the issue of dependence. France, for example, is not in favour of Western Europe being dependent on the US in respect of intelligence (Villadsen, 2007: 10). Intelligence lies at the core of national sovereignty. EU Member States are hesitant to provide 'hot' intelligence to *inter alia* Europol, and it is stated that the lack of political will to share information is "one of the largest problems facing intelligence cooperation in Europe" (Herzberger, 2007: 101).

There is a close relationship between the degree of cooperation and the degree to which the loss of sovereignty is outweighed by the gain in intelligence capacity or policy gains. Increased intelligence cooperation occurs usually in cases where the benefits of such cooperation are either extremely high or where the costs and risks are low (Fagersten, 2007: 14).

2.3. The effect of sovereignty within the context of international organisations

The issue of sovereignty in relation to intelligence is most acute on international levels of intelligence cooperation such as within the UN and the AU. Traditionally international organisations were reluctant to become engaged in intelligence activities as such, as they are dependent on intelligence received from Member States and engaging in activities that could be viewed as espionage on Member States were regarded as intruding on the sovereignty of Member States

(Champagne, 2006: 6). The roles of international organisations are increasing with a concomitant increase in responsibilities, which established a need for 'independent intelligence'. As a result, this negative view is slowly changing (Champagne, 2006: 6). Various 'complex' emergencies globally, and the deployment of peacekeeping and peace enforcement forces, involved in classical military operations with the same intelligence needs to ensure effective operations as well as the safety of not only the peacekeeping forces, but the populace at large, resulted in a recognition of the need for intelligence in such operations (Cline, 2002: 179). As has been pointed out in Chapter 3, within SADC and now also on the AU level, there is some confusion between early warning and warning intelligence and warning intelligence seems to be included in the concept of 'early warning' (Hough: 2004: 27).

Whilst the UN shied away from the use of the term 'intelligence', the Military Adviser to the UN Secretary General recently reported that the word 'intelligence' has finally become acceptable in the UN system (Cline, 2002: 179) (Fagersten, 2007: 3). A Situation Centre had been established in 1993, as part of the UN Secretariat's Information Management System to support the decision-making process and connecting civilian, military and police flows of information at the strategic level. The UN recognises the elements of peacekeeping missions to include political, humanitarian, human rights, electoral issues, the involvement of numerous role-players and the 'need for a consolidated flow of information'. The functions of the UN Situation Centre consequently includes communications functions with peacekeeping field missions; monitoring of events in order to determine potential threats to UN personnel in peacekeeping operations; information gathering and reporting, including open source intelligence and 'information from the field'; threat assessments ensuring the security of personnel in the field; and crisis management (UN, 2005(c):1, 2). International structures for intelligence sharing are poorly equipped and not transparent. These structures are complex and bureaucratic (Herzberger, 2007: 8). Nevertheless the opinion is held that the focus should not be on building elaborate new structures, but to

speed up means of practical exchange on operational matters (Aldrich, 2004: 733). The extraterritorial exercising of power also has an effect on intelligence cooperation.

2.4. The effect of extraterritorial exercising of power on intelligence cooperation

In terms of the principle of sovereignty states provide for powers of their law enforcement and intelligence agencies within their own national territories, but also outside such territories. Normally law enforcement agencies do not have executive powers within the territory of other states, other than within the legal framework provided for by the other state. The exercising of extraterritorial powers by one state may not only may be illegal in another state, but may also cause a loss of trust where intelligence cooperation or intelligence sharing lead to extraterritorial actions which are controversial and sometimes regarded as unethical or inconsonant with international law, relating for example to torture. The US, for example, provides in terms of national legislation for extremely wide powers for its intelligence, law enforcement and military forces, and foreign agents (which could include intelligence, law enforcement and military personnel) to act extraterritorially, whilst the country has criminalised any unauthorised actions by 'foreign agents' in the US. Any individual who agrees to operate within the US subject to the direction and control of a foreign government, except diplomatic personnel, is regarded as a 'foreign agent'. Acting unauthorised in the US as a foreign agent is a criminal offence for which imprisonment of up to 10 years may be imposed (US, 2002(a): Section 951).

Embarrassing situations which have developed as a result of intelligence cooperation in respect of clandestine operations have led to conscious decisions by intelligence and law enforcement agencies not to participate in such operations or to cooperate only within clearly defined circumstances. The practice of the US to perform so-called 'renditions' is an example of such actions.

'Rendition', which could include any extra-judicial transfer of persons from one jurisdiction or country to another, can be further categorised according to the nature and purpose of such rendition: (UK, 2007(a): 6)

— 'Rendition to justice'- where the rendition is performed to enable the trial of a person in a court of law ("within an established and recognised legal and judicial system");
— 'Military Rendition'- in instances where the rendition is performed for "the purposes of military detention in a military facility";
— 'Rendition to detention'- rendition for purposes of "detention and interrogation outside the normal legal system"; and
— 'Extraordinary rendition' – rendition for the purposes of detention and interrogation outside the normal legal system, where "a real risk of torture or cruel, inhuman or degrading treatment" exists.

A further complicating factor is where there is a request to perform a rendition, where the death penalty is unconstitutional in the requested state and such cooperation may lead to the death penalty being imposed in the country to which the person is removed (UK, 2007(a): 13). The US policy is to "identify terrorists and those who support them and to eliminate their ability to conduct or support [terrorist] attacks [and for suspects] to be detained and when tried, tried… by military tribunals" (UK, 2007(a): 19).

This policy, backed by a *Presidential Military Order* applies to non-US citizens who are members of Al-Qaida, have knowingly harboured such member, or have engaged in, conspired or aided to commit international terrorism prejudicial to the interests of the US (UK, 2007(a): 20). The US Government publicly acknowledged the existence of the rendition programme and secret CIA-run overseas detention facilities (referred to in the media as 'black facilities) (UK, 2007(a): 26, 27). Upon enquiries from the President of the EU, the US Secretary of State issued a statement on 5 December 2005, in which the US Government gave assurances that the US will comply with its treaty obligations, including

those under the *Convention against Torture*; that it will continue to respect the sovereignty of other countries; that it does not transport detainees from one country to another for purposes of interrogation using torture; and that the US does not use the airspace or the airports of any country for purposes of transporting a detainee to a country where he or she will be tortured (UK, 2007(a): 28). As a result of the practice of rendition, the UK authorities placed conditions on the use of intelligence provided to 'liaison partners', to ensure that other agencies do not endanger the UK agency's sources through the incautious use of intelligence (UK, 2007(a): 53). The safeguards developed for the Secret Intelligence Service and the Security Service in the UK can be viewed as best practices, namely: (UK, 2007(a): 53)

— Not to condone the use of torture or mistreatment;
— To use caveats and assurances in case torture or mistreatment is foreseen. A caveat could be that no arrest will be effected or other action taken on the basis of the intelligence involved, or that the intelligence will not be forwarded to another country or agency. A typical assurance would be that the person would not be tortured or mistreated.
— When such caveats and assurances are not enough to minimise the risk, senior management or ministerial approval must be obtained.

In terms of legality, rendition would only be lawful if it complies with the domestic law of both countries involved as well as with the international obligations of both countries. There are instances where intelligence agencies use sovereignty to advance intelligence cooperation.

2.5. Use of sovereignty to advance intelligence cooperation

Sovereignty is discussed above within the context of a factor inhibiting international intelligence cooperation. Sovereignty can also be used to the advantage of intelligence collection through international intelligence cooperation. In this respect the Menwith Hill station in the UK is an example. This facility is

jointly operated by the National Security Agency (NSA) of the US and the UK's Government Communications Head Quarters (GCHQ). It is described as the principal NATO theatre ground segment node for high altitude signals intelligence satellites, and capable of carrying two million intercepts per hour. The activities have shifted from monitoring cable and microwave communications passing through the UK to the sifting of international messages, telegrams and telephone calls of citizens, corporations or governments to select information of political, military or economic value. It also monitors high frequency (HF) radio transmissions, including military, civilian embassy, maritime and air radio communications. (Pike, 2003(b): 1, 2). Being operated outside the US territory this site has obvious advantages in respect of freedom of operations outside the legal restraints of the US legal system. The UK IC shares the intelligence, which is collected through the joint collection process. Although such extraterritorial operations may have legal implications also for US citizens, the locality outside the US reduces prospects for intelligence oversight, especially on the US side. This is so because the intelligence product becomes grey as regard to the origin thereof, in terms of jurisdiction. The next challenge to intelligence cooperation is interagency rivalry.

3. NATIONAL INTERAGENCY RIVALRY/ORGANISATIONAL CULTURE CHALLENGES

Whilst sovereignty is one of the main challenges to international intelligence cooperation, interagency rivalry is one of the main factors inhibiting intelligence cooperation on national level. International intelligence cooperation is dependant on the level of interagency cooperation on national level in the participating countries. This calls for organisational differences within national security, intelligence and law enforcement agencies in each country to be resolved. In many instances there are long-standing rivalries and conflicting organisational objectives and operational doctrines that must be resolved. One example in this

regard is the conflicting standard of evidence between the CIA and the Federal Bureau of Investigation (FBI). The FBI uses the court standard of evidence 'beyond reasonable doubt', while the intelligence standard is described as 'far more nebulous'. This problem was solved with the investigation of the embassy bombing investigations in Kenya and Tanzania by the establishment of a Counter-Terrorism Centre that provided a forum for resolving disputes (Johnston, 1998: 3).

An example of the problem caused by organisational culture is the approach the US NSA followed before the 11 September events: Although it was possible to identify some of the hijackers before the event with information that was actually available on the databases of the NSA, the NSA did not think it was its job to research those identities. It saw itself as an agency that supports other intelligence agencies and functioned on a request basis. If the identities of these persons were known they could have been tracked successfully (US, 2004(b): 353). There was also basically no sharing of intelligence between the FBI and the National Security Council (NSC) and the rest of the security community (US, 2004(b): 358). There was also a perception that the FBI itself could not share any intelligence received from civilian intelligence with criminal investigators of the FBI. This led to valuable information of NSA and the CIA not reaching criminal investigators (US, 2004(b): 79).

One of the most glaring failures resulting from interagency rivalry was the effect of actions of the Canadian Secret Intelligence Service (CSIS) on the investigation by the Royal Canadian Mountain Police (RCMP) of the Air India Flight 182 bombing, attributed to Sikh terrorists. During the first phase of the investigation, CSIS members, in a bid to protect their informers, destroyed audiotapes and in the process denied crucial evidence to the RCMP. Reference is made to an 'enduring conflict" between the CSIS and the RCMP which allegedly resulted in the case remaining unsolved. The events resulted into the *Commission of Inquiry into the Bombing of Air India Flight 182* which was aimed at determining ways to

address the challenge to establish "a reliable and workable relationship between security intelligence and evidence that could be used in a criminal trial" (Brodeur, 2007: 30).

4. TECHNICAL ADVANCES AND GLOBALISATION

Transnational organised crime groups and terrorists have to a large degree exploited advances in electronic banking, encryption, and telecommunications technology. This poses two problems for law enforcers. Government agencies with their bureaucracies are much slower than the small flexible criminal groups or terrorists to incorporate new technologies in their systems. There is also no consensus in government on sharing of technology such as encryption, without which intelligence and law enforcement cannot function properly (Johnston, 1998: 3). Globalisation has created, instead of a 'global village' a 'mega-metropolis' in which there is vast anonymity and diminished privacy. It is not necessary to use intrusive technology to establish why a person is at a specific place at a specific time. Judicious use of information technology with sensible intelligence cooperation may protect society (Aldrich, 2004: 736).

In multinational operations, such as peace missions, technical problems include complicated lines of communications; lack of a common language; lack of interpreters; mistrust towards interpreters; different levels of training and competencies of officers seconded from the various countries; and the numbers of officers seconded from the different countries. In order to fuse the intelligence contributions from different nations in a multinational operation a multinational intelligence centre needs to develop a "standardised methodology for disseminating and exchange of information" (Cline, 2002: 186, 187).

In respect of multilateral cooperation such as in regional and international organisations for intelligence cooperation the combining and sharing of databases is an important element. Every intelligence agency, however, has a

different way of indexing of information. This causes problems with interoperability. Within regions such as the EU, communications systems between institutions such as the Council of Europe, the Commission and Europol are not connected (Herzberger, 2007: 108). In order to ensure interoperability or the connection of databases the following is needed: "compatible information exchange systems protected against unlawful access…common standards for information storage, analysis and exchange between the different services" (Herzberger, 2007: 109). Such standardisation may even relate to issues such as the way in which Arabic (or other language) names are spelt. At international level classification codes which differ from national codes may be used, such as Restricted, Confidential, Secret and Cosmic Top Secret (Herzberger, 2007: 110). Incompatible data systems were a key factor which led to intelligence problems preceding the 11 September 2001 events (Aldrich, 2004: 741). The next factor, which affects intelligence cooperation, and perhaps the most important is trust/mistrust.

5. MISTRUST

Trust is the most essential prerequisite for intelligence cooperation, whether on national, regional or international level. Similar interests and a desire to reach the same outcomes are factors which enhance the exchange of intelligence and other intelligence cooperation between governments (Walsh, 2006: 628). Mistrust is regarded as the key barrier to fully effective intelligence sharing in the EU (Walsh, 2006: 625, 638). Factors which instil trust for the sharing of intelligence are when the receiver state and the sending state both know that they share the same policies; that they desire the same outcomes from the intelligence sharing; and where they have confidence in the accuracy of the shared intelligence (Walsh, 2006: 628). There is always the possibility of the sending state deliberately altering shared intelligence to influence the receiving state's policy choices in a direction that would suit the sending state, in circumstances where it may be impossible for the receiving state to verify the intelligence. Similarly the

sender may provide outright untruths; good and verified intelligence may be withheld to influence policy decisions; or intelligence may be exaggerated (Walsh, 2006: 628). The greatest risk to intelligence cooperation is the increased threat of espionage and counterespionage (Clough, 2004: 606).

The receiver of intelligence may deliberately or inadvertently share intelligence with a third party. Security services are very reluctant to share operational information and such sharing is indicative of a high level of trust (Walsh, 2006: 634). Intelligence is mostly shared with trusted friends and colleagues. It takes years to build such trusted relationships. Informal channels for information sharing are important, even within a particular institution (Herzberger, 2007: 8).

Intelligence agencies are reluctant to disclose the full details of their sources or methods employed to gather intelligence. This is also true in respect of different agencies of the same government (Walsh, 2006: 629). In addition to protection of sources, different states have different notions of privacy and resist large-scale-data-sharing. It must be accepted that high-grade intelligence will continue to be shared on a selective and bilateral basis. The need remains to share routine background intelligence at a faster rate and to acquire a better joint understanding about the relationship between privacy and security (Aldrich, 2004: 732). Intelligence exchanged between states may be used by the receiving state for a purpose which was not intended by the state which provided the intelligence, and without being informed or requested that it be used for that purpose. An example is where Israel used US satellite imagery to perform a strike against the Iraqi Osirak nuclear reactor in 1981. This was damaging to US Israeli relations, in terms of trust (Fagersten, 2007: 13). The protection of the sources and methods of intelligence gathering and the extent of the capabilities of intelligence institutions are the most treasured assets. Mistrust often emanates from fear of compromising these through intelligence cooperation (Walsh, 2006: 629). Intelligence cooperation between three parties may lead to circular reporting, especially where the respective parties are not aware of cooperation

agreements between other participants. Information shared by one party may reach a third party, and again be shared with the country where the intelligence originated, which country could erroneously interpret it as confirmation of the information. The bigger the number of participants, the bigger the risk is for circular reporting (Clough, 2004: 606).

One way of overcoming mistrust, but with increased risk to sources or collection methods, is to allow receiving parties access to the 'raw intelligence' in addition to the analysed intelligence product (Walsh, 2006: 630). Economism, namely the focus by the industrialised world and the emerging market nations on economic issues, forced transnational law enforcement and intelligence issues off the international agenda at fora such as the G-8 (Johnston, 1998: 2). In multi-national peace operations, the problem of trust is notable in the practice of marking intelligence products as 'not releasable to foreign nationals' and a consequent 'sanitising' of the product, by removing from the product the sources and the methods of collection. In many instances the usefulness of the intelligence relies on it being shared or made available to the actors who need it in the field. The sanitisation process causes time delays which could be problematic and lead to acting too late or the opportunity to act may pass (Cline, 2002: 189).

The difference (in respect of mandate; means of operation; culture and focus), between law enforcement and positive intelligence is often referred to as a gap. The effect of this gap on intelligence cooperation therefore needs to be analysed.

6. DIFFERENCE BETWEEN LAW ENFORCEMENT AND CIVILIAN INTELLIGENCE

In the following sections the effect of the organisational differences of 'culture', and the differences between the mandate, tasks, role, focus and functions of crime intelligence and positive intelligence are analysed to make proposals on

how the gap between the two could be bridged for the sake of promoting intelligence cooperation.

6.1. Effect of organisational differences on intelligence cooperation

The bureaucratic nature of the intelligence process in government and how members of the IC interact with each other can create serious barriers to interagency communication (Boardman, 2006: 6). In most countries the IC consists of numerous agencies. In the US it consists of 16 major organisations ranging from the CIA to the FBI, the different military intelligence agencies, Homeland Security and Treasury intelligence offices (Boardman, 2006: 8). The strict separation between intelligence and law enforcement are intended to prevent intelligence services from overstepping their bounds, but this factor in the US inhibited cooperation in investigating terrorism (Boardman, 2006: 12).

The difference between the respective intelligence functions/services is sometimes referred to as ‘organisational culture’, with reference to core values, cultural form, such as even the jargon used in a particular agency and formal management structures and policies (Boardman, 2006: 13 - 15). The different organisational cultures amongst intelligence agencies may lead to distortion or withholding of information; turf battles; agencies taking credit for successes derived from intelligence received from another agency without recognition given; and competition as a result of fragmentation. Through competitive intelligence gathering intelligence agencies effectively undermine each other for purposes such as justifying a higher budget allocation (Boardman, 2006: 16 - 18). The non-sharing of intelligence may lead to mistrust and refusal of future cooperation. Some agencies “…are accused of an obsession with secrecy and with some degree of its own internal agency version of political correctness, sometimes to the point of stupidity” (Boardman, 2006, 22). The classification and in particular over-classification by agencies is a factor that may severally hamper the sharing of intelligence (Boardman, 2006: 44). Organisational cultural differences can be

overcome through steps such as the creation of a culture of communication and sharing of intelligence and the adoption of a 'common systems architecture' (Boardman, 2006, 2006: 60).

6.2. Effect of the different tasks and focus of civilian and law enforcement intelligence on intelligence cooperation

Traditionally law enforcement and civilian intelligence services have different tasks- intelligence services to identify from information gathered, threats to the democratic order, whilst law enforcement must gather information on crime for submission to courts of law as crime intelligence. Such crime intelligence, submitted as evidence will be tested in court. Civilian intelligence services are traditionally not tasked with the investigation of crime, and intelligence gathered by them is not subject to such public scrutiny. There is also a difference in the manner in which law enforcement and civilian intelligence services perform their respective functions (Vervaele, 2005: 3, 4). The purpose of 'security intelligence' is to prevent violence before it can be carried out, by various means of which recourse to the courts is just an option, in many instances the last resort (De Koster, 2005: 39). "Security intelligence' refers mostly to crime intelligence, but in the latter reference is used to refer to civilian intelligence which is primarily charged with the security of countries. After the Madrid attacks, the Council of Europe invited Member States of the EU to promote efficient and systematic cooperation between the police and civilian intelligence services. In view of the ever-present risk of confidential information being disclosed in court proceedings, and the consequent reluctance of security (civilian) intelligence services to share intelligence with police, it was pointed out that "the interlinking of networks will not be achieved without difficulty, if it is ever achieved at all" (De Koster, 2005: 39).

Brodeur distinguishes between security 'high policing' intelligence and criminal 'low policing' intelligence. High policing intelligence agencies, according to Brodeur include civilian intelligence agencies such as the CIA as well as

domestic law enforcement agencies such as the FBI, which both deals with intelligence relating to the security of a nation, regarded as on a higher level than what Brodeur refers to as 'lamp post policing', in other words common crimes. The normal law enforcement response is aimed at bringing criminal cases before court, whilst security intelligence agencies, meaning civilian intelligence, see recourse to the courts only as an alternative and sometimes the last alternative (Brodeur, 2007:27). There is a marked difference between intelligence and evidence. Police often through unrelated cases disrupt criminal activities permanently or temporarily. Civilian intelligence services on the other hand, have a culture of circumvention. An example of circumvention is where a criminal group was infiltrated by scores of informants who directed the organisation in such a manner that it no longer posed a threat (Brodeur, 2007: 30).

Secret services (civilian intelligence agencies) are primarily focused on prevention and counteraction. Shared information in that regard will probably not land in the public domain. On the other hand, police intelligence, telecom data and passenger records, present problems when placed in the public domain, as would most probably happen with law enforcement investigations ending in court proceedings (Aldrich, 2004: 734). Law enforcement intelligence often seems insignificant in comparison to the intelligence collected by secret services. It is, however, of importance that the dutiful collection of information such as names and addresses sometimes lead to successes. In Italy the decision to enforce regulations obligating landlords to inform the authorities of the names of their tenants turned up many sought-after terrorists (Aldrich, 2004: 742). The transfer of police data is described as a 'legal minefield' as a result of different structures of protection accorded to personal information in respectively the US and Europe, with strict data protection laws in the latter.

In the US the gap between civilian intelligence and law enforcement (crime intelligence) before 11 September 2001, represented the cardinal principle of what is referred to as the intelligence ethos (Turner, 2005: 389). The divide

between information gathered for law enforcement and civilian intelligence has been described as a 'firewall' (Gill, 2004: 472). The wall between law enforcement and civilian intelligence was aimed at the protection of civil liberties and American democracy. This divide, however, led to an entrenchment of intelligence agencies to "engage in the bureaucratic politics of interagency competition for turf, money, people and access to policymakers". The intelligence failures of the 11 September 2001 events demanded reforms in this regard (Turner, 2005: 388). Since 1970 there has already been increased intelligence cooperation between military, intelligence and law enforcement agencies targeting organised crime. The increased use of tactics of disruption instead of arrest and prosecution already weakened the divide described above between law enforcement and civilian intelligence (Gill, 2004: 472). After 11 September 2001 with increased demand for intelligence cooperation, the *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001*, generally referred to as the *PATRIOT* Act, granted increased powers permitting prosecutors to use information obtained through the *Foreign Intelligence Surveillance Act (FISA)* authorised interceptions in the prosecution for terrorist offences. The special appellate panel of the Foreign Intelligence Court of Review upheld the provisions of the *PATRIOT* Act in respect of such use of the *FISA* intercepts (Gill, 2004: 472). Sometimes intelligence cooperation between intelligence agencies and law enforcement is absent simply as a result of working methodology. For example: law enforcement agencies accumulated a great deal of information about Al-Qaida and other terrorist groups during the 1990's, which were kept in law enforcement evidence rooms, and unknown or inaccessible to counterterrorism analysts within the IC (US, 2003(c): 18).

6.3. Bridging the gap between civilian intelligence and law enforcement intelligence

Following the intelligence failures in the US in respect of WMD in Iraq, it was also realised that the remnants of the 'old wall' between foreign intelligence and domestic law enforcement needs to be removed, without sacrificing domestic liberties and the rule of law (US, 2005(c): 466, 452). Previously the guidelines and directives for the FBI's conducting of criminal investigations, national security investigations and foreign intelligence investigations were provided for in separate documents and involved different standards and procedures for comparable activities. The latest guidelines for the FBI's domestic operations integrate and harmonise standards. Consequently these guidelines do not require the labelling of information gathering activities as 'criminal investigations', 'national security investigations' or 'foreign intelligence collections'. There is also no segregation of FBI personnel based on the subject areas which they investigate or in which they operate, ensuring that all the FBI's legal authorities are available for deployment in all cases to protect the public from crimes and threats to the national security and to further the US foreign intelligence objectives (US, 2008(e): 7). The guidelines are clear that the FBI is also authorised to perform effective collection of foreign intelligence within the US. Although the main function of the FBI relates to the investigation of federal crimes and threats to the national security, the FBI is able to gather within the US, information not related to criminal activity and threats to the national security, even information which may concern lawful activity and "information pertinent to the US conduct of its foreign affairs" (US, 2008(e): 9). There is, however, a caveat that where the gathering of foreign intelligence in the US involves activities that are not unlawful, the FBI should "operate openly and consensually with US persons to the extent practicable" (US, 2008(e): 9).

The investigation of criminal cases, in most instances is reactive in nature, namely the investigation of a crime after it has been committed. The *Attorney*

General's Guidelines for Domestic FBI Operations emphasises vigilance in detecting criminal activities at their early stage and prevention thereof (US, 2008(e): 17).

The obtaining of information on persons and organisations involved in crime and in particular the use of HUMINT in that process is emphasised (US, 2008(e): 17). The term 'investigation' is also interpreted more broadly to include, in addition to the gathering of evidence for use in particular criminal prosecution, also critical information needed for broader analytic and intelligence purposes to "facilitate the solution of crime, protect the national security and further foreign intelligence objectives" (US, 2008(e): 16).

Following the 11 September 2001 events the powers of particularly law enforcement agencies in the US were enhanced to enable them casting the intelligence net much wider. Although the investigations into the intelligence failures linked to the events identified a lack of proper use of existing and available intelligence as a failure, the *PATRIOT* Act focused on granting law enforcement wider powers to collect vastly greater volumes of information "without particularised suspicion". If there is a problem using available information, more information or an overload of information may exacerbate the problem (Berman & Flint, 2003: 2). The *Intelligence Reform and Terrorist Prevention Act* in the US envisaged the building of an integrated intelligence capability to address threats to the US. The structural changes effected by the Act, established the National Counter Terrorism Centre with six Directorates: namely for mission management, intelligence, information sharing and knowledge, plans and administration, operations support, and strategic operational planning, and established the new independently budgeted position of Director of National Intelligence (DNI). The *National Intelligence Strategy of the DNI* (US, 2005(a)), in essence calls for the integration of foreign, military and domestic dimensions of intelligence "into a unified enterprise that meets the high standards of objectivity, accuracy and timeliness" (Nicoll & Delaney, 2007:1).

Before 11 September 2001 there was no single US government agency for coordinating counter-terrorism, no single database, no electronic library of terrorist information on inter-agency basis, and no single database of all known suspected international terrorists. The National Counter Terrorism Centre (NCTC) is regarded as having produced significant results in terms of moving to the above goal. It can access over 30 networks from the IC, military, law-enforcement agencies and the Department of Homeland Security (DHS). The NCTC has consolidated all terrorist databases to ease watch-listing and analysis. Despite being described as "a formidable vehicle for realising a truly inter-agency approach to counter-terrorism" the NCTC faces considerable bureaucratic competition from the CIA which has established an operational and analytical, but single-agency Counter-Terrorism Centre (CTC). The conclusion is that in the US intelligence coordination and cooperation is still afflicted by bureaucratic politics (Nicoll & Delaney, 2007: 2).

On the law enforcement side, the FBI, despite enhanced powers in respect of intelligence gathering "remained primarily a law enforcement agency geared to uncovering evidence to facilitate the prosecution of those who have already committed crimes". The 'cultural transition' of the FBI is stated to be slow centred on a counter-productive 'zero tolerance' towards illegal immigrants ((Nicoll & Delaney, 2007:2). It is stated in the US 500-day plan that: "We will not change the culture of the [intelligence community] overnight. The process is iterative: we will review our progress every 100 days and refine our progress as we learn" (Nicoll & Delaney, 2007: 2). What is clear from the above, is that despite being aware of the problem of institutional differences between law enforcement and civilian intelligence and interagency rivalry, it is one of the most difficult to address and some form thereof will probably always be experienced. In some instances it is only the total restructuring of the intelligence community that has the potential to solve the problem, such as the establishment of the DNI and the Department of Homeland Security in the US.

Another factor affecting intelligence cooperation, is the rise of the private intelligence and private security industry. This will be discussed in the next section.

7. RISE OF PRIVATE INTELLIGENCE AND PRIVATE SECURITY

Over the last decade there has been a huge growth in private intelligence companies, which successfully apply methods of the IC to big business. As a result of the lucrative business, large numbers of experienced former intelligence operators from intelligence agencies such as the FBI, the CIA, the UK MI5, and the UK SIS or MI6 moved to the private sector, with a mission to collect and analyse information ranging from fraud and other crime to terrorism to determine the risks for business in a particular country. There is a tendency for governments to also employ private intelligence, for example, Aegis which was awarded a $300m US contract to supply intelligence and security for reconstruction in Iraq. One of Aegis' functions in Iraq is to provide other private security companies in Iraq with operational intelligence on what is going on in the country. The fact that the main players in Aegis are military and not civilian intelligence operators, is indicative of the fact that the company's focus is on military and not civilian intelligence matters, though it offers "a range of geopolitical intelligence, threat assessment and investigative services tailored to the specific requirements of the corporate, institutional and government clients" (Smith, No Date: 2).

Other such private intelligence companies are Control Risks Group, Diligence, Grayson, Pender and Wordsworth (GPW), Hakluyt and Kroll and Associates (Smith, No Date: 2 – 6).

The use of private intelligence by governments, even if it is done overtly as in the case of Aegis, holds various implications- firstly for accountability of the government using private intelligence. Secondly private security can be used to establish deniability of the government involved. In the long run the use of private intelligence may be extremely negative in the sense that it may destroy trust in the government involved and be detrimental to future intelligence cooperation. Other intelligence services may become reluctant to share intelligence with the intelligence services of a government which extensively rely on private intelligence. As pointed out above, mistrust is one of the factors which inhibit intelligence cooperation.

The availability of private intelligence to the highest bidder creates a situation with much the same dangers for global security as mercenary activities- the rise of private intelligence, to some extent forms part of what is referred to as the privatisation of security. Without a vetting process an intelligence agency in one country would never know whether a private intelligence company is a front of another government.

The different oversight mechanisms for law enforcement and civilian intelligence are factors influencing intelligence cooperation, both on national and international level.

8. DIFFERENT OVERSIGHT MECHANISMS OF CIVILIAN AND LAW ENFORCEMENT INTELLIGENCE

As a result of the fact that civilian intelligence and law enforcement institutions are structured differently in different countries, it cannot be generalised that intelligence oversight mechanisms are different for law enforcement and civilian intelligence. In the US, the FBI is regarded, for example as both a law enforcement and crime intelligence agency (US, 2008(e): 9). In Canada, the Commission of Inquiry into the Actions of Canadian Officials in relation to Maher

Arar, undertook a comparative study of the review mechanisms in respect of law enforcement and civilian intelligence agencies in eight countries, including Canada, the UK, the US and Belgium (Canada, 2006(a): 309). The Commission pointed out that the structure of review mechanisms is closely related to the constitutional structure and the structure of the police and security (meaning in this case 'civilian') intelligence agencies. It is not possible to provide a benchmark that will necessarily apply to all countries. In the UK the covert investigation review authorities have jurisdiction over both the activities of police and civilian intelligence agencies. In England and Wales, however, two different review bodies have jurisdiction over national security activities of the police, namely the Independent Police Complaints Commission and the Investigating Powers Tribunal. In the US, oversight is conducted by inspectors general for different departments, namely the inspectors general respectively for Homeland Security, the Department of Justice, the CIA, Department of Defence and the State Department. All these mentioned institutions are involved in intelligence gathering which might overlap in respect of international crimes such as terrorism and organised crime. The oversight is organised in respect of departments and not in respect of functions such as covert intelligence gathering (Canada, 2006(a): 310). For purposes of this study, it is not deemed necessary to reflect the details of the above study. The value of the comparative Canadian study lies in the common challenges identified in the study in providing for accountability of law enforcement and civilian intelligence.

8.1. Common challenges for accountability of intelligence

There is an increased integration and sharing of intelligence between law enforcement (crime) intelligence and civilian intelligence agencies. There is also an increased blurring of the distinction between civilian intelligence and criminal (crime) intelligence. In Canada, for example, there is an increased integration of the functions of the RCMP and the Canadian Secret Intelligence Service. The accountability mechanisms of law enforcement intelligence and civilian

intelligence in many instances are still separate institutions. Where law enforcement has performed criminal investigations and had been supplied with intelligence products from civilian intelligence the accountability mechanisms would therefore still be performed by different institutions. In the case of law enforcement, account will normally be taken of court processes. The same needs to be done when civilian intelligence accountability institutions review actions by civilian intelligence which were performed together with law enforcement agencies (Canada, 2006(a): 313).

The Commission of Inquiry into the Actions of Canadian officials in relation to Maher Arar proposes some best practises from this study, such as the advantages of an accountability system that allows for monitoring integrated activity, in other words developing an accountability body with jurisdiction over multiple government agencies or by establishing "robust mechanisms for information exchange and co-operation between accountability bodies" (Canada, 2006(a): 214). In this respect, the Commission refers to the highly developed cooperation in the US amongst oversight bodies and access by the respective inspectors general to information held by government departments or agencies other than the agency under scrutiny. Essential features for ensuring accountability are: (Canada, 2006(a): 316, 317)

— The review/oversight body must be under an obligation to preserve the secrecy of sensitive information. This is important for gaining the trust of the agencies. The independence of the members appointed and processes (vetting) of appointees to oversight bodies are important for public trust and confidence.
— Oversight bodies must have wide access to information and documents. The study showed wide variations of access to information covered by Cabinet privilege, information subject to third party caveats or information that could disclose the identity of informants or human sources.
— Oversight bodies must be able to initiate investigations, as well as to investigate complaints.

It is understandable that different review mechanisms in respect of the same or a similar intelligence function may be problematic, especially if there is no exchange of information or review activities between the respective mechanisms.

The RCMP was restricted by a Ministerial direction to have written record and ministerial approval of all oral agreements with foreign civilian intelligence agencies. The direction did not apply to oral agreements with foreign police agencies. Thus the requirement was applicable to intelligence cooperation between the RCMP and the CIA, but not between the RCMP and the FBI (Canada, 2006(a): 113).

Oversight over intelligence activities should not be seen as a hindrance to intelligence cooperation. It is, however, important to analyse such oversight from the perspective of international intelligence cooperation. International intelligence cooperation has grown vastly since the 11 September 2001 events, and such growth has generated major challenges for democratic accountability and parliamentary control of intelligence services. The exposure of practices such as secret detention centres shows a lack of accountability of intelligence cooperation (Born, 2007: 2, 3). In some states oversight mechanisms are not allowed to perform oversight over international intelligence cooperation and where such power exist it is limited (Born, 2007: 4). There is, however, some movement towards interaction between different national and international institutions to at least share experiences on oversight practices. The International Intelligence Review Agencies Conference meets biannually, whilst the EU Member States' and candidate Member States' parliamentary intelligence oversight committees met in Bucharest during October 2006. In view thereof that such meetings are not regularly held; only take place on an informal level; and are limited to a small number of countries, they do not really impact on improving oversight over international intelligence cooperation (Born, 2007: 6, 7). Born suggests a "network accountability" working towards a balancing between the power

generated by international intelligence cooperation and the powers of effective accountability mechanisms (Born, 2007: 8). It is understood that this suggestion means in practice that international intelligence cooperation needs to be accountable on a wider scale than simply the individual accountability mechanisms provided for in the respective national systems.

Crime intelligence activities often lead to prosecution in open court where not only investigative methods, but in many instances the intelligence processes are scrutinised in public. In respect of civilian intelligence, even elaborate structures of oversight may prove to be difficult to ensure compliance with certain norms and standards: “Oversight is hindered by insufficient cooperation from the executive and the intelligence agencies, scant and vague mandates of oversight committees, lack of resources as well as insufficient motivation of parliamentarians to engage in pro-active oversight” (Wetzling, 2006: 19).

Intelligence cooperation is performed with the aim to gain an advantage, but may bring about human rights abuses, the mismanagement of government funds, the exercise of plausible deniability and other forms of ministerial abuse (Wetzling, 2006: 4). Oversight mechanisms are established mainly to oversee the activities of national intelligence agencies and are not in particular directed at international (intra-governmental) intelligence cooperation. There is some recognition that current security threats, such as international terrorism, international organised crime and the proliferation of WMD, demand new strategies to also address non-state actors (Wetzling, 2006: 7). The clandestine nature of intelligence cooperation and the acceptance that intelligence actions are often in breach of the law, not of two collaborating States, but probably a third, or may involve extralegal processes, even assassination, makes it imperative that human rights are not regarded as “an obstacle to national security” (Wetzling, 2006: 9).

Sceptics refer to intelligence cooperation as ‘networked torture’ (Wetzling, 2006, 9). Oversight over intelligence activities should ensure adherence to human

rights standards, without curbing operational flexibility and effectiveness of intelligence agencies and unauthorised disclosure of information by oversight institutions criminalised (Wetzling, 2006: 29). Oversight should involve five actor groups, namely the intelligence services; the legislature; the executive; the judiciary and civil society organisations (Wetzling, 2006: 33). Intelligence cooperation on the international level, for example within the EU or UN, is not subject to traditional oversight mechanisms.

Within international organisations the intelligence processes, including intelligence collection is often performed 'independent' from the nation states of which such international organisation comprises. Although some proposals have been made on oversight mechanisms outside the national mechanisms, such oversight over international intelligence cooperation is improbable in view of issues such as sovereignty, except for the limited role of the UN Security Council.

Born also expresses a concern about the lack of general standards for entering into agreements with the services of other countries, standards for receiving or sending of information, and standards on a requirement for political authorisation of international cooperation (Born, 2007: 4).

8.2. Public-private Intelligence partnerships and oversight

Another area, in which the different oversight regimes in respect of civilian intelligence and law enforcement intelligence play a role in the US, is in respect of public-private partnerships. What is questioned is not the practice, but the lack of legal formalities and the fact that it can be arranged to "evade oversight and, at times, evade the law" (Michaels, 2008: 901). The private sector has unparalleled access to private information of the public- through transactions performed on social, personal and economic level. Should government agencies wish to have access to the same information, it would be subject to legal restraints, which are not necessarily required for the private sector (Michaels: 2008: 902). In the

process of accessing information from the private sector, actors in the private sector are courted, through persuasion, coaxing and sometimes deceiving them into 'informal' partnerships for intelligence cooperation. Such cooperation is sometimes inscrutable by oversight mechanisms.

Intelligence agencies depend upon private data resources for data, such as shopping and frequent traveller clubs' membership for data-mining to determine significant patterns of behaviour (Michaels: 2008: 908). Numerous examples are quoted of instances where public-private intelligence partnerships had a huge impact on human rights, such as the Terrorist Surveillance Programme (access allowed by major telecommunications companies to the US NSA to telecommunications switches, and enabling the NSA to intercept communications without having to obtain warrants in terms of the *FISA)* (Michaels: 2008: 911). More background on the TSP is provided in the next chapter. Access was similarly gained to call information, such as names, lists of calls and e-mails placed and received and call duration. In some instances access was provided voluntarily by telecommunications service providers even in respect of information which requires subpoenas (Michaels, 2008: 912, 914). At least one company refused to provide information which required legal processes in order to access it (Michaels: 2008: 912). Access to information on wire transfers, postal articles and banking databases were also obtained from the Western Union Company, Fedex and the Worldwide Interbank Financial Telecommunications (SWIFT). SWIFT is described as the central nervous system of international banking (Michaels: 2008: 914, 915, 916).

Operationally there are numerous advantages to this informal type of intelligence cooperation, and it continues precisely because there is no credible sanction in respect of national security investigations not aimed at prosecution. In criminal investigations, for example, investigators are deterred from using informal or dubious methods to gain access to information as it may lead to suppression proceedings and may jeopardise the prosecution (Michaels: 2008: 925). In view

thereof that intelligence gained from informal cooperation needs to be used in court for example, governments engaged in what is referred to as 'data-laundering', namely the cleansing of the unlawful or unauthorised origin of the data, or using information obtained through 'informal' means to obtain authorisation for further access (Michaels: 2009: 930). The practise of informal public-private intelligence partnerships has numerous harmful effects, such as lack of accountability; the privatisation of the intelligence and resultant powerful position it places the private sector in; and the ripple-effect of questionable practices. The lack of oversight also leads to uninformed political decision-making on intelligence activities (Michaels: 2008: 932). Eventually the practise of such informal cooperation may be counter-productive for even formal intelligence cooperation, in view of mistrust developing with public exposures of unauthorised access by intelligence agencies to public information. One of the solutions proposed, is minimisation, namely to restrict the use of information obtained through informal intelligence cooperation from corporations, for intelligence purposes only and not for ordinary law enforcement purposes (Michaels: 2008: 960). This is, however, no guarantee that such informal intelligence cooperation might not jeopardise criminal investigations and prosecutions, should the basis of cooperation not be legally sound.

8.3. Oversight role of the United Nations

The UN also exercises some oversight over international intelligence cooperation through the office of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism. In the report of the Special Rapporteur following the country visit to the US he identified "deficiencies in United States law and practice pertaining to the principle of *non-refoulement*; the rendition of persons to places of secret detention; the definition of terrorism; non-discrimination; checks in the application of immigration laws; and the obtaining of private records of persons and the unlawful surveillance of persons, including a lack of sufficient balances in that context" (UN, 2007(c): 23).

Only two days after taking up office, the US President issued an executive order for the closure within one year of the Quantánamo Bay detention facilities (US, 2009). In respect of international mechanisms for oversight over international intelligence cooperation, Born mentions the danger of enquiries by intergovernmental organisations being "scuppered by the national interests of states" and when they are successful in obtaining a reply to the enquiries, states are under no binding obligation to cooperate or enforce the findings made by such intergovernmental organisation (2007: 5).

The Special Rapporteur has proposed to the UN Human Rights Council a compilation of 35 good practices on legal and institutional frameworks and measures that ensure respect for human rights by intelligence agencies while countering terrorism, including on their oversight. Five of these principles in particular relate to intelligence sharing and cooperation, namely to provide clearly in law the parameters for national and international intelligence sharing; a requirement for executive approval for intelligence sharing agreements; taking into account the human rights records of intelligence 'partners' and ensuring that shared intelligence will not be abused to violate human rights; independent oversight mechanisms to examine intelligence sharing arrangements and practices; and an explicit prohibition on intelligence agencies to employ foreign agencies in order to circumvent national legal standards and institutional control of their own activities (UN, 2010: 27 – 30).

9. CONCLUSION

Intelligence cooperation on all levels, namely national, regional and international levels, is increasing despite the vast challenges set out above. International crime cannot be combated without such cooperation. Some challenges, such as those posed by sovereignty cannot be countered to the extent that countries will always place their own interests first. The focus of intelligence cooperation

should therefore be on common threats. One of the most significant threats to international intelligence cooperation is the negative effect of covert or clandestine operations, such as extralegal rendition and sometimes assassination of terrorist targets. Although such actions may result in successes for the countries executing them, it led in numerous instances to embarrassment for countries that cooperated and to subsequent policy decisions on the highest level not to further allow cooperation in respect of such actions. This is true even amongst the closest partners in intelligence cooperation, such as the US and the UK. Intelligence cooperation aimed at pure law enforcement actions seems to have the best chance for success. It is, however, in many instances imperative to be able to utilise the intelligence support of civilian and even military intelligence in order to ensure successful investigation of, or the prevention of international crimes. The rise of the privatisation of intelligence and informal cooperation between intelligence agencies and private intelligence also poses challenges for cooperation as informal cooperation with private intelligence may jeopardise even criminal investigations, if there is no sound legal basis for the cooperation or outright unlawfulness. Private-public intelligence partnerships have various negative effects, such as a lack of accountability.

There is also a lack of intelligence oversight over international intelligence cooperation and the move towards interaction between various oversight and review mechanisms nationally and between countries can only be supported. The issue of human rights should not be ignored in intelligence cooperation, as future cooperation may be jeopardised where a cooperation partner tends to develop practices which have no or little regard for human rights, for example where torture is involved.

Sovereignty is sometimes used to promote international cooperation in a manner which can be questionable in terms of accountability. This is in particular true in respect of joint surveillance efforts such as that between the US and the UK, where the product of the joint surveillance is based on different mandates and

sharing of intelligence which would probably have been unlawful for the host country to gather in the particular circumstances.

Challenges on international level such as the problem of dysfunctional or failed states require cooperation on international level, not only in respect of intelligence, but also diplomacy and the use of international and regional organisations to overcome the negative effects of the fact that the state in question is actively engaged in international crime or either unwilling or unable to cooperate with the international community to combat those crimes, such as war crimes, genocide, piracy or terrorism.

On a national level, challenges such as interagency rivalry and the differences in the organisational cultures between law enforcement and civilian intelligence can be overcome through the restructuring of intelligence structures and liaison forums such as fusion centres. It is important to be constantly aware of the challenges to intelligence cooperation in order to use all possible means to counter those challenges.

In the next chapter the methodologies of law enforcement intelligence and positive intelligence will be compared to establish where cooperation is possible.

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.

CHAPTER 7

MODELS FOR INTELLIGENCE COOPERATION ON THE REGIONAL LEVEL

1. INTRODUCTION

In the previous chapter, models of intelligence cooperation on national level were discussed and analysed. In Chapter 3 Europol, ASEANAPOL, the ACSRT, SARPCCO and CISSA were referred to within the context of the legal basis on which each organisation had been established, and international obligations in respect of information and intelligence sharing and intelligence cooperation. Each of these models is of particular importance within the context of regional intelligence sharing and cooperation. Furthermore, it is important to establish whether some of the principles in respect of enhancing intelligence and intelligence cooperation, including the sharing of information and intelligence on national level, can be applied in respect of regional cooperation. As a result of the principle of sovereignty and self-interest of states, which are major factors inhibiting intelligence cooperation, the regional level of cooperation is of particular importance, in view of the fact that within particular regions there are numerous factors, such as common threats, common economic interests and common borders to protect, which to some extent diminish the influence of sovereignty.

In this chapter the focus is on practical intelligence cooperation, and how factors inhibiting intelligence cooperation are addressed in furthering common interests. Within the EU, the open borders and consequent freedom of movement for people and goods provide unique opportunities for the commission of crime, and

requires measures to ensure that jurisdiction of the respective countries is not abused in the commission of crime. Each region has its own challenges in terms of intelligence cooperation with diverse forms of government and legal systems, different policing and intelligence structures and diverse capacities. In this chapter different models of crime and civilian intelligence cooperation on the regional level are discussed and analysed with a view to determine common approaches between national and regional intelligence cooperation and also the relationship between national and regional intelligence cooperation. The first model of regional crime intelligence cooperation is Europol.

2. INTELLIGENCE COOPERATION: THE EUROPEAN POLICE OFFICE MODEL

Europol is described as a regional supranational body with the intended objective to "produce and diffuse 'finished intelligence' derived from the compilation and analysis of national law enforcement authorities" of the countries participating in Europol (Gerspacher, 2005: 414, 419). The personnel strength of Europol is as follows: 124 liaison officers; 461 Europol staff and 37 national and seconded experts, trainees and contractors (Europol, 2009(a): 42). Officers working at Europol come from diverse law enforcement backgrounds, including police, border guards, customs and intelligence services, affording a multi-lingual and multi-cultural approach conducive to a swift and efficient exchange of information to and from Europol and Member States (Saccone, 2006: 6). The main outstanding features of Europol are the following: (Saccone, 2006: 2, 6 – 8)

— Europol established a network of liaison officers from national units, stationed at Europol and linking the national units to Europol, focusing on swift exchange of information on serious crimes committed transnationally, such as drug trafficking; human trafficking and illegal migration; fraud; Euro counterfeiting; commodity counterfeiting and money laundering. The network is further strengthened by the presence of liaison officers from

other cooperating countries with which Europol has cooperation agreements, such as Norway, Switzerland and the US.

— A strong analysis function enabling the receipt, storage, processing and production of strategic assessments and operational support for ongoing investigations. This function is supported by some 100 analysts from the different countries.

— Three computerised systems, namely firstly an information system to check suspects in investigations on serious crime and terrorism in the EU, which is the largest database on organised crime available to law enforcement in the EU. The second system is the analysis system which supports the reception, storage processing and analysis of information and intelligence gathered during criminal investigations. Access to the system is restricted and is used for the analysis work files (AWFs), described as a legal tool that creates a platform for a safe and well regulated sharing of criminal information and intelligence on ongoing cases. The third system is the index system aimed at "querying the presence of entities stored in the analysis system", in other words serving as a search engine.

— Expertise developed by Europol for the detection, dismantling and analysis of illicit laboratories for the production of synthetic drugs.

The EU Ministers agreed in 2005 on a European Criminal Intelligence Model (ECIM) (EU, 2004). This model is to a large extent based on the principle of intelligence-led policing, also referred to in the previous chapter as the basis of a system of intelligence cooperation in both the US and the UK. Intelligence-led policing is described as a law enforcement theory "that stresses intelligence gathering and the targeting of police resources on the worst criminals". The ECIM, which forms the basis of crime intelligence cooperation within the EU and more specific Europol, is described in more detail hereunder.

2.1. European Criminal Intelligence Model

ECIM sets out how the different police forces in the EU can plan investigations together using the best intelligence available, by ensuring that national police forces, Europol's intelligence analysts and the police chiefs' operations work together against the same criminal threats (Brady, 2008: 103). The law enforcement agencies of Member States of the EU have direct access to the central computerised system provided for in the Europol Convention. In line with the intelligence-led approach, security operations in the EU are increasingly relying on information technology, such as converting close circuit footage of covert surveillance of a suspect into data in respect of persons and vehicles (with identification), which data is then analysed against other data and criminal records (Segell, 2004: 83). Practical access to information by law enforcement agencies in the EU is based on the EU Information Policy, adopted during 2004, which also sets out the broad concepts for the introduction of intelligence-led law enforcement in the EU region (EU, 2004: 3). Member States are called upon in the EU Information Policy to make available to law enforcement agencies the relevant 'data and information', which is defined in the EU Information Policy as 'data, information and intelligence', to prevent and combat not only terrorism, but also other forms of serious or organised crime and threats related thereto. In the process it must be taken into account that criminal activity which might at first glance not be regarded as serious or organised could be connected to or related to serious or organised crime. Member States are expected to also produce high quality EU criminal (crime) intelligence and must enhance trust between the law enforcement services.

Of particular importance is that the EU Information Policy is aimed at improving information exchange between police authorities as well as between customs; authorities; financial intelligence units; the interaction between the judiciary and public prosecution services, and all other public bodies "that participate in the process that ranges from the early detection of security threats and criminal

offences to the conviction and punishment of perpetrators" (EU, 2004: 4). The EU Information Policy set as aim to expand the access that law enforcement agencies have to their national databases, to having equal access to equivalent rights of access to data and databases of EU Member States on comparable conditions as law enforcement authorities in that Member State. This principle of equal access implies a recognition of a common responsibility towards the security of the EU, interdependency of Member States to address threats and crimes of a serious and organised nature; the similarity of the tasks of law enforcement in all the countries, which requires equal access; and lastly that these agencies need to act lawfully in accessing data or databases within set boundaries of common standards, data protection and data security (EU, 2004: 7). In respect of an intelligence-led model of policing for the EU, the need to use standard analytical tools to produce a crime threat analysis for the region in respect of serious and organised crime has been identified. This threat analysis must be used to develop priorities from the operational assessment in respect of specific desired outcomes such as arrests, searches, seizing and forfeiting of assets derived from criminal activities (EU, 2004: 11).

The EU Information Policy emphasises the introduction of common standards on data access and processing as well as compatible methodologies related to threat, risk and profile assessments as a basis for effective sharing of information and intelligence at strategic as well as operational levels. This is also crucial to establish a trusted information environment (EU, 2004: 12). In Chapter 3, reference has already been made to the Europol EU Organised Crime Threat Analysis and the EU Terrorist Threat Analysis, which form the basis of Europol operations. The EU Information Policy strengthens the role of Europol in the sharing of data and information. This policy seems to have rendered positive results as police in EU Member States on the operational level now view Europol more favourable as a useful channel for coordinating the combating of organised crime, as well as appreciating the value of pro-active cross-border police cooperation (Brady, 2008: 104). Europol is unique as a regional police

organisation as to the degree of 'independence', not only in respect of intelligence cooperation, sharing and analysis, but also operationally- through Joint Investigation Teams (JITs), as referred to in Chapter 3, as well as the flexibility of some national police forces to work across borders within the EU, with less bureaucracy involved than would normally be the case between different states. Joint criminal investigations and operations of Europol are discussed hereunder to illustrate the degree of operational flexibility of Europol.

2.2. Criminal investigations and operations of the European Police Office

Following reluctance by Member States of the EU to participate in JITs, the European Council established an informal JITs Experts Network, to come into operation by September 2005. The JITs Network required each state to designate one or more expert to it (all Member States have done that); that the Network must meet informally and regularly in smaller groups; national experts must liaise with other persons and organisations within their Member States to provide information and advice from that Member State; and national experts to the JITs must share best practices with the group (EU, 2005: 2). The JITs furthermore provide information about the legal frameworks in the respective Member States, the national contact points as well as assist to overcome linguistic problems. Intelligence and operational investigative support and involvement of Europol covers a wide range of crime, not only organised crime and terrorism.

At the most recent annual meeting of the JITs experts a manual was produced in which guidelines are provided on how to set up a JIT (Europol, 2009(a): 51). Some of the most recent operations involving Europol are the following: (Europol, 2009(a): 18, 19, 24, 25)

— Operation Hammer, dealing with child abuse, including child sexual abuse on the Internet, where Europol provided an initial intelligence package,

assisted in identifying suspects and coordinated meetings. Operation Hammer led to the arrest of 60 offenders and the rescue of 11 child victims of sexual abuse. Operation Hammer also involved various US law enforcement agencies, including the FBI.

— Operation Pipas, targeting an international credit card fraud network. Europol provided strategic and operational analysis coordination to the Spanish National Judicial Police as well as providing a mobile office. The successes of Operation Pipas included the arrest of 99 criminals, the dismantling of an international credit card fraud network, and the seizure of € 6 million of profits derived from crime.

— Operation Decan, targeting skimming fraud (*inter alia* obtaining credit card particulars and codes to fraudulently obtain money from credit card accounts). Europol provided strategic and operational analysis, a mobile office, coordination and video-conferencing services. The successes of Operation Decan included 15 criminals arrested, 34 houses searched, investigations and prosecutions in eight EU Member States, as well as Australia and Canada, and an international credit card fraud network dismantled.

— Operations Trufas and Baghdad, targeting human trafficking. Europol provided assistance through exchange and analysis of information, and intelligence reports and identified new criminal links. Operation Trufas resulted in the arrest of 65 suspects, and Operation Baghdad in the arrest of 75 suspects, in both cases throughout Europe. Both operations led to the dismantling of a Europe-wide human trafficking network.

A major legal instrument towards the facilitation of criminal investigations across national borders, is the *Council of Europe Convention on Mutual Assistance in Criminal Matters*, updated in 2009 by the Council of Europe to also include requests for undercover operations abroad; the interception of phone and internet communications across borders; and surveillance operations to secretly monitor crimes such as drug trafficking; and performance of controlled deliveries (Brady,

2008: 104). As mentioned above, the combating of crime in the EU is greatly enhanced through JITs, on a more frequent and practical level through operational flexibility to act across national borders of the EU. This is in particular true in respect of the Schengen countries, where police forces have extra powers to pursue crimes with a cross-border dimension. Examples in this regard are: (Brady, 2008: 105)

— The power of Dutch police officers to perform surveillance, with or without prior notification, in Belgium;
— the power of Italian police officers to follow a suspected drug trafficker over the border into Austria, until the Austrian police arrive; and
— before the 2006 FIFA Soccer World Cup, Germany and Austria signed a treaty placing their police under each other's command and allowing police officers of each others countries unrestricted undercover operations in the other's territories.

Europol also provides analytical support to the Comprehensive Operational Strategic Planning for Police (COSPOL) Project of the European Police Chiefs Task Force (EPCTF). The EPCTF initiated the COSPOL Project, a multilateral law enforcement instrument to improve operational results in respect of top criminals and terrorist networks and to provide support and strategic planning; coordination and communication between all relevant partners (Saccone, 2006: 9). The operations which are launched in terms of the COSPOL Project are mainly derived from the Europol Organised Crime Threat Analysis (OCTA) (EU, 2008(a): 1). From the above, it is clear that Europol is not the only role-player in respect of crime intelligence, joint investigations and joint operations on the regional level in the EU. The operational role of Europol is important to assess the organisations' practical value in respect of crime intelligence cooperation.

2.3. Operational role of European Police Office: Exchange of information

Some 124 397 searches were performed on the Europol Information System during 2008 and at the end of 2008, the Information System contained 88 419 objects (Europol, 2009(a): 35). Data is deleted automatically after three years, but the information system has started to grow at a rate where the additions to it are more than deletions. Hits or matches produced by the information system have grown in a year from 86 to 140 (Europol, 2009(a): 36). Europol also has an important strategic role which needs to be highlighted.

2.4. Strategic role of European Police Office

The intelligence products of Europol include the Europol OCTA and the EU Terrorist Situation and Trend Report (Europol TE-SAT). These reports are presented to the EU decision-makers and are important in terms of strategic direction and focus of resources (Europol, 2008(b)) (Europol, 2009(b)). Europol's value is hugely enhanced by other European partners, which are mentioned hereunder.

2.5. European Police Office and other European partners

Eurojust is a new EU body and the first network of judicial authorities to be established in the world. Eurojust had been established to enhance the effectiveness of the competent authorities in the Member States in dealing with the investigation and prosecution of serious cross-border and organised crime. Eurojust facilitates the execution of requests for mutual legal assistance and extradition between Member States (T.C.M. Asser Instituut, 2009: 5). Europol and Eurojust have cooperated in a number of cross border investigations, by using Eurojust to supplement the investigative actions of JITs with mutual legal assistance and extradition requests to ensure successful prosecutions. Another

important European partner of Europol is the European Agency for the Management of Operational Cooperation at the External Borders of the (EU) Member States (Frontex), with which Europol had concluded a strategic agreement. Frontex is based in Warsaw. It is an independent organisation tasked to coordinate operational cooperation between EU Member States in respect of border security, and operates on an intelligence-driven basis. Its purpose is described as the coordination of operational cooperation at EU level to strengthen security at external borders. It is a key player in implementing the concept of an EU Integrated Border Management (Frontex, 2009: 1).

The exchange of strategic intelligence between Europol and Frontex for intelligence products has increased, and whilst Frontex contributed during 2008 to the Europol OCTA, Europol in turn contributed to the Frontex Annual Risk Assessment. Europol has also signed cooperation agreements with all the countries of the Western Balkans, namely Serbia, Montenegro and the Former Yugoslav Republic of Macedonia. Europol has operational agreements in place between the following states: Australia; Canada; Croatia; Iceland; Norway; US, and operational agreements with Eurojust and INTERPOL. Europol has strategic agreements with Albania; Bosnia and Herzegovina; Colombia; Moldova; Russian Federation; Turkey and the Former Yugoslav Republic of Macedonia; as well as strategic agreements with the European Anti-Fraud Office (Olaf); European Central Bank (ECB); European Monitoring Centre for Drugs and Drugs Addiction (EMCDDA); European Police College; United Nations Office on Drugs and Crime (UNODC); World Customs Organisation (WCO) and Frontex (Europol, 2009(a): 52). It is necessary to explore the difficulties or challenges experienced by Europol on the practical level, to determine the value of the Europol model.

2.6. Challenges experienced by European Police Office

Although improved intelligence work and “having officers from 27 European countries on the same corridor in The Hague is an unparalleled resource in day-

to-day police cooperation", there are major challenges still facing Europol (Brady, 2008: 107). Contributions by Member States to the Europol OCTA remains varied and from some countries almost absent. Officers designated by Member States are in some instances unauthorised in their national jurisdiction to resolve cross-border issues, with resultant negative effects on trust building and the strengthening of cooperation in international investigations. On the level of prosecutors there is also a disparity between the Member States of the EU in respect of the basic powers to issue formal requests for evidence and to authorise controlled deliveries, interception of communications and undercover operations (Brady, 2008: 107, 108).

The level of bureaucratic stumbling blocks, emanating from Europol's founding Convention in that even minor administrative decisions by the Europol director require approval of all 27 Europol Member States. New envisaged EU legislation is, however, to provide wider investigative powers to Europol, covering more crimes, cause Europol to be less bureaucratic and have more freedom to gather intelligence and information like DNA data. The following reforms have been proposed for Europol to address full police cooperation: (Brady, 2008: 108)

— Harmonisation of the different roles of police and prosecutors in the respective Member States.
— Harmonisation of the powers of officers designated to Europol by the respective Member States.
— Merging Europol, Eurojust and the EPCTF to form a single European law enforcement coordinating body. Eurojust and Europol are reported to co-locate in 2009. Advantages of such a merger include the prevention of duplication in intelligence gathering and analysis and a better "follow through from investigation to prosecution in cross-border cases".

It is not known whether the co-location of Europol and Eurojust will indeed take place, but a new agreement between the two organisations, with the objctive to "enhance the cooperation between Eurojust and Europol in fighting serious forms

of international crime" was concluded on 1 October 2009. The new agreement provides for the exchange of information, and the establishment of JITs composed of judicial authorities and law enforcement authorities in the EU upon request of Member States. In respect of the role of Europol, it is stated that: "When it is decided to participate in such a team, Europol shall endeavour to bring its support in order to facilitate co-ordination between the judicial authorities concerned and Europol shall endeavour to support the intelligence gathering and investigative efforts of the team" (Europol, 2009(c).

It had also been suggested that Europol second Europol experts in specific regions to assist law enforcement initiatives run by different Member States. The role of Europol should also be clearly defined in relation to the other EU law enforcement and intelligence agencies, in order to avoid duplication of efforts and potential for competition. Such defining of roles should be part of a: (Saccone, 2006: 12)

> structured reflection on the overall architecture of the security approach in the European Union, with a clear definition of tasks and functions of each EU agency, the description of the interaction amongst the various agencies and the technical, legislative and procedural conditions that need to be put in place to achieve the interoperability of the various computerized systems.

The above dealt with crime intelligence cooperation in Europe, through Europol. Intelligence cooperation in respect of military and civilian intelligence is also of importance, especially to compare the models in respectively Europe and Africa. In Chapter 3 some reference was made to institutions for intelligence cooperation such as the Club of Berne, NATO and the European Union Military Staff. In the following sub-section, intelligence sharing in the EU in respect of military, crime and civilian intelligence is reflected upon, in order to indicate possible solutions to

one of the main factors inhibiting intelligence sharing and cooperation, namely mistrust.

2.7. Intelligence sharing and cooperation in the European Union

It is clear that the expansion of the EU led to a much greater demand for intelligence to combat international crime. At the same time the expansion led to a lack of trust, especially with the joining of the EU of what was previously referred to as East bloc countries and now 'emerging democracies'. In the reform process of the intelligence services of emerging democracies in these (former East bloc) states, extensive vetting was undertaken to purge intelligence services from what is referred to as "legacy personnel". This led to a huge cut in the personnel of intelligence services in these countries, in some instances also resulting in a loss of expertise. The vetting was only partial successful as many of the personnel who were found unsuitable for further employment in intelligence services, were redeployed in departments where vetting was no requirement, but where they might have access to intelligence. In addition factors such as corruption; personal vendettas; unfair legal processes; the manipulation of the vetting process by experienced intelligence personnel being vetted; and a lack of complete records played a negative role in the early "post-communist personnel vetting processes" (Watts, 2001: 21 -23).

The intelligence sharing institutions of the EU, in addition to the crime intelligence sharing institution (Europol), discussed above, are: (Walsh, 2009: 7, 8, 9, 10)

— In respect of civilian intelligence, the Berne Group or Club, referred to in Chapter 3, has expanded from six to twenty-seven members, including all EU Member States. It serves as a principle point of contact between the heads of national security (intelligence) services, meeting regularly. The Berne Club produces, through cooperation between Member States as well as the US, common threat assessments that are shared amongst

Member States. The Berne Club has established working groups on terrorism and organised crime and also the Counter Terrorist Group.

— In respect of military intelligence, the EU Military Staff is of importance for intelligence sharing to support the Military Committee and the Political Security Committee. Each Member State seconds at least one representative to the Intelligence Division of the Military Staff numbering 30. These staff members' functions are similar to that of the experts seconded to Europol, namely to serve as conduit for intelligence between the EU and Member States. Intelligence from Member States as well as intelligence gathered by bodies of the EU are used to produce assessments for the Military Committee. Together with the SitCen referred to in Chapter 3, intelligence products include early warning, intelligence assessments, and operational support on external security matters, including terrorism.

Although NATO as organisation had been established for defence cooperation between countries of the EU as well as the US, it plays a significant role in EU intelligence cooperation, as NATO is involved in a number of military operations, including naval operations to combat maritime piracy in the Horn of Africa. During 2008, NATO was requested by the Secretary-General of the UN to provide naval escorts to UN World Food Programme vessels transiting in the Gulf of Aden and the Horn of Africa firstly under Operation Allied Provider and since March 2009 under Operation Allied Protector. The NATO naval force is described as a multinational integrated maritime force made up of vessels of various allied countries and is permanently available to NATO to perform different tasks including operational intervention (NATO, Undated(a)). NATO, in the Alliance's Strategic Concept, underlines its support for arms control, disarmament and non-proliferation of WMD, as playing a major role in its security objectives (NATO, 1999: par 40). NATO is also committed to combating terrorism and is linked by various cooperation agreements with the EU (NATO, 2009). Intelligence activity represents an inherent element of NATO, which was established as a security

and political organisation (Črnčec, 2009: 155). NATO had been involved in peacekeeping operations in Yugoslavia, Bosnia and Herzegovina, the Darfur region of the Sudan (airlift rotations in support of the AU mission in Darfur) and is still involved in the peacekeeping mission in Kosovo. It is presently also involved in military operations in Afghanistan through the International Security Assistance Force. In the Mediterranean, NATO performs a critical counter-terrorist function in respect of surveillance and the boarding of suspect ships (NATO, Undated(b)).

None of the institutions referred to above, including Europol and NATO has rules that force Member States to share intelligence with each other, nor any mechanism to monitor non-compliance or non-sharing of intelligence. Neither NATO nor the EU has an intelligence service of its own (Črnčec, 2009: 156). Operational and 'sensitive' intelligence is seldom shared in the EU (Walsh, 2009: 13). Intelligence sharing is promoted through the practice of masking the origin and source of the intelligence, for example in reports of the Intelligence Division. However, few (seven) of the Member States have foreign intelligence services, which makes it possible to sometimes derive from the type of intelligence, the source thereof. The Intelligence Division seldom receives 'raw intelligence' from Member States (Walsh, 2009: 15). As pointed out in Chapter 4, mistrust remains a factor which inhibits multilateral sharing of intelligence. Mistrust is probably the reason why the integration of intelligence, in other words a single EU intelligence institution, which had been proposed in the past by countries such as Belgium and Austria is problematic (Walsh, 2009: 20). Despite the huge advances made in the EU with the sharing of crime intelligence through Europol, there is still, in respect of Europol, the Berne Club and the EU Military Staff, no obligation regarding the sharing of intelligence, with the result that shared intelligence seldom includes 'raw intelligence', and that intelligence shared is voluntary and contains no 'sensitive' information (Walsh, 2009: 13, 15). Self-interest, as pointed out in Chapter 4 also plays a huge role in this regard and it is stated that: "(Intelligence) Liaison relationships are pay-as-you-go propositions, and no nation is given a free ride on anything but a temporary basis" (Rosenau, 2007: 4).

As with intelligence sharing on national level between intelligence agencies, described in Chapter 6, mutually beneficial intelligence cooperation between countries within a regional context requires that some autonomy should be forfeited. At the same time the regional organisations should be capacitated to have enough powers to act in the interest of the region. As integration or the establishment of a regional intelligence agency with autonomous powers which would include collection of intelligence is highly improbable, the following has been suggested: (Walsh, 2009)

— To create more sophisticated networked databases, allowing the sender to post a description only of intelligence on the database, allowing others with access to the database to determine the value of the intelligence, without either having access to the sources or methods through which it was obtained, or having access to actionable details. The full intelligence report could then be obtained from the sender through a "mutually beneficial bargaining process".

— Some subsets or smaller groups of states within the broader EU could meet and cooperate amongst themselves as well as with other partners forming "multi-speed lines", simply meaning not all states participating in all cooperative ventures. The G5, namely Britain, France, Spain, Germany and Italy, is mentioned as such a nucleus of EU Member States with common interests and a high degree of trust among each other, which could provide a basis for being regarded as a group of "like-minded States" which could take the lead in enhancing intelligence cooperation in the EU. This is required because there is no single state in the EU which could take such a lead (Walsh, 2009: 35).

EU military commands responsible for individual, mostly crisis response operations, have a greater need for tactical and operational intelligence. This need is expressed as follows: The provision of appropriate permanent intelligence support is one of the key challenges of every crisis response

operation" (Črnčec, 2009: 159). An advantage of the G5 taking a lead in enhancing EU intelligence cooperation is the fact that: "(t)he United States regularly shares high-grade intelligence with the G5 countries … but appears much less willing to do so with other nations". Nevertheless, it is stated that the speed of exchange of intelligence between the US and the EU is a negative factor, in that neither the EU or NATO is "cut out for swift action- a key shortfall in the case of operational intelligence, whose utility is short-lived" (Rosenau, 2007: 9).

It is clear from the above that the Europol and EU models for intelligence cooperation have overcome many of the negative effects of sovereignty and mistrust. Especially joint police operations are valuable requiring effective and intensive operational intelligence sharing and cooperation in respect of particular projects or investigations of common interest. On the strategic level huge advances have been made with strategic intelligence products such as the EU OCTA and the Terrorist Trend and Threat Analysis. Although a European 'FBI', in other words an independent intelligence agency for Europe had been envisaged as an ideal, it will probably not realise in view of the sovereignty principle. Mistrust also remains a problem. There are proposals to overcome the problem of mistrust and the lack of an independent intelligence agency by means of special databases; and the clustering of Member States in smaller groups with common interests and a higher level of trust between them, such as the G5 to take the lead in enhancing regional intelligence cooperation. A multiplicity even in respect of regional crime intelligence agencies, such as Europol and the EPCTF is a further challenge which is addressed through an arrangement between Europol and the EPCTF called the COSPOL Project. A merger of Europol, EPCTF and Eurojust has been suggested. A further important characteristic of the EU model for crime intelligence cooperation is the cooperation between Europol and Eurojust, including prosecution and justice authorities to ensure successful investigations and successful prosecutions. In Chapter 5 reference was made to a similar arrangement between the US and the UK, which is

yielding positive results. Of importance within the Europol model is its links with both the national law enforcement agencies of EU Member States and through various cooperation agreements with organisations such as NATO, INTERPOL and various cooperative countries.

The following model for crime intelligence cooperation that will be discussed is the ASEANAPOL model in South East Asia.

3. INTELLIGENCE COOPERATION: THE ASSOCIATION OF SOUTH-EAST ASIA CHIEFS OF POLICE MODEL

The establishment, membership and functions of ASEANAPOL as well as its relationship (agreement) with INTERPOL have been discussed in Chapter 3. Little information is available on the actual operations and successes of ASEANAPOL. One example of regional cooperation through ASEANAPOL is Operation Storm, held jointly between ASEANAPOL, INTERPOL, the World Health Organisation, the World Customs Organisation and national authorities in Cambodia, China, Laos, Myanmar, Singapore, Thailand and Vietnam. It resulted in 30 arrests and the seizures of more than 16 million counterfeit medicines worth millions of US dollars (Boon, 2009: 1). This can probably be ascribed to the fact that to date ASEANAPOL does not have a permanent secretariat. At the latest annual general meeting of the 10 ASEAN Member States with five dialogue countries (China; Republic of Korea; Japan; Australia and New Zeeland), as well as INTERPOL, some 330 delegates met from 12 to 16 May 2009, in Hanoi, Vietnam. It became clear that the establishment of an ASEANAPOL Secretariat is imperative, to enhance coordination and cooperation between Member States and to ensure proper and effective implementation of resolutions adopted during the respective annual general meetings. A working group discussed the establishment of an ASEANAPOL Secretariat during March 2009, and made recommendations to the abovementioned conference (Begawan, 2009: 1). During the May 2009 conference the terms of reference for the establishment of

an ASEANAPOL Secretariat, expected to start operating on 1 January 2010, were adopted and key appointments to the Secretariat approved. The ASEANAPOL Secretariat is based in Kuala Lumpur, Malaysia. The conference also approved the implementation of proposals to strengthen cooperation with dialogue partners. The specific proposals included a proposal from Japan to establish a shared database of websites on terrorism (Othman, 2009: 4). In Chapter 3 the broader ASEAN regional structures were described. It is clear that within the ASEAN structures, positive intelligence is shared between the Member States, in addition to the sharing of crime intelligence within ASEANAPOL.

It is clear that ASEANAPOL is still developing, but is following on the African model discussed hereunder and it is expected that its links with INTERPOL and the establishment of a permanent secretariat, will soon lead to increased crime intelligence cooperation and joint transnational police operations to combat international crime.

The following model for intelligence cooperation, mainly in respect of the combating of terrorism, is that of the ACSRT, in Algiers, Algeria.

4. CIVILIAN INTELLIGENCE COOPERATION ON THE AFRICAN CONTINENT

There are two institutions in Africa responsible for the promotion of intelligence cooperation on the African Continent, namely the ACSRT and CISSA, both focused on civilian intelligence, although the products of the ACSRT are also of importance for law enforcement. ACSRT is firstly discussed.

4.1. The African Centre for the Study and Research of Terrorism

ACSRT was established in September 2002, in Algiers, Algeria, and inaugurated on 13 – 14 October 2004. ACSRT originated from the Plan of Action of the AU

High Level Inter-Governmental Meeting on the Prevention and Combating of Terrorism held from 11 to 14 September 2002. The formal structuring of ACSRT was enabled by the *OAU Convention on the Prevention and Combating of Terrorism (Algiers Convention)*. As mentioned in Chapter 3, the *AU Non-Aggression and Common Defence Pact* provides for the establishment of the ACSRT to centralise, collect and disseminate information; studies, and analysis on terrorism and terrorist groups, provide training programs and assist Member States to develop expertise and strategies for the prevention and combating of terrorism. The Parties to the Pact are obliged to support and actively participate in the activities of the ACSRT (AU, 2005(a): Article 13). The intelligence functions of ACSRT include the following: (ISS, 2009(a))

— Assist Member States of the African Union in developing strategies for the prevention and combating of terrorism.
— Develop and maintain a database on a range of issues relating to the prevention and combating of terrorism, particularly on terrorist groups and their activities in Africa, as well as on experts and technical assistance available. This database that will include analysis, will be accessible to all Member States.
— Initiate and disseminate research studies and policy analysis periodically to sensitise Member States, based on the current trends and/or the demand of the Member State(s).
— Develop capacity for early warning to encourage early response, integrating the concept of Preventive Management of crisis.

Once again, as mentioned in Chapters 3 and 4, within SADC and the AU confusion between early warning and warning intelligence seems to exist and warning intelligence seems to be wrongly included in the concept of ‘early warning’. At the head of ACSRT is a Director reporting to the Chairperson of the Commission of the PSC, as ACSRT was established as a structure of the PSC of the AU. The Director must submit an annual report on ACSRT activities to the said Chairperson, to be considered by the policy organs of the AU. The Director

is assisted by a Deputy Director. The respective units of ACSRT are the following: (ISS, 2009(a): 9)

— The Training and Equipment Unit, responsible for organising workshops, seminars, symposiums and training programs to enhance the capacity of Member States of the AU to combat terrorism, amongst other fields in investigation; analysis and operational use of information; crime scene and forensic training; and training on the combating of terrorist financing. This Unit's functions include the distribution of surveillance equipment, equipment to detect explosives; equipment to detect forgeries as well as specialised software.
— The Alert and Prevention Unit, which has to sensitise Member States on current trends through research initiated and performed and the results disseminated by the ACSRT or upon demand by Member States. The Alert and Prevention Unit is also charged with research on converging studies on other global security challenges with links to terrorism which pose a threat to peace and security in Africa.
— From an intelligence point of view, the Data Bank and Documentation Unit can be considered as the most important. This Unit is responsible for establishing operating procedures for information gathering, processing and dissemination; the development of a databank on issues relating to the combating and prevention of terrorism, and to develop strategies to counter terrorism.

The ACSRT and the Member States of the AU interact through National and Regional Focal Points, established within the Member States and the Regional Economic Communities. The national focal points' function is to facilitate the timely exchange and sharing of information on terrorist groups and their activities on regional, continental and international levels. The ACSRT must also cooperate and develop partnerships with similar centres and other institutions involved in counter-terrorism on national, regional, continental and international levels. In this regard the EU offered its support to ACSRT to strengthen

cooperation between the two institutions, in particular through the exchange of information. The EU also undertook to provide financial support to ACSRT (EU, 2008(b): 1). ACSRT also received recognition from the UN, within the context of the new approach of the US to the combating of terrorism, as adopted by US President Obama, by "fostering a climate which is more favourable to the United Nations Strategy's emphasis on addressing the political and economic conditions that have been conducive to the spread of terrorism". It is further recognised that Africa had been the first region in the world to develop a regional counter-terrorism framework, which includes the ACSRT "to help foster regional approaches to countering terrorism." (UN, 2009(d): 1).

The AU and the ACSRT are prompted by the UN to continue to take the lead in raising awareness of the threat (of terrorism) and stimulating more information-sharing and capacity building activities on the African continent (UN, 2009(d): 1, 2). The following view has been expressed regarding UN/AU cooperation: (UN, 2009(d): 2)

> Turning to the United Nations engagement in Africa on issues of terrorism, the experts emphasized that implementation of the United Nations Global Strategy should also reflect a "bottom-up" approach, rather than being dictated by stakeholders in New York or other United Nations centres. This could be done, a number of experts suggested, through greater information sharing, more field missions and United Nations sponsored programmes for building African capacities and additional efforts to bring African voices to the work of the Security Council's Counter-Terrorism Committee and other New York initiatives.

From the above it appears as if the ACSRT is functioning more on a strategic/policy level, and not on the operational level, but that it could play an

important role with international partners to build the capacity of Member States of the AU to effectively counter terrorism.

Another organisation on the African Continent in respect of intelligence cooperation, and in particular civilian intelligence, is CISSA, discussed hereunder.

4.2. The Committee of Intelligence and Security Services of Africa

CISSA's establishment resulted from a meeting of intelligence agencies from various African countries that was held in Luanda, Angola, following the unsuccessful *coup* attempt in Equatorial Guinea (EG) in 2004. The purpose of the meeting was to discuss the rise of mercenarism in Africa (ISS, 2003 – 2006). It is understandable that the aborted *coup* had a profound effect on intelligence cooperation. Countries on the African continent have been ravaged by *coups* and *coup* attempts. Between 1964 and 2004, there had been 80 successful *coups*, 181 failed ones and an unknown number of *coup* attempts in African countries. Between 1995 and 2004 there was a marked increase in *coup* attempts in Africa (Ngoma, 2004: 87). The *coup* in the EG followed the classical pattern of many other *coups* in Africa, with ex-special forces mercenaries (Nick du Toit, ex-32 Battalion soldier, and Simon Mann, ex-Special Air Services soldier); a foreign sponsor (Sir Mark Thatcher, and allegedly Eli Calil); and an exiled politician (Severo Moto). The *coup* plot was foiled with the arrest of Nick du Toit and 18 other persons in Malabo, the capital of EG; and the arrest of a further 70 mercenaries on the airport in Harare, Zimbabwe where they were going to buy and load the arms and ammunition to execute the *coup*. Apparently the UK intelligence services were aware of the intended *coup*, months before the planned execution thereof, but did not alert the EG authorities (Sourcewatch, 2004).

Following preparations by a Commission of Experts, a *Memorandum of Understanding* was drafted setting out the procedures for Member States to join CISSA. Subsequently almost all AU Member States have signed the *Memorandum of Understanding*. As mentioned in Chapter 3 the Assembly of the AU endorsed the establishment of CISSA in Abuja, Nigeria on 26 August 2004 and directed that an Intelligence and Security Committee located in the Office of the Chairperson of the AU Commission shall be created for that purpose (AU, 2005(b). CISSA is fully functional and as also mentioned in Chapter 3, developed a Continental Threat Assessment which is updated annually and which identifies key intelligence priorities. Furthermore an Africa-wide secure communications system between the CISSA headquarters and Member States' services to facilitate intelligence exchange and interaction was established (Kasrils, 2008: 4).

CISSA was established to "carry out functions to enhance continental intelligence cooperation aimed at providing the AU, especially its PSC with data and intelligence necessary for the forecasting of future evolution and resolution of seemingly intractable conflicts that continue to threaten the stability of Africa" (AU, 2009: 1).

Membership of CISSA is open to all intelligence and security services of all African countries. It is composed of three permanent bodies, namely the Conference, which is composed of heads of intelligence and security services of Members of CISSA; the Panel of Experts, composed of the representatives from Members of CISSA, and the Secretariat based in Addis Ababa and staffed by officers recruited from intelligence and security services of Members of CISSA based on the principle of equitable regional representation. The vision of CISSA is set out as follows: "To be the primary provider of intelligence to the policymaking organs of the African Union, thereby strengthening its capacity to deepen and preserve stability in Africa" (AU, 2009: 1).

The mission of CISSA is stated as follows, namely "(t)o coordinate intelligence as well as promote cooperation, confidence building measures and capacity building among intelligence and security services of Africa" (AU, 2009: 1). In addition, CISSA's role and functions include providing a platform for cooperation with similar organisations outside Africa; to provide a back channel (in other words a secret, secure and supplementary channel) for communicating highly sensitive issues; and to enhance the development of an endogenous African Security Doctrine (ISS, 2006 – 2009: 3). The first executive secretary appointed to CISSA is Dennis Dlomo of the South African Secret Service (ANC, 2006). CISSA is certainly unique in the sense that it fosters cooperation between the civilian intelligence services of the whole African continent within the folds of the AU. Whilst CISSA is involved in the cooperation and coordination of civilian intelligence activities on the African continent, the issue of police cooperation and in particular crime intelligence cooperation in Africa, is of importance in respect of the combating of international crime.

CISSA is unique in the sense that it joins such a huge number of countries on the continent under one umbrella to enhance intelligence cooperation. In addition to civilian intelligence cooperation on the African continent, the model for crime intelligence cooperation in Africa is unique and needs to be described in more detail.

5. REGIONAL POLICE AND CRIME INTELLIGENCE CO-OPERATION IN AFRICA

Police cooperation structures in Africa provide a model of regional cooperation which could be used to globally structure regional police and crime intelligence cooperation. During the opening of the 29th ASEANAPOL Conference in May 2009, the President of INTERPOL remarked that: "INTERPOL has already seen great results from the strong cooperation between regional police chiefs' bodies in Africa and its Regional Bureaus on the (African) continent, so I encourage all

of you to make use of this valuable resource" (Hui, 2009: 4). In Chapter 3 police cooperation within the Southern African Region was discussed, providing some detail on SARPCCO – its legal basis, structures, and operations. INTERPOL has seven Regional Bureaus, of which four Regional Bureaus are based in Africa, operating from:

— Harare, Zimbabwe, serving Southern Africa and linked to SARPCCO;
— Nairobi, Kenia, serving East Africa and linked to the East African Regional Police Chiefs Cooperation Organisation (EAPCCO);
— Abidjan, Côte d'Ivoire, serving West Africa and linked to the West African Police Chiefs Cooperation Committee (WAPCCO); and
— Yaoundé, Cameroon, serving Central Africa and linked to the Central African Police Chiefs' Committee (CAPCCO).

The above Regional Bureaus of INTERPOL are serving as the permanent secretariats for the respective organisations mentioned above, providing a unique link in respect of secure communications, operational cooperation and coordination as well as direct access to INTERPOL databases and services. These Regional Bureaus have been updated and modernised since 2005, involving standardised working equipment, installation of video equipment and telephone facilities, and access to INTERPOL's Intranet and message handling system, which has speeded up the sharing of information and effectiveness among Regional Bureaus, National Central Bureaus and the INTERPOL General Secretariat (INTERPOL, 2009(j)). The respective police cooperation organisations in Africa are discussed hereunder with reference to the international crimes they focus on, the exchange of information and interaction between the respective organisations and INTERPOL. Although SARPCCO has been discussed in Chapter 3, in respect of its establishment, structures and cross-border operations, some of the latest developments in respect thereof are pointed out.

5.1. Southern African Regional Police Chiefs Cooperation Organisation

SARPCCO previously remained independent from the SADC structures, such as the Organ on Politics, Defence and Security Cooperation. In 2007, a decision was ratified by SADC Summit to bring SARPCCO "squarely under the mantel of SADC" (Van der Spuy, 2009: 245). The process of incorporating SARPCCO into SADC structures has made good progress (SARPCCO, 2009: 4). SARPCCO is dependent on Member States' contributions for cooperative ventures and although it has been successful in accessing funding from non-governmental organisations and third parties, the opinion had been expressed that it is curtailed by the absence of a dedicated budget, also in respect of the training needs of the Southern African Region (Van der Spuy, 2009: 245). The joint operations of SARPCCO in respect of the destruction of armament as a legacy of civil wars in the region as well as some other joint operations have been discussed in Chapter 3. SARPCCO in the past year focused on a variety of projects which relates to transnational crime: Project Diamante to combat crimes related to precious stones; Project Signal to establish an early warning mechanism on terrorism; and Project White Flow to combat trafficking of cocaine (SARPCCO, 2009: 5). SARPCCO also participated in the INTERPOL project to capacitate police agencies through the Operational Assistance Services and Infrastructure Support (OASIS) Africa.

A key activity of Project OASIS Africa is to provide training and tools in crime analysis, focusing on the threats to the African region of organised crime (such as stolen motor vehicles, and trafficking in human beings, drugs and illegal firearms; international terrorism and public corruption). The program is aimed at providing law enforcement officials in Africa extended access to INTERPOL's global secure communications network (I-24-7) and operational databases. In the process the mobile/fixed INTERPOL network database (MIND/FIND), also described in Chapter 3, is rolled out from the National Central Bureaus to main border points to enable law enforcement officials to carry out instant checks

against stolen and lost travel documents databases and identify criminals. Investigative tools and *ad hoc* operational support are also provided through joint police operations targeted against high-priority crime areas.

Twenty African countries, for example participated across the African continent, with some 1 250 police officers trained in using the database and relevant investigative techniques – leading to the checking of 32 000 vehicles and the arrest of more than 300 persons. The German Government is funding Project OASIS Africa for four years (INTERPOL, 2009(k): 2). The effectiveness of the OASIS Project is notable from an example of a person holding a Pakistani passport and who visited South Africa during the Confederations Cup in 2009. He claimed to be a businessman. Upon control the passport was revealed to be part of a batch of 2 000 blank passports stolen in Pakistan in 2001 (Afrol News: 2009).

Another notable SARPCCO project is the Effective Research on Organised Crime Project (EROC). The Project has entered its second year and is aimed at studying the nature of organised crime in the Southern African Region, to track its incidence and to enhance the regional response to organised crime. The EROC Project is a joint venture between SARPCCO and the Institute for Security Studies (ISS). The EROC Project includes a newsletter, based on open source information and research, and has shifted to primary data collection and field research. The EROC Project has already indicated some trends in organised crime, such as the growth of domestic drugs markets; increases in armed robberies and motor vehicle theft; the trade in endangered species; natural resources exploitation; and offences relating to the smuggling of migrants (ISS, 2009(b): 1).

It has been pointed out above that within the EU crime intelligence cooperation is to some extent supported through cooperative agreements on mutual legal assistance and extradition agreements and cooperation between crime

investigators and Eurojust. Within the SADC region, cooperation agreements have also been concluded in this regard in the form of the SADC *Protocols on Extradition and Mutual Legal Assistance in Criminal Matters*, respectively (SADC, 2002(a)) (SADC, 2002(b)). SARPCCO does provide an operational cooperation mechanism with legal support in the SADC region, but not in so far as linking with prosecutors during investigations. This is an area which could probably be addressed when SARPCCO is fully integrated within SADC structures through cooperative efforts of the SARPCCO Legal Sub-Committee and the SADC Legal Sector. The Protocols, however, still provide for rather formal processes, which do not differ much from those applicable before the conclusion of the said two Protocols. In respect of extradition for example, the principle of non-extradition of a country's own citizens is recognised. Although this can be overcome through assistance to prosecute the person in the requested country, jurisdictional issues and the making available of evidence and witnesses to another country remain challenges.

A similar police cooperation organisation has been established in respect of the Eastern African Region.

5.2. East African Police Chiefs Cooperation Organisation

The following countries comprise the East African Region: Burundi; Djibouti; Eritrea; Ethiopia; Kenya; Seychelles; Somalia; Sudan; Tanzania; Uganda; and Rwanda. Tanzania is a member of both SARPCCO and EAPCCO. The Secretariat of EAPCCO is the Regional Bureau of INTERPOL in Nairobi Kenya. The Regional Bureau Nairobi and EAPCCO focuses on terrorism; cattle rustling; environmental crime; maritime piracy off the Somali coast; trafficking in human beings and illegal migration; trafficking in narcotics; financial hi-tech crime; trafficking in firearms and fugitive tracking. One of the primary functions of the Regional Bureau Nairobi is the "preparation and dissemination of relevant information on criminal activities" (INTERPOL, 2009(l)). An international crime of

particular importance in the region is piracy. The International Maritime Bureau reported that in 2008 there were 111 attacks of piracy in the Region (Somalia/Gulf of Aden) as opposed to 148 attacks by 30 June 2009; 30 vessels were successfully hijacked by June 2009 compared with 42 vessels hijacked in 2008. Some 495 crew members had already been taken hostage by June 2009 as compared to 242 in 2008. (ICC International Maritime Bureau, 2009(a): 22) (ICC International Maritime Bureau, 2009(b): 20). This is despite the presence of war ships and the actions by the international community, referred to in Chapters 4 and 6, such as the 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 (Hanson, 2009).

From 29 to 30 June 2009, Djibouti, Eritrea, Kenya, Somalia, Seychelles, Sudan and Tanzania held a conference in a further bid to combat the crime of piracy in the seaways along the Horn of Africa. Thirty-five participants drawn from the navy, police, marine police, INTERPOL and selected legal representatives from the mentioned countries participated. The workshop was jointly organised by EAPCCO; the Hans Seidel Foundation and the ISS (Allvoices, 2009).

The police cooperation organisation for Western Africa is described hereunder.

5.3. West African Police Cooperation Committee

The INTERPOL Regional Bureau in Abidjan, Côte d'Ivoire serves 16 West African countries. Key functions of the Regional Bureau are to assess and analyse police information of relevance to the region and to provide crime intelligence, as well as to study and provide information on international crime trends in the West African Region. WAPCCO has sixteen Member States from the West African Region: Republic of Benin; Burkina Faso; Republic of Cape Verde; Republic of Côte d'Ivoire; Republic of the Gambia; Republic of Ghana; Republic of Guinea; Republic of Guinea Bissau; Republic of Liberia; Republic of

Mali; Islamic Republic of Mauritania; Republic of Nigeria; Republic of Senegal; Republic of Sierra Leone; Republic of Togo. WAPCCO was established in 1997 and held annual meetings ever since. Within the Regional Bureau: Abidjan there are five groups, focusing on respectively public security and terrorism; crimes against persons and property; traffic in human beings; economic crime; and drugs (INTERPOL, 2009(m)).

The West African Police Cooperation Organisation previously included a number of Central African Countries, but a separate organisation has recently been established to serve Central Africa in this regard.

5.4. Central African Police Cooperation Committee

CAPCCO is served by the INTERPOL Regional Bureau, in Yaoundé in Cameroon, which was officially opened in 2008. CAPCCO is constituted by Cameroon; Congo; Gabon; Equatorial Guinea; Central African Republic; Sao Tome and Principe; and Chad. CAPCCO focuses on maritime piracy; human trafficking; war crimes; trafficking in vehicles and drug trafficking. The activities of the INTERPOL Yaoundé Regional Bureau include the compilation of periodic reports on crime tendencies in the Region and crime intelligence analysis (INTERPOL, 2009(n)).

The African model for police cooperation is often referred to as the ideal model in view of the fact that the respective regional police cooperation organisations cover a huge number of countries and the fact that INTERPOL is providing secretariat services to almost all of the organisations, providing not only cohesion on the African continent, but internationally.

6. CONCLUSION

Comparing the models for national and international intelligence cooperation respectively, it is clear that the concept of intelligence-led policing is important in respect of both those levels of intelligence cooperation. It is also clear that mistrust and self-interest - in the case of national agencies linked to so-called institutional culture and unhealthy competition between agencies and on regional level, sovereignty, are inhibiting factors. In both instances agencies or states need to 'give up' such interests to either intelligence coordinating mechanisms or regional organisations for the greater good. Sovereignty nevertheless causes the establishment of independent regional intelligence organisations to be highly unlikely. Both in the EU (Europol) and on the African continent (the respective regional police cooperation organisations), crime intelligence cooperation has made huge strides through the involvement of INTERPOL either as a cooperative partner by agreement or providing secretariat services. The African regional police cooperation organisations are unique in the sense that in almost all instances INTERPOL provides such secretariat services. A lack of trust within a regional community can be partly overcome by means of clustering smaller parts of the community, such as countries with common interests together for more intense intelligence cooperation. Such clusters can then take the lead in enhancing cooperation in the community.

Within regional communities cooperation on a strategic level is also undermined by disparate capacities, creating suspicions of compromising sources and methods of intelligence, which requires screening and selective negotiated access to sensitive intelligence. Also on a strategic level, intelligence products such as those relating to organised crime and terrorist threat analysis, are hampered by the lack of input by some countries. In view of the principle of intelligence–led policing, a jointly developed threat analysis is of paramount importance in order to lead joint operations effectively and to focus resources.

As in the case with national intelligence cooperation, issues such as secure communications and security of information are of the utmost importance, as is the development of common standards. A lack of harmonisation or plain lack of legislation on intelligence powers and special investigative techniques such as surveillance and undercover operations remains a factor inhibiting the combating of international crime.

Within a regional community, joint operations to combat transnational crime are of huge importance, and tend to be highly successful in sharing operational intelligence. In this case it is also important for effective intelligence cooperation that agreements are concluded to allow a degree of flexibility for the law enforcement officers of the respective states to operate in each other's countries. The establishment of joint investigation teams, as provided for in the EUROPOL model, is of particular importance for regional intelligence cooperation within the context of the investigation of international crime.

In order to effectively combat international crime through intelligence cooperation, such cooperation needs to be enhanced by efforts to integrate intelligence cooperation with the exchange or obtaining of exhibits and evidence through mutual legal assistance, the extradition of suspects and guidance of prosecutors, as is the case with Eurojust within the EU. Specific arrangements for speedy mutual legal assistance in criminal matters and extradition are required in regional contexts, as is the case in SADC and the EU.

Regional intelligence cooperation organisations, both in respect of crime intelligence and positive intelligence, benefits largely through personnel from member states of the respective countries stationed at the respective organisations providing a spectrum of expertise and access to national agencies and their databases, through established protocols.

Regional intelligence cooperation organisations have established networks with international institutions such as INTERPOL, and the UN, providing the benefit of both regional and international cooperation. This to some extent provides a basis for military intelligence, crime intelligence and civilian intelligence cooperation. There seems, however, to be a lack on the regional level of integrating the three forms of intelligence activities. It appears as if on regional level crime intelligence and civilian intelligence cooperation respectively are well-developed, but without a structure ensuring cooperation on that level between civilian and crime intelligence. Within the EU structures such as the CitCen may play a positive role in this regard. The African model of regional police cooperation with INTERPOL providing secretariat services to all of them, and CISSA enhancing intelligence cooperation between the civilian intelligence services of most countries on the Continent, can serve as a model for other regions.

In the next chapter models of intelligence cooperation on the international level will be analysed, in particular crime intelligence cooperation through INTERPOL and the ways in which the UN as international organisation cooperates to satisfy its intelligence needs as watchdog over world peace and in relation to the combating of war crimes, genocide and crimes against humanity.

CHAPTER 8
MODELS FOR INTELLIGENCE COOPERATION ON INTERNATIONAL LEVEL

1. INTRODUCTION

In Chapter 3, the legal basis on which INTERPOL had been established, its databases, and the most important links through agreements with international organisations in respect of law enforcement, have been described. The links and relationship to police cooperation organisations on regional level were also described in Chapter 7. It is stated that operational independence is key to international organisations dealing with law enforcement. Operational independence (OI) includes the ability of such an organisation to, without restrictions by states, fulfil its mandate through developing and implementing policies and procedures: (Gerspacher, 2002: 24)

> (I)ndependence gives latitude to the IO to develop an information sharing system that truly addresses the obstacles to cooperation providing real time benefits for national competent authorities. In essence, sub-state actors such as police, custom and other law enforcement authorities should be in direct contact with the IO and have direct exposure to its systems and services, eventually bypassing the political level.

In this chapter the databases and operational intelligence support provided by INTERPOL to its members are described and analysed in more detail in order to establish the effectiveness of INTERPOL in respect of operational independence in dealing with crime intelligence in respect of international crimes. INTERPOL is not an intelligence agency in the sense that it has an independent operational

capacity for intelligence gathering within the organisation. Each INTERPOL Member State has a National Central Bureau (NCB) acting as the link between the law enforcement agencies of the relevant country and the INTERPOL General Secretariat in Lyon. However, through agreements with other organisations, such as the UN, and regional security institutions such as NATO, Europol, and the AU, which do obtain intelligence from sources other than Member States, INTERPOL can enrich its databases and add value to operational support to its members and other cooperative partners beyond the collective abilities of the INTERPOL Member States.

In respect of the UN, it has been mentioned in Chapter 4 that it has accepted the need for information and that the term 'intelligence' is no longer avoided in UN context. The ICC had been established under the UN banner with jurisdiction to investigate war crimes, genocide and crimes against humanity. As such, the investigative arm of that court is as much in need of crime intelligence as any other law enforcement agency. Intelligence and intelligence cooperation in respect of war crimes, genocide and crimes against humanity, namely crimes such as murder, slavery, extermination, torture and rape committed within the context set out in the *Rome Statute of the International Criminal Court,* has not yet been addressed in this study and will be discussed in this chapter. Mention had been made in Chapter 3 of various sanctions committees and other institutions of the UN – institutions which cannot fulfil their functions without information/intelligence beyond what can be obtained from Member States.

For the UN to fulfil its functions, the first source of information is of course from Member States, but national interests and jurisdictional barriers in many instances require the UN to collect information required to make crucial decisions regarding world peace, enforcing peace, or invoking the jurisdiction of the ICC. In addition, peacekeeping and peace enforcement forces under the banner of the UN need typical operational intelligence which can be classified as military intelligence, for their own safety and to conduct operations. In order to ensure

lasting peace, peace operations are focused on capacity building also of the law enforcement institutions in countries in a transitional process to peace, involving police officers as an integral part of peacekeeping and peace enforcement forces.

In this chapter attention is given to intelligence gathering, analysis and cooperation on a global level, in relation to the national and regional levels.

Firstly, the INTERPOL model for crime intelligence cooperation is discussed.

2. CRIME INTELLIGENCE COOPERATION AND THE INTERNATIONAL CRIMINAL POLICE ORGANIZATION MODEL

Intelligence exchange and information in respect of law enforcement is far more advanced than the case with positive intelligence, as is evident from the mere existence of INTERPOL - a mechanism for crime intelligence cooperation of which 188 countries globally are members. One of the reasons is that the combating of international crime threats is in the national interest of the international community at large. Exceptions are failed states or where states are involved in providing safe havens for criminals as a result of corruption or for political or other reasons. INTERPOL has the benefit of individual Member States contributing directly to its databases and regional crime threat analysis received from Regional Bureaus, especially in cases such as in Africa where INTERPOL provides secretariat services through its Regional Bureaus. INTERPOL also collects open source intelligence to analyse crimes as reported through the NCBs in a global as opposed to a national context; to ascertain whether available information from confidential sources are representative of the real situation; and to detect unreported elements and detect new investigative leads (Lejeune, 1999: 4). In addition, INTERPOL exchanges information with its other international partners, such as the respective UN agencies, and institutions such as the ICC.

INTERPOL is equipped in terms of its communications systems, databases, and structures to enhance and diffuse crime intelligence to its members and cooperative partners. These elements are discussed hereunder.

2.1. International Criminal Police Organization's communications-, command- and coordination systems

The respective INTERPOL databases can be accessed by all Member States through the I-24/7 communications systems linking all 188 NCBs with the INTERPOL General Secretariat in Lyon, France. The database is described as a secure global communications system communicating in real time. Some countries link the I-24/7 communications systems with all their law enforcement agencies (INTERPOL, 2008(b)). The NCBs in all 188 Member Countries of INTERPOL as well as the Regional Bureaus of INTERPOL are also linked through the INTERPOL Command and Coordination Centre (CCC), which provides a 24-hours service in all four of INTERPOL's official languages. In addition to determining the priority level of each message received and attending to it in accordance with priority, the CCC is responsible for coordinating the exchange of intelligence and information for important operations involving several countries. The CCC administers the issuing of the notices referred to hereunder on a priority basis and provides fugitive investigative support. The CCC operates on a shift basis- three shifts of teams constituted from seconded officials from Member States to INTERPOL, acting as team leaders (INTERPOL, 2008(b)).

2.2. International Criminal Police Organization's databases

The most important databases of INTERPOL to fulfil the need of the police to combat international crime are: The MIND/FIND, which has been mentioned briefly in Chapter 2, and will be discussed hereunder in more detail; data on suspected terrorists; nominal data on criminals (names and photos); fingerprints;

DNA profiles; lost or stolen travel documents; child sexual abuse images; stolen works of art; stolen motor vehicles; the INTERPOL Weapons electronic Tracing System (IWeTS) and the INTERPOL Money Laundering Automated Tracing System (UN, 2009(a)) (INTERPOL, 2008(c)) .

2.3. International Criminal Police Organization's notices system

Requests for assistance from Member States of INTERPOL are used to generate a number of notices in the official languages of INTERPOL. Similar notices are also used by international tribunals and the ICC to bring to justice persons wanted for genocide, war crimes and crimes against humanity. In addition NCBs may use INTERPOL's I-24/7 communications system to send a diffusion, which is a message concerning a wanted person immediately and directly to other NCBs without the involvement of the General Secretariat. Minimum criteria in respect of information submitted to INTERPOL must be met before INTERPOL will communicate a notice to the NCBs. INTERPOL describes the notices as follows: (INTERPOL, 2008(e))

— Red Notice: To seek the arrest or provisional arrest of wanted persons with a view to extradition.
— Yellow Notice: To help locate missing persons, often minors, or to help identify persons who are unable to identify themselves.
— Blue Notice: To collect additional information on a person's identity or activities in relation to a crime.
— Black Notice: To seek information on unidentified bodies.
— Green Notice: To provide warnings and criminal intelligence about persons who have committed criminal offences and are likely to repeat those crimes in other countries.
— Orange Notice: To warn police, public entities and other international organisations of disguised weapons, parcel bombs and other dangerous materials.

— INTERPOL-UN Special Notice: Issued for groups or individuals who are targets of UN sanctions against Al Qaeda and the Taliban.

INTERPOL maintains a public wanted fugitive list, which represents a small proportion of the full list of wanted persons, available to NCBs.

2.4. Crime intelligence analysis structures of International Criminal Police Organization

The Specialised Crime and Analysis Directorate of INTERPOL has a Sub-Directorate: Crime Analysis (CAS) which provides analytical support to units in the General Secretariat and also to Member States, upon request. Currently 11 criminal intelligence analysts, from different nationalities are based at the INTERPOL General Secretariat in Lyon, and three such analysts based in the Sub-Regional Bureaus at Buenos Aires, San Salvador and LoBang. The relative independence of INTERPOL from its Member States is hugely strengthened by INTERPOL's relations with other international and regional organisations, some of which have been listed in Chapter 3. More information on these agreements is provided hereunder.

2.5. International Criminal Police Organization's agreements with other international and regional organisations

The conclusion of cooperation agreements between INTERPOL and international organisations with the combating of various international crimes as their aim, is an ongoing process. INTERPOL has concluded cooperation agreements, in addition to the agreements with ASEANAPOL, Europol, and Frontex, with the Caribbean Community (CARICOM), which was signed on 19 March 2009); the Regional Security System (an intergovernmental organisation consisting of seven Carribean States), which came into force on 16 March 2007); the Caribbean Customs Law Enforcement Council which came into force on 22 October 2004; the Anti-Terrorism Centre of the Commonwealth of Independent States (signed

on 17 December 2008); the International Maritime Organisation which came into force on 20 February 2006); the General Secretariat of the Andean Community which came into force on 21 January 2003; the AU, which came into force on 28 September 2001; and the Organisation of American States (OAS) which came into force on 2 May 2000 (INTERPOL, 2008(a). The agreements indicated above as being signed, have not come into force yet. Standard to most of these agreements are provisions providing for the exchange of information; reference to the rules and regulations governing the confidentiality of the exchange of information; the communication of information being exchanged; and verification of and ensuring the validity and updating of exchanged information. INTERPOL's agreements with regional organisations provide an almost global network for intelligence cooperation in terms of regional organisations.

The unique arrangements between INTERPOL and its Regional Bureaus in Africa have been referred to in Chapter 7. Some INTERPOL Member States in Africa are still not included in the areas of responsibility of the Regional Bureaus in Africa. Understandably cooperation between INTERPOL and its regional partners are not on the same level as in the regions where INTERPOL provides secretariat services, as is the case in Africa. Although INTERPOL has not concluded agreements with regional civilian intelligence organisations such as CISSA in Africa and CitCen in the European Union, it has concluded agreements with regional organisations such as the EU, and AU, which have within their structures organisations with the aim of cooperation on civilian intelligence. The reason for this is probably to be found in Article 3 of the INTERPOL Constitution, which strictly forbids INTERPOL to undertake any intervention or activity of a political, military, religious or racial character.

2.6. International Criminal Police Organization's role in respect of intelligence cooperation on war crimes, genocide and crimes against humanity

Cooperation between INTERPOL and the UN in respect of "carrying out investigations and other police-related matters in the context of peacekeeping and similar operations" dates back to before the conclusion of an agreement in that regard in 1997. A number of other agreements have also been concluded between INTERPOL and UN established structures to facilitate cooperation in respect of *inter alia* international humanitarian law. These agreements are discussed hereunder.

2.6.1. Agreement between International Criminal Police Organization and the United Nations

This agreement serves to further strengthen cooperation which stretched over years between INTERPOL and the UN in the field of crime prevention and criminal justice. The scope of cooperation in terms of the agreement relates to investigation of contraventions of international humanitarian law (war crimes, genocide and crimes against humanity), in particular in the former Yugoslavia and Rwanda; and cooperation in response to international threats in respect of national and transnational crime. Particular reference is made to the combating of activities of organised criminal groups in the form of money-laundering, illicit trafficking in human beings and drug trafficking. The agreement provides for consultation and cooperation, exchange of information and documents, technical cooperation, exchange of personnel and joint representation in the respective organisations. The agreement gives specific recognition to the UN Commission for Crime Prevention and Criminal Justice's Crime Prevention and Criminal Justice Division as the only office within the UN Secretariat with responsibilities in respect of crime prevention and criminal justice. A number of agreements were concluded to promote cooperation between INTERPOL and international

tribunals established by the UN Security Council. These agreements are discussed hereunder.

2.6.2. Agreements between International Criminal Police Organization and specific tribunals

The first of these agreements was concluded in 2002 with the UN Mission in Kosovo (UNMIK) in support of the International Criminal Tribunal for the former Yugoslavia (ICTY). In this agreement INTERPOL and UNMIK agreed on full and prompt exchange of 'police information'. UNMIK had to designate in terms of the agreement within its offices a contact point which would perform the same functions normally assigned to an NCB, and that contact point would have the same rights as an NCB, including the right to circulate diffusions to the INTERPOL General Secretariat as well as to NCBs of INTERPOL Member States. UNMIK was also allowed access to INTERPOL databases and to use INTERPOL communications systems. INTERPOL agreed to circulate notices, including Red Notices through its system for arrest warrants issued by the ICTY (INTERPOL, 2009(b)).

A similar agreement, but limited to the exchange of "police information and circulation of notices, including Red Notices and arrest warrants" by INTERPOL on its system, was concluded in 2003, with the Special Court for Sierra Leone. The Special Court's warrants received preference over those issued by national courts in Sierra Leone (INTERPOL, 2009(c)). An Interim Agreement between INTERPOL and the Special Tribunal for Lebanon was concluded in August 2009, which provides only for cooperation between INTERPOL and the Special Tribunal for Lebanon on a 'case-by-case' basis (INTERPOL, 2009(d)).

Since the adoption of the *Rome Statute of the International Criminal Court* in 1999, the ICC, despite having only complementary jurisdiction to national jurisdictions, has become active in the prosecution of war crimes, genocide and

crimes against humanity. A cooperation agreement between the Office of the Prosecutor, who in terms of the *Rome Statute of the International Criminal Court* is also in charge of investigations for the ICC, and INTERPOL came into force on 20 February 2005. The agreement provides a framework for cooperation between the ICC and INTERPOL "in the field of crime prevention and criminal justice, including the exchange of police information and conduct of criminal analysis, the search for fugitives and suspects, the publication and circulation of INTERPOL notices, the transmission of diffusions and access to INTERPOL telecommunications network and databases". Provision is made that information received from INTERPOL Member States may be provided to the Office of the Prosecutor on the basis that it will not be disclosed without the express written consent of the provider of the information. As mentioned in Chapter 2 some of the major powers such as the US, the Russian Federation and China, are not Party to the *Rome Statute of the International Criminal Court.* The Office of the Prosecutor may also request through INTERPOL, the assistance of relevant national teams such as national Disaster Victims Identification Teams or war crimes units. INTERPOL must approve the hardware, software and services used by the Office of the Prosecutor to access INTERPOL databases, and communications lines must be secured by the Office of the Prosecutor. Police information may only be forwarded by the Office of the Prosecutor to approved addressees under the same conditions as supplied by INTERPOL (INTERPOL, 2009(e)). In the next sub-section, the role of INTERPOL in intelligence cooperation in respect of terrorism, organised crime; mercenary crimes; crimes relating to the proliferation of WMD and piracy will be discussed.

2.7. International Criminal Police Organization's role in intelligence cooperation on terrorism, organised crime; mercenary crimes; crimes relating to the proliferation of WMD and piracy

Before INTERPOL's role in intelligence cooperation in respect of terrorism, organised crime; mercenary crimes; crimes relating to the proliferation of WMD

and piracy can be discussed, the issue of the convergence of international crime needs to be elaborated upon.

2.7.1. The convergence of international crimes

At the most recent General Assembly of INTERPOL, 60 ministers from around the world supported a plan of action to promote international police peacekeeping as an essential counterpart to the military in helping re-establish the rule of law and rebuild conflict-ridden societies. The aim is that police peacekeepers must assist to rebuild failed states, and to promote good governance and sustainable peace. Of particular importance is that INTERPOL undertook to make its communications systems and databases available to police peacekeepers, not only for peacekeeping purposes, but in view of the realisation that there is a link between conflict and organised crime as there is a link between failed states and safe havens for terrorists: “Criminal elements are increasingly fuelling wars by providing belligerents with the resources to finance expensive military activities” (INTERPOL, 2009(i)). It is becoming increasingly clear that in the Gulf of Aden and Somalia, there is not only a link between piracy and terrorism, but also a link between organised crime and piracy. INTERPOL officials recently announced that organised crime syndicates are behind the piracy attacks and in particular the huge amounts of ransom money obtained through hijacking of vessels off the Somali coast (Abbugao, 2009).

There are at least eight areas of similarity between terrorism and organised crime: (Makarenko, 2002: 8)

— The use by both organised crime and terrorists of networks and cell-based structures;
— the national- regional and transnational nature of both;
— both require safe havens and take advantage of ‘diaspora communities’;
— both groups use similar targeting and deployment techniques and have sophisticated intelligence and counter-intelligence capabilities;

— both have “a programme of government and public relations”; and
— both organised crime and terrorism are dependent on external funding.

The characterisation of the interaction between organised crime and terrorism is important to provide law enforcement and intelligence agencies with actionable information, to focus investigations, improve warning time and reveal vulnerabilities (US, 2005(d), 2005: 23). Both military and civilian analysts have been using the technique of “Intelligence Preparation of the Battlefield (IPB)” to accomplish the above goals in their area of interest. The common areas between organised crime and terrorism have been utilised to develop a similar technique in respect of crime intelligence analysis, referred to as “Preparation of the Investigative Environment (PIE)”. In terms of PIE some 12 ‘watch points’ or ‘indicators’ have been identified to serve as a focus for crime intelligence analysis. The nature of these watch-points is such that it should serve as the focus of crime intelligence cooperation. As was pointed out above, there is also an overlap or convergence between piracy and terrorism and even conflict and organised crime. Although it is not deemed necessary to go into the full details of these watch points, an outline thereof needs to be provided as this could be used in especially a draft instrument on intelligence cooperation for which a need has been expressed as mentioned in Chapter 5.

It is also important to establish whether the databases of INTERPOL, for example relate to these ‘watch points’: (US: 2005(d): 45 – 58)

(a) Watch Point 1. Open activities in the legitimate economy: Terrorists, criminals involved in organised crime, and indeed criminals involved in all international crimes, on an operational level, need to carry out legitimate transactions, including to buy food, clothing, specialised equipment, computers, rent apartments, buy plane tickets, obtain visas and passports and open bank accounts. Crime intelligence therefore needs to focus on travel information, mail and courier services, customs transactions and

documents and companies or legal entities which could possibly serve as front companies.

(b) Watch Point 2. Shared illicit nodes: These are of particular importance in countries with effective law enforcement where activities of criminals need to be covert, as opposed to lawless countries or failed states where criminal activities can be more overt. Illicit nodes include obtaining forged passports, drivers' licences and fraudulent documents; obtaining the assistance of dishonest accountants and bankers for money laundering or money transfers; illegally obtaining firearms and explosives; and setting up training camps and safe houses.

(c) Watch Point 3. Communications. Criminals involved in organised crime and terrorism have a need to communicate, and have realised the value of encrypted communications. Elements within organised crime open their encrypted communications systems to whoever can pay, including terrorist groups. In the Tri-Border region of South America clandestine telephone exchanges connected with *Jihadist* networks were found. There may also be overlaps where both organised criminals and terrorists use the same high tech crypto specialists and couriers.

(d) Watch Point 4. Use of information technology (IT): In view of the relative anonymity offered by digital transactions, online transactions are used by organised crime to commit crime, whilst terrorists use it for fundraising. In this instance the same technical experts are also often shared between organised crime and terrorists.

(e) Watch Point 5. Violence. Although no indicators have been developed in this regard, it is not excluded that indicators may be developed, such as the hiring by both organised crime and terrorists of the same persons to perform for example assassinations.

(f) Watch Point 6. Corruption. Especially in failed states or states where law enforcement is less effective, corrupted law enforcement officers, judiciary, border guards, politicians, or internal security agents may be abused by both terrorists and organised crime groups.

(g) Watch Point 7. Financial transactions and money-laundering: The indicators in this regard are shared methods of money-laundering and mutual use of front companies, as well as financial experts.

(h) Watch Point 8: Organisational structures. Persons involved in organised crime such as drug trafficking have been recruited by terrorists, whilst terrorists often act as suppliers of arms and ammunition especially in some conflict areas. Terrorists often supply drugs to finance their operations.

(i) Watch Point 9: Organisational goals. Whilst terrorists usually pursue political or religious goals, and criminals involved in organised crime pursue personal profit, in some countries both groups could share a strong dislike of “those in power, of legislation and regulation and the economic system” and consequently would cooperate to attain success.

(j) Watch Point 10. Culture: The manner in which culture links and strengthens relationships within any organisation, as well as how culture could link criminal networks to each other, is the focus in this watch point. Indicators in this regard could be religion, shared nationalism of suspects and their relationship with particular societies.

(k) Watch Point 11. Popular support: Both terrorist groups and organised criminal groups often appeal to disadvantaged groups in order to gain popular support.

(l) Watch Point 12. Trust: Both organised criminal groups and terrorist groups use initiation rituals and ‘tests of allegiance‘, in order to ‘test’ the trust that can be placed in their members.

In the following section, the role of INTERPOL in intelligence cooperation in respect of terrorism, organised crime; mercenary crimes; crimes relating to the proliferation of WMD and piracy is discussed.

2.7.2. International Criminal Police Organization's role in intelligence cooperation on terrorism

INTERPOL established the Fusion Task Force (FTF) in 2002, with counter-terrorism specialists from Member States serving on the FTF. Six regional FTF's have been established in regions most "susceptible to terrorist activities", namely South East Asia, Central Asia, South America, Africa, Europe and the Middle East. The objectives of the FTF include the identification of active terrorist groups and their membership; to solicit, collect and share intelligence; and to provide analytical support to Member States. INTERPOL cooperates with the UN (see for instance the notices relating to the lists of suspected Taliban and Al-Qaida terrorists circulated by INTERPOL). INTERPOL also maintains a secure website with information on meetings of the FTF, analytical reports, photo-boards of suspected terrorists, notices and diffusion lists. The FTF has built a network of over 200 contact persons in 100 countries (INTERPOL, 2008(f)). INTERPOL has issued guidelines to Member States regarding the reporting of information to INTERPOL on terrorism, including information on other crimes which may be linked to terrorism such as suspicious financial transactions, weapons trafficking, money-laundering, falsified travel and identity documents, and seizure of nuclear, chemical and biological agents (INTERPOL, 2008(g)). It can be argued that the above watch-points are relevant to all international crimes, as war criminals, especially top politicians often become fugitives, utilising fraudulent passports and also the financial system to move funds to sustain themselves.

2.7.3. International Criminal Police Organization's role in intelligence cooperation on organised crime

INTERPOL assists 188 countries to monitor and analyse information relating to specific activities and criminal organisations; to identify major crime threats with potential global impact; and to evaluate and exploit information received from NCBs, law enforcement agencies, open sources, international organisations and

other institutions. INTERPOL also monitors open source information and reports and provides support in ongoing international investigations on a case-by case basis. This cooperation enables INTERPOL to identify links between transnational crime investigations which would not otherwise have been possible and to follow such links up with special projects, such as targeting Eurasian and Asian criminal organisations. INTERPOL acts as a clearinghouse for the collection, collation, analysis and dissemination of information on organised crime and criminal organisations. It also monitors the organised crime situation on a global basis and coordinates international investigations.

Part of INTERPOL's mission is to "stimulate the exchange of information between all national, international enforcement bodies concerned with the countering of organized crime groups and related corruption" (INTERPOL, 2008(h)). Money-laundering is interlinked with organised crime and in this regard the INTERPOL Money-Laundering Unit sifts through thousands of messages received from Member States to notify investigators of previously unknown links. The Anti-Money-Laundering Unit is dedicated to improve the flow of money-laundering information amongst financial investigators by forging alliances with financial intelligence units and financial crime units around the world. As with the FTF, liaison officers have been identified around the world to act as national contact officers regarding money-laundering investigations (INTERPOL, 2008(i)).

2.7.4. International Criminal Police Organization's role in intelligence cooperation on mercenary crimes

INTERPOL does not have a specific focus on intelligence or information relating to mercenary activities other than the overlap that might exist between terrorist activities and mercenary actions. The reason for this are the deficiencies in the international framework relating to mercenaries, set out in Chapter 2; that few countries have strengthened their national legal frameworks to combat mercenary crimes; and that private military companies find it easy to evade those

domestic acts that do exist. In view of the fact that so many states actively rely on private military companies enough political support to effect what is logically needed, namely an international ban on private military companies is improbable (Gaston, 2008: 240, 241). There are steps to improve the regulation of private military companies, but without strengthening the international legal framework regarding mercenaries, international intelligence cooperation in respect of mercenary crimes will probably remain limited to the African continent where the need for such cooperation has been a catalyst for the establishment of CISSA.

2.7.5. International Criminal Police Organization's role in intelligence cooperation on the proliferation of weapons of mass destruction

INTERPOL, in addition to activities in respect of both terrorism and organised crime in so far as it relates to WMD, has concluded an agreement with the primary UN watchdog relating to nuclear proliferation and regulation, the IAEA. More information on the IAEA will be provided in this chapter. The agreement provides for cooperation between INTERPOL and the IAEA to exchange and use information, including information relating to illicit trafficking and relevant to the nuclear security regulatory infrastructure for the prevention of nuclear terrorism and illicit trafficking in nuclear and other radio-active materials; and also to most effectively utilise their resources in the collection, analysis and diffusion of the information referred to above (INTERPOL, 2009(f)).

2.7.6. International Criminal Police Organization's role in intelligence cooperation on piracy

INTERPOL hosted a meeting of the Maritime Piracy Working Group, in September 2009, with the purpose of increasing information sharing among Member States and also with the General Secretariat of INTERPOL on maritime piracy issues in order to further support Member States in their investigations, and to enhance cooperation between military and police forces. INTERPOL

actively liaises with some 12 organisations including the United Nations Office on Drugs and Crime (UNODC), Europol, the International Maritime Organisation and the International Maritime Bureau on the issue of piracy, which is regarded as a form of organised crime (INTERPOL, 2009(h)). INTERPOL has also concluded an agreement with the International Maritime Bureau on the exchange of information on piracy and maritime safety (INTERPOL, 2009(g)).

INTERPOL is fast progressing in improving crime intelligence cooperation in respect of all international crimes, with the exception of mercenary crimes. As pointed out in the previous chapter its Regional Bureaus in Africa are of particular importance. There is still scope for expanding regional offices of INTERPOL on the same basis as in Africa. INTERPOL is well connected with relevant regional and international organisations dealing with crime. It is gaining more and more independence as an organisation, contributing to its effectiveness. Although it cannot be regarded as an independent intelligence agency, the General Secretariat does at least gather open source intelligence independently, and it can source information through its international partners which is far more than the collective input from the NCBs of its Member States. It not only serves as a communications and dissemination tool for law enforcement on a global basis, but independently analyses information received, which leads to joint operations between Member States.

There is clearly a need to further build on INTERPOL's independence. Article 3 of INTERPOL had not really been a stumbling block in combating crimes with a political motive such as terrorism, as a result of the fact that terrorist crimes are captured in various international instruments which alleviates the lack of an universally accepted definition of terrorism. INTERPOL's databases and intelligence cooperation to a large degree reflect the 'watch points' set out above in order to generate and distribute actionable intelligence to combat international crime. It is clear that there is a high degree of trust in INTERPOL as organisation, although it had been pointed out in Chapter 1 that Member States do not always

utilise INTERPOL databases sufficiently. Although it was indicated that INTERPOL wishes to enhance cooperation between police and military forces in respect of the combating of piracy, there is in view of Article 3 of the INTERPOL Constitution no formal relation between INTERPOL and civilian or military intelligence organisations and it is highly improbable that this will develop. Cooperation between positive intelligence and crime intelligence therefore will be the strongest on national level, and takes place to some extent in regional organisations such as the EU, and AU on a limited scale. The links between INTERPOL and the UN as an international organisation which needs and uses intelligence has been mentioned.

It is, however, necessary to establish how the UN deals with intelligence. The UN requires positive intelligence for peacekeeping operations, which is received to some extent from the Member States, involved in these operations, but is also generated by the UN peacekeeping missions. Crime intelligence required for decision-making processes of the UN to invoke the jurisdiction of the ICC, or for the prosecution of war crimes, genocide and crimes against humanity is mostly gathered by *ad hoc* institutions such as international commissions of inquiry or special missions set up to investigate transgressions of the *Rome Statute of the International Criminal Court*. Crime intelligence cooperation takes place through the UN's international partners, such as INTERPOL, and independent agencies such as the IAEA.

3. UNITED NATIONS INTELLIGENCE ACTIVITIES AND COOPERATION

In Chapter 3 it was pointed out that the UN needs intelligence for peacekeeping and peace enforcement, for the safety of UN forces, as well as effectively performing its peacekeeping operations. The UN Situation Centre was referred to, as an instrument in this regard as well as the fact that various methods are used to gather intelligence for the UN. In this chapter it was also pointed out that

the role of peacekeeping forces are expanded to empower police components as permanent features of peacekeeping forces and that they are empowered to also play a role in combating international crimes which impact negatively on peace processes. The UN plays a huge role in respect of the application of international criminal law, especially through sanctions of the UN Security Council, which need to be enforced not only on the diplomatic level, but practically through the national laws adopted by countries to combat the proliferation of WMD; assistance to terrorist members, organisations and associates; and the illicit trade in conventional arms to countries subject to such sanctions. In addition, though the ICC has only complementary jurisdiction to the jurisdiction of national courts in respect of war crimes, genocide and crimes against humanity, it remains the principal court in which such crimes are being prosecuted.

The UN has two areas of intelligence activities in this regard, firstly to lay a basis for a resolution by the UN Security Council to invoke the jurisdiction of the ICC in respect of a particular country; and secondly the investigation of war crimes, genocide and crimes against humanity, which is tantamount to crime intelligence gathering by the investigation authority of the ICC, namely the Chief Prosecutor thereof, in order to be able to prosecute cases. In Chapter 4 it was only mentioned that the structures of the UN in this regard are bureaucratic. The methods and structures employed by the UN to obtain the required intelligence for the above purposes are described hereunder, with particular reference to the complicating factor of sovereignty and self-interest of states. The first area that is elaborated upon is the gathering of intelligence in respect of the enforcement of international obligations and UN sanctions in respect of the proliferation of WMD.

3.1. Intelligence support of the United Nations to enforce compliance with international obligations and United Nations sanctions relating to weapons of mass destruction

The first enforcement issue that is described is the combating of the proliferation of WMD. Mention has been made in Chapter 2 of Resolution 1540 of the UN Security Council in respect of the obligations on Member States of the UN to combat the proliferation of WMD as well as crimes that need to be adopted in national statutes in respect thereof. The 1540 Committee was established by the UN Security Council to monitor the implementation of the Resolution by Member States. The focus of the Committee is, however, more on the promotion of the implementation of the Resolution through encouraging Member States to become party to the relevant international instruments and to adopt and implement national legislation to give effect to those instruments, than on crime intelligence in respect of transgressions of non-proliferation legislation (UN, 2008(f): 6). In respect of enforcement on a more practical level, also of sanctions of the UN Security Council, the UN relies on two organisations in respect of the combating of the proliferation of WMD, namely the Organisation for the Prohibition of Chemical Weapons (OPCW) in respect of the Chemical Weapons Convention (CWC) and the IAEA in respect of the combating of the proliferation of nuclear weapons in terms of the Non-Proliferation Treaty (NPT). The UN Security Council sanctions on providing any assistance relating to nuclear arms and material, such as those against the Democratic People's Republic of Korea, in effect determines the scope of application of national laws to combat the proliferation of WMD (UN, 2009(f): 3). The OPCW staff complement consists of less than 500, which includes 150 inspectors who are trained and equipped to inspect military and industrial facilities in the 188 Member States who are party to the CWC (Sweden, 2006: 129).

The UN has concluded a special agreement with the IAEA to report annually to the UN General Assembly and when "appropriate" to the UN Security Council

regarding non-compliance by states as well as "on matters relating to international peace and security" (IAEA, 1959). The IAEA Secretariat consists of a staff of 2 200 multi-disciplinary professional and support staff from more than 90 countries. It is an independent organisation related to the UN System ("in the UN family") (IAEA, 2009(a)). The agreement between the UN and the IAEA provides for the 'fullest and promptest' exchange of appropriate information and documents between the two institutions. Both institutions also have the reciprocate obligation to furnish 'studies or information' upon request to each other (IAEA, 1959: Article VII). In respect of the proliferation of WMD, in particular access to nuclear material by terrorist groups, the IAEA and the UN's role is more of a preventive nature. Libya's actions in its quest for constructing nuclear weapons were exposed through intelligence actions and eventually solved through diplomacy and political pressure (Sweden, 2006: 66). The IAEA is in an ongoing process of installing digital surveillance systems and unattended monitoring systems, and to expand its capabilities to transmit data directly from the field for monitoring and evaluating in its headquarters or regional offices (IAEA, 2009(b)). The IAEA is primarily dependent on intelligence from its members and other members of the UN. Western intelligence agencies, for example, during 2005, were providing the IAEA with documentation of suspected Iranian nuclear weapons-related activities, with the *caveat* that these documents may not be shared with Iran.

One of the constraints in this regard is that the IAEA must be careful not to compromise sensitive military information during its investigations- in the Iranian investigation Iran claimed that its experiments with high explosives and work on its ballistic missile programme are "solely related to its conventional military capabilities". Iran therefore claimed that the investigation could jeopardise military secrets. Intelligence received from members of the IAEA or from national intelligence agencies, should such intelligence indicate non-compliance with non-proliferation measures, may prompt site visits to the country in question. Such site visits of IAEA inspectors include taking swabs for forensics testing for the

presence of nuclear material. The cooperation of the country visited is important as is evident from how IAEA inspectors were frustrated in site visits to Pakistan's Kalaya Electric installation (Frantz & Collins, 2007: 285). The following observation has been made about the intelligence cooperation between national intelligence agencies and international inspectors, with reference to Iraq: (Sweden, 2006: 172, 173)

> National intelligence agencies may acquire information through such means as electronic and aerial surveillance, export controls and intelligence gathering. Their need to protect sources and techniques sets limits on the information they can provide international inspectors. Nevertheless it is clear that national intelligence services can greatly assist international inspection by providing important information…However, it is crucial that this remain a one-way street. Inspectors and inspections must not become the extended arms of intelligence services – otherwise as experience has shown, they will loose their credibility and international respect.

It has been recommended that the UN Security Council should set up a small technical unit, parallel to the IAEA, to provide it with professional technical information and advice on WMD and be available to organise *ad hoc* inspections in states as well as monitoring in the field. The UN Security Council has the power to authorise intrusive fact finding missions in Member States and also to authorise even military action to be taken in appropriate cases, and the effectiveness of such a unit would probably be higher than that of the IAEA (Sweden, 2006: 174, 176, 203). The fact that the IAEA inspection teams cannot force Member States to provide access and to cooperate, results into dependence on the goodwill of the countries visited. For that reason, intelligence collected or obtained from other sources remains of cardinal importance to the IAEA. The IAEA is dependent on extra-budgetary assistance from Member

States such as the US, and in view further of what is referred to as the IAEA's 'ageing staff', doubt has been expressed about the IAEA's abilities to perform its fundamental mission as the world's nuclear watchdog to detect the illicit diversion of nuclear material and discovering clandestine activities associated with weapons programmes (US, 2008(d): 45).

It has been argued that the *ad hoc* use of intelligence processes by a small number of IAEA Member States has been inadequate to curb the black market activity in nuclear materials. Intelligence functions, namely analysing open-source intelligence and assessing imagery are performed by two units of the Safeguards Information Management Directorate of the IAEA, whilst there are allegedly no technical personnel in the unit responsible for the investigation of illicit trafficking in nuclear material. An ex-employee of the IAEA's intelligence branch, Mowatt-Larssen proposed that the IAEA should establish a more productive intelligence unit with about a dozen investigators with "a professional intelligence background". He, however, made it clear that such collection should be based on open-sources and not through clandestine activities. Concern has at the same time been expressed of the risk of exposure of state secrets and that the IAEA does not have a security culture in respect of the protection of information (Grossman, 2009: 2, 5, 6).

3.2. United Nations intelligence activities in respect of the combating of terrorism

In Chapter 3, as well as in this chapter, reference has been made to the listing in terms of Resolution 1267 of the UN Security Council of suspected Taliban and Al-Qaida terrorists and associates. The listing process in the UN Security Council, through the Resolution 1267 Committee, places the UN Security Council in the operational arena, in that the persons or entities thus listed are subject to travel bans, sanctions on access to weapons, as well as subject to asset freezing and must be denied any financial assistance or banking facilities. The listing

takes place following a statement of case by the applicant Member State to the UN Security Council. The problem has arisen that the protection of sources is of particular importance in counter-terrorism work. The proposed listing of a person or entity is often based on confidential information or information subject to national security classification. States are reluctant to allow foreign nationals access to their secret information and even more so to allow the examination of the veracity of those sources. There is a danger that the authority of the UN Security Council may be eroded if Member States act in contravention of their national laws (if there is a lack of information to substantiate not only the listing, but to support administrative and legal action to enforce the UN Security Council sanctions applicable to listed persons or entities). The possibility of appointing a review committee outside the UN Security Council to review such a listing has been mentioned (UN, 2009(b)).

3.3. Intelligence relating to war crimes, genocide and crimes against humanity

In terms of the *Rome Statute of the International Criminal Court,* the ICC shall *inter alia* have jurisdiction if a situation in which one or more war crimes, crimes relating to genocide or crimes against humanity, appear to have been committed, is referred to the Prosecutor of the ICC by the UN Security Council acting under Chapter VII of the Charter of the UN (UN, 1999 – 2003 : Article 13(b)). The UN Security Council, in order to adopt a resolution for such referral needs information, comparable to crime intelligence, collected by an independent institution. The mechanism used for such investigation is by means of an international commission of inquiry set up by the Secretary General under the authority of a UN Security Council Resolution under Chapter VII of the *Charter* of the UN. The International Commission of Inquiry on Darfur, set up in terms of Resolution 1564 (2004) to inquire into reports of violations by all parties in Darfur of the IHL and Human Rights Law and to identify the perpetrators is an example in this regard. This Commission of Inquiry clearly illustrates the challenges faced

in obtaining the relevant information as well as the sources thereof. One of the major challenges is that the government security forces, including the defence, law enforcement and intelligence agencies of the Sudan have been the subjects of the Commission of Inquiry.

There were, however, a number of other challenges. Reports of the UN, Human Rights Groups and Non-Governmental Organisations (NGO's) were primary sources of information for the International Commission of Inquiry. The Commission, however, had to independently verify the reports. The sheer number of incidents reported required a proper prioritisation by the Commission based on incidents most representative of acts, trends and patterns of the alleged transgressions of the IHL and human rights law, with greater possibilities of fact-finding. Access to sites of incidents; protection of witnesses; and the potential for gathering the necessary evidence, were major considerations to select particular sites (UN, 2005(b): 61).

Some of these reports contained satellite imagery which documented systematic and widespread destruction of entire villages. This evidence was confirmed by site-visits where the Commission witnessed the destruction. This was further corroborated by eyewitnesses (UN, 2005(b): 81, 82). Eyewitnesses also described their attackers, according to the uniforms, weapons, physical appearance and language as the Janjaweed, government sponsored agents; or soldiers who intimidated, raped, abducted or killed civilians in Darfur (UN, 2005(b): 88, 94). During visits to the Sudan, the Commission interviewed victims, eye-witnesses, government officials, soldiers, Internally Displaced Persons (IDPs), NGOs and UN officials. This includes interviews with witnesses who fled to Chad (UN, 2005(b): 13). The Commission became aware of interference with witnesses by government agents; the placing of infiltrators between the IDPs; the offering of money not to agree to be interviewed by the Commission; and harassment and threat of injury or death (UN, 2005(b): 16).

The Commission decided to keep confidential the names of both identified perpetrators and witnesses, especially for protection of the witnesses (UN, 2005(b): 133, 134). Most witness statements were taken in confidentiality and were unsigned. Police reports, judicial decisions and hospital records as well as records of burial sites were kept by the Commission (UN, 2005(b): 134). The Commission has not been vested with investigative or prosecutorial powers, nor could it make any finding on criminal guilt. Its function, however, was to pave the way for future investigations, and possible indictments by a prosecutor and convictions by a court of law (UN, 2005(b): 134, 161). The Commission performed its inquiry in strict confidentiality and avoided interaction with the media (UN, 2005(b): 11).

The Commission's efforts to gain access to minutes and documentation of the Government of Sudan's security institutions on the use of force against rebels and the civilian population were unsuccessful and the Commission was provided only with selected final decisions on general issues, despite reliable information of the existence of minutes in that regard. A full set of records on the use of aircraft or helicopters used by the Sudanese security forces, could also not be obtained from the Government of Sudan (UN, 2005(b): 16). The Commission had to perform its inquiry during ongoing conflict in Darfur.

More recently, a somewhat different approach as with the above UN Commission of Inquiry, in respect of Darfur, was followed into the alleged war crimes committed in Gaza, during Operation Cast Lead, launched between 27 December 2008 and 18 January 2009, by the Israeli military in response to missile attacks by Hamas. In the Gaza case, the UN Security Council appointed and mandated a UN Fact Finding Mission to investigate the relevant events. The fact that it is called a UN Mission, linked with the fact that the secretariat for the mission was established by the UN High Commissioner for Refugees, underlined the diplomatic status and immunity of a UN Mission (UN, 2009(c): 5). The Mission utilised in some respects the same sources of information as the

Commission of Inquiry in Darfur, in order to compile its report to the UN Security Council, such as field or site-visits where incidents occurred; the review of reports from different sources, including NGOs; human rights organisations, academics and analysts and other UN organisations; and obtaining witness statements.

The Mission, however, also called for written submissions from the public and held public hearings in Gaza, and in order to reduce the possibility of intimidation or influencing of witnesses, public hearings were in addition held in Geneva. As in the case of Darfur, the names of victims and perpetrators were generally not mentioned in the report. The Mission also obtained forensic analysis of weapons and ammunition remnants collected at incident sites; held meetings with a wide range of interested parties. Interviews were conducted, (some by telephone) both with witnesses and persons in possession of relevant information, and some in private. Medical reports of injuries were obtained and examined and media reports studied (UN, 2009(c): 7, 8, 47). Of particular importance are the video and photographic images that were studied, including satellite imagery obtained from UNOSAT and analysed by experts (UN, 2009(c): 48).

UNOSAT is an UN agency with the mission to provide satellite imagery and geographic information to the UN humanitarian community in the most straightforward, efficient and cost-effective manner possible. The result of increasing scientific development and "privatisation of space" is that military intelligence agencies lost their monopoly over imagery with a high level of detail. This has a profound impact on political decision-making in view thereof that in respect of such high resolution imagery, UN agencies, NGOs and the media have similar access as military and foreign affairs ministries, leading to more transparency in international diplomacy. UNOSAT has negotiated discounted prices for satellite imagery to the UN community. The service delivery is extraordinary, for example: "(t)he UNOSAT partners' SPOT image and Space Imaging Eurasia, can acquire a satellite image of the Middle East and deliver this to UNOSAT within 24 hours" (UN, 1949 - 2009: 5). Of further importance for this

study is that UNOSAT cooperates with the UN Interregional Crime and Justice Research Institute (UNICRI) by providing satellite derived mapping and geographic information regarding the following: (UN, 1949 - 2009(c))

- To advance understanding of crime-related problems;
- to gather and analyse criminal intelligence data;
- to identify geographical crime patterns; and
- to facilitate international law enforcement cooperation and judicial assistance.

3.4. Crime intelligence gathering and analysis for prosecution of war crimes, genocide and crimes against humanity

The investigation of war crimes in particular, differs to a large extent from national investigations into crime, as a result of the following circumstances: (ICTY-UNICRI, 2009:7)

- Breaches of the IHL normally involve immense geographical areas, take place over long time periods and involve military, paramilitary and mercenary actors.
- The crimes involve hundreds or thousands of victims and therefore result in a massive volume of evidentiary material.
- Interference in the cases by influential and high ranking politicians or officials could be experienced, requiring extensive witness protection programmes and even relocation to other counties. To further protect witnesses their identities can only be made known to the defence shortly before the hearing.
- Crimes are committed during periods of “chaos and stress” and sometimes many years before investigations commenced.
- The cooperation of the state in which the investigations are performed may be lacking or the state may be obstructive to the investigations.

The investigation of the abovementioned international crimes by the Chief Prosecutors of respectively the ICTY and the International Criminal Tribunal for Rwanda (ICTR), served as a benchmark for future investigations by the ICC. Information gathering for the ICTY had to take place whilst the conflict was ongoing. The ICTY developed practices to ensure that states which are in possession of intelligence relating to war crimes present the same to the ICTY on a confidential basis and with the undertaking that it will not be revealed without the permission of the state that has provided it, if it is feared that intelligence practices might be revealed or if the state fears that its role towards a particular party to the conflict or in the conflict itself might be revealed (ICTY-UNICRI, 2009: 8).

The importance has been realised to identify at an early stage of investigations sensitive sources, to evaluate such sources and to take measures to protect the sources' personal safety and the confidentiality of information. Military intelligence and operational documents may be central to the investigation of a war crimes case, but would normally not be accessed by courts. It is, however, considered better to have access to such sensitive information even if it could not be used as evidence (ICTY-UNICRI, 2009: 19). The ICTY was aware of many instances where sensitive witnesses who were to testify against high ranking persons were assaulted or even killed. Adequate measures for witness protection must therefore be taken. The ICTY also used informants, namely persons who will provide confidential information sometimes for payment, without being expected to testify. Verification of such information is essential and the source must be protected. Proper records should be kept, not only for the protection of the informer, but also to counter allegations of impropriety or corruption. Special measures were taken to allow states or NGO's or other organisations to provide sensitive and confidential information as a lead only, not to be disclosed other than by consent. The name of the provider or staff members of the provider of such sensitive and confidential information, often may not be disclosed (ICTY-UNICRI, 2009: 20).

Vulnerable witnesses and sensitive sources could provide evidence and information in the form of "witness statements, documentary evidence, experts' reports, intelligence reports, intercepts, etc" Proper record-keeping and arrangements for securing sensitive information must be taken (ICTY-UNICRI, 2009: 27). Best practices have been developed to keep record of and dispose of evidence as diverse as: "archives, diaries, journals and books, military reports, situation reports, dispatches, minutes of government sessions, command and control documents, international reports, photographs and videos, intercepts and open sources". Other sources of evidence include "computer equipment, clothing, ballistic and trace metals and firearms found at crime scenes and other locations" (ICTY-UNICRI, 2009: 27).

Many humanitarian and other organisations, through their involvement during and directly after a conflict in the relevant country, are exposed to information and victims of war crimes. It is important that members of these organisations are encouraged to gather general information of the details and in particular note the future contact details of the victims, but they should leave the taking of comprehensive witness statement to professional investigators (ICTY-UNICRI, 2009: 16). In addition to informers and witnesses, the investigators may gather evidence through formal search and seizure processes to obtain documents and other evidence. Mutual legal assistance requests can also be made to the authorities in other countries for *inter alia* the collection of information and evidence, the location and handing over of suspects, and on-site inspections. An international tribunal and for that matter, the ICC may also receive and need to assist with similar requests from countries which are exercising national jurisdiction to prosecute war criminals (ICTY-UNICRI, 2009: 18).

Crime intelligence analysis is performed under the functions of "military analysis, political analysis and criminal analysis". During the pre-trial or investigative phase crime intelligence analysis is aimed at finding gaps in available evidence which

need to be covered by further investigations. The analyst becomes involved in field-work in the follow-up stage especially in obtaining documentary evidence through warrants (ICTY-UNICRI, 2009: 28). During the trial phase the analyst performs a monitoring and assistance role in view of his or her knowledge about the available evidence (ICTY-UNICRI, 2009: 28).

Of particular importance in war crimes investigations is that investigative teams need to follow a multi-disciplinary approach. Investigators with a police background, including those experienced in organised crime and financial investigations are required, but also military, criminal and political analysts, historians, demographers, forensic specialists and linguists (ICTY-UNICRI, 2009: 12). The range of specialists required is further illustrated in respect of exhumations. The Office of the Prosecutor in Kosovo alone was responsible for the exhumation of approximately 2000 bodies. The following experts are required to ensure that exhumations are performed in support of prosecutions: forensic pathologists; forensic dentists; forensic anthropologists; radiologists or radiographers; mortuary technicians; scene of crime officers and DNA specialists (Vanezis, 1999). In respect of the investigation of sexual offences within the context of war crimes, the following expertise is required: prosecution counsel, investigators, doctors, nurses, counsellors, interpreters, and witnesses' assistants, all trained on how to deal with victims of sexual offences (International Criminal Tribunal for Rwanda, 2008: 4).

Civilian intelligence agencies of especially major powers could assist Commissions of Inquiry, such as the above, as well as the investigative authorities of international tribunals or the ICC mandated to inquire into or investigate war crimes, genocide and crimes against humanity, with for example satellite imagery. Human rights observers raised serious questions about the US and other Western powers in relation to the Bosnian situation. The question is asked on whether the US had advance knowledge of the Bosnian Serb attack on Srebrenica and failed to warn the UN forces guarding the city. The US IC focused

on the war with vast resources, including spy planes, spy satellites, radio intercepts, and human sources in the region. The opinion has also been expressed that other Western intelligence agencies were slow in releasing evidence of Bosnian Serb war crimes committed during the four year conflict. Although the ICTY commenced its work in 1993, the intelligence agencies of the US, UK France and Germany only agreed on a policy of declassification of their information to assist the ICTY in early 1996, after "being shocked in action" by the "bloody fall" of Srebrenica. The realisation of what was happening in the Balkans evoked international response after the US in a controlled manner released intelligence (photographic material) to the UN Security Council on mass killings in the former Yugoslavia, which was gathered by U-2 spy planes. Furthermore, the discovery by spy planes and satellites of suspected mass graves prompted Western countries to prevent further bloodshed (Shanker, 1996). Following up hints that the IC in the US had advance warning of the attacks, and media reports confirming the existence of intercepts by the US IC, the ICTY's Chief Prosecutor, Richard Goldstone filed a formal request to the US for greater assistance by the IC to the ICTY investigations (Shanker, 1996).

Applying special investigative techniques such as the interception of communications by the investigators of war crimes under the ICC or an UN sanctioned tribunal is highly improbable, firstly because the crimes are in many cases committed years before being investigated. Secondly such an investigation method is specialised and involves expensive equipment usually only at the disposal of the IC's. The only source of intercepts which could be used by the ICC or similar tribunal is the national ICs of states. The same is true about IMINT.

4. CONCLUSION

There is a growing need in international organisations dealing with intelligence to become more independent from the member states involved in these organisations, which is also a requirement for the success of such organisations.

Both in INTERPOL and the UN, there is a tendency to gather and use especially OSINT in support of analysis. These international organisations can play a huge role on the policy and strategic level by having additional sources of information, independent of the individual Member States. Such independence is also important for transparency and avoiding abuse of the powers vested in international organisations through the manipulation of intelligence, or withholding of intelligence or disinformation. In respect of satellite imagery, the UN has accomplished a high level of independence. INTERPOL has established an unrivalled status for crime intelligence cooperation on regional and international level, capitalising on a network of cooperation agreements. This is not only in respect of the use of its secure communications in a controlled manner, but for a two-way exchange of intelligence which contributes to INTERPOL's ability to provide analysis and guidance in the coordination of information on all international crimes far beyond the competence of its individual Member States or of individual regions. It is clear that INTERPOL should further build on its relations to become totally inclusive of all countries globally and even to strengthen its ties with regional police organisations, and to play an active role in establishing more such regional police cooperation organisations.

In the UN structures, such as the IAEA, the need to establish an improved, open-source ability and strengthen intelligence analysis has also been identified. In respect of regional intelligence cooperation, it was mentioned that it is highly improbable even in a close-knit region such as the EU, that an independent EU intelligence organisation or 'FBI' will be established. The same is true with regard to an international organisation, such as INTERPOL. It is not likely that INTERPOL will develop an independent intelligence gathering capacity which will be empowered to gather intelligence other than OSINT. This is basically as a result of the sovereignty principle.

Concerning the investigation of war crimes, genocide and crimes against humanity, it is clear that an international organisation, such as the UN, could through an establishment such as the ICC with its investigative authority in the form of the Chief Prosecutor, investigate crime and gather crime intelligence in the same manner as any other law enforcement agency. The ICC and other international tribunals will remain highly dependent on national intelligence and law enforcement agencies for intelligence such as intercepts and also satellite imagery, despite the level of access gained to open-source satellite imagery by the UN. The ICTY has provided a highly developed model for intelligence gathering, analysis and use in the form of a manual developed in this regard.
International organisations need to cultivate an improved sense of information security in dealing with sensitive information in order to build trust with national intelligence agencies to provide them with more detailed and sensitive intelligence.

In future, there might be an increased demand to extend the jurisdiction of the ICC to crimes other than war crimes, genocide and crimes against humanity. Should the jurisdiction of the ICC be expanded to all international crimes, the demand for increased cooperation between national intelligence and law enforcement agencies and the ICC would increase exponentially. For an increased effectiveness of international organisations, it is clear that national intelligence agencies and regional organisations should participate more actively in contributing to INTERPOL databases, use such databases, and effectively allow international organisations to add value to the intelligence picture through dedicated analysis of as broad as possible a data-pool.

In respect of positive intelligence, there is simply no comparative international organisation to what INTERPOL does in respect of crime intelligence. It seems that cooperation between positive intelligence and crime intelligence should be improved as much as possible on national and regional levels.

UN structures, in cooperating with national positive intelligence and crime intelligence agencies, must be careful not to be viewed as extensions of such national agencies, but must retain their independence and objectivity. The UN is also successful in the gathering of military type intelligence in respect of peacekeeping and peace enforcement.

In the next chapter of this study, which forms an evaluation, a summary of the study will be provided; the assumptions formulated in the Introduction will be evaluated; certain conclusions will be drawn, and models for increased intelligence cooperation on the national, regional and international levels will be proposed.

CHAPTER 9
EVALUATION

1. SUMMARY

The main objective of the study as set out in Chapter 1, was to identify ways of improving intelligence cooperation between law enforcement (crime intelligence) and positive intelligence (civilian and military intelligence), in combating international crime, on the following levels:

— At national level, between the respective law enforcement agencies and positive intelligence agencies within a state.
— On regional level, between particular regional organisations and their member states.
— On international level, between member states and particular international organisations and their member states, as well as between such organisations and regional organisations.

A secondary objective was to identify and analyse the respective challenges or blockages which inhibit intelligence cooperation between crime intelligence and positive intelligence, in order to determine what can be done nationally and internationally to improve cooperation between crime intelligence and positive intelligence in combating international crime.

A further secondary objective was to compare the intelligence gathering techniques employed by crime intelligence, such as undercover operations, controlled delivery and surveillance, to the techniques employed by positive intelligence.

The study has been done with reference to the recent response (post-11 September 2001), to these challenges in respect of intelligence cooperation and sharing. Best practices, which on their own or in combination could be used to benchmark solutions for improved cooperation between crime intelligence and positive intelligence, have been identified to meet the above objectives. Proposals are made on how the sharing of intelligence, including "raw intelligence" can be improved on operational level.

Primary sources, including international instruments, legislation and government policies, jurisprudence, and reports of national and international commissions of inquiry have been used. Various secondary sources, including journal papers, media reports, and theses have also been used.

In pursuit of the above objectives, the study was structured as follows:

(a) In Chapter 2 concepts such as international crime, transnational organised crime, intelligence, civilian intelligence, human intelligence, domestic intelligence, foreign intelligence, military intelligence, signals intelligence, technical intelligence, crime/criminal intelligence and strategic intelligence were defined within the context of and for the purposes of the study. War crimes, genocide, crimes against humanity and piracy are well defined in international law. It was pointed out that in international legal instruments there are no universally accepted definitions of international crimes such as terrorism and organised crime, whilst crimes required by such legal instruments to be established in national laws in respect of mercenary activities are limited, contain gaps, are ambiguous and are not suited to address recent developments. The extensive use by governments in conflicts of private military and private security companies in particular is not addressed in either the regional (AU), or the international (UN) instrument in this regard. The use by governments of mercenaries is therefore not adequately addressed in international law. Definitions for

terrorism and organised crime were proposed in Chapter 2. Law enforcement in respect of crimes relating to the proliferation of WMD is closely related to 'international legislating' in the sense of enforcement required by the international community of UN Security Council sanctions relating to WMD. The concept of intelligence cooperation was also defined to include the law enforcement, military and intelligence responses to international crimes as well as a combination of the said responses. Intelligence was defined within its respective meanings such as referring to respectively an institution, activity/process or product.

(b) In Chapter 3 the change in the focus of intelligence in the post-Cold War era from a mainly military focus to drug trafficking, terrorism, organised crime, WMD, and in Africa, early warning (or rather warning intelligence), regarding conflict was described. The shift in focus to peacekeeping intelligence to support the peacekeeping and peace support operations of the UN was pointed out. It was observed in Chapter 3 that the 11 September 2001 events in the US revealed major intelligence weaknesses, amongst others an overly reliance on SIGINT and IMINT and a need for the US intelligence agencies to cooperate with smaller agencies of other countries with HUMINT capabilities. The need for improved intelligence cooperation in respect of international crimes is also evident in South East Asia. Furthermore, the international and regional international instruments which require states to cooperate in respect of intelligence to combat international crimes, including cooperation in respect of special investigative techniques were reflected upon, with reference to the UN, INTERPOL, the EU, including Europol, the AU, SADC and ASEANAPOL. It was pointed out that the strongest form of intelligence cooperation between states is on the bilateral level. In addition to international obligations, the drivers or incentives for intelligence cooperation were discussed, namely globalisation; utility or the success that can be gained from intelligence cooperation; the common threat

posed by international crimes; and increased expectations of the public to address such threats. Such drivers also include the availability of OSINT, commercial technologies, the sheer volume of intelligence as well as the 'privatisation' of intelligence. The intelligence-driven approach to law enforcement, common to many countries, demands intelligence cooperation on all levels, nationally and internationally. INTERPOL was identified as the common factor between states on regional and international level for crime intelligence cooperation. There is, however, much room for improvement in respect of intelligence cooperation on the regional and international level.

(c) The challenges for cooperation between civilian and law enforcement intelligence were discussed in Chapter 4. Sovereignty (affecting cooperation between states as well as intelligence cooperation between member states and international organisations such as the UN) was identified as a major challenge in this regard. Within the context of sovereignty the issue of failed or "rogue" states in different typologies, and the effect of corruption on intelligence cooperation were discussed with reference to piracy in Somalia, terrorism in Pakistan, narco-terrorism in Colombia and corruption in Mexico. The precarious situation of international organisations not to be accused of spying on member states, whilst forced through involvement in activities such as peacekeeping to obtain intelligence is described. The use of states of sovereignty to their advantage to gather intelligence which would domestically be difficult or impossible to gather was also discussed, as well as extralegal actions such as renditions and the use of so-called "black facilities" for interrogation of suspects. The negative effect of such methods on intelligence cooperation was discussed as well as best practices developed to counter such negative effects. Other factors negatively affecting intelligence cooperation are differences in the approach of respectively crime intelligence and positive intelligence, interagency

rivalry, mistrust and the differences between the oversight mechanisms of crime intelligence and positive intelligence. The lack of standardisation both in respect of methodology (such as analysis) and even equipment and language differences was also discussed. It was pointed out that large scale data-sharing, the sharing of high grade intelligence and raw intelligence is seldom undertaken. The difference between intelligence and evidence was pointed out, as well as the difference between positive intelligence and crime intelligence in respect of focus and tasks, such as prevention as opposed to reaction. The concern of a lack of general standards for entering into intelligence cooperation agreements, the exchange of intelligence and requirements for political authorisation for intelligence exchange were identified. The effect of public/private relationships on intelligence cooperation and the informal obtaining of information from the private sector were also discussed.

(d) In Chapter 5 the methodologies used by law enforcement (crime intelligence) and positive intelligence respectively, were discussed in order to find common ground for maximum cooperation between positive intelligence and crime intelligence, whilst focusing on law enforcement rather than military action. In respect of law enforcement intelligence the special investigative techniques of controlled deliveries, undercover operations, and surveillance, including electronic surveillance were discussed with reference to case studies in the EU, the UK and the US.

The use of intercepted information as evidence in particular was discussed, with reference to the UK. The trends in positive intelligence, namely the centralisation of intelligence and the reliance on COMINT and SIGINT were also discussed. Whilst surveillance as practised by crime intelligence within the ambit of authorising legislation is not controversial, the scope of COMINT and SIGINT collection by positive intelligence is controversial with concomitant negative effects for cooperation in this regard between crime intelligence and positive intelligence. The extremely

wide-ranging and effective COMINT and SIGINT collection cooperation between the US, the UK and other partners was discussed. It is pointed out that the benefits thereof could be shared with crime intelligence on a strategic level and operationally to support for example interdictions and controlled deliveries. It was pointed out that cooperation between crime intelligence and positive intelligence should not be focused on court directed processes, but rather pure intelligence processes such as data-mining and bulk interceptions focused on operational support in combating international crimes.

(e) Chapter 6 describes the models for intelligence cooperation on national (interagency) level, with reference to intelligence failures such as the 'walls of separation' in the US before the 11 September 2001 events between civilian and law enforcement (crime) intelligence caused by widely criticised domestic intelligence activities by the CIA and other intelligence agencies with a foreign intelligence mandate. The intelligence failures identified by commissions of inquiry, including inquiries into the intelligence failures surrounding the 11 September 2001 events and US and UK commissions of inquiry into how civilian intelligence agencies dealt with the issue of WMD in Iraq, as well as intelligence regarding the attacks on the London train stations were analysed. Various policies and strategies guiding military, crime and civilian intelligence and information sharing in the US and the UK were analysed and the concept of the fusion of intelligence discussed, including the weaknesses identified in respect of practical implementation of the concept. The common areas between the US and UK models of intelligence cooperation were identified. The elements of an ideal national model for intelligence cooperation were also identified as well as the elements of an ideal national model for intelligence cooperation.

(f) In Chapter 7 of the study, models for intelligence cooperation on the regional level were discussed with reference to practical intelligence

cooperation and how factors inhibiting intelligence cooperation are addressed in furthering common interests. Europol as a regional crime intelligence institution, which also utilises the intelligence-led approach towards combating international crimes on a strategic as well as an operational level, was discussed. The Europol Crime Intelligence Model ensures intelligence cooperation not only between the EU Member States' national police forces, but also with customs authorities, financial intelligence centres, the judiciary and public prosecution services, and all other public bodies that participate in the process that ranges from the early detection of security threats and criminal offences to the conviction and punishment of perpetrators. It was pointed out that Europol is important in respect of a standardised approach to threat, risk and profile analysis and data access and distribution. Europol has established a trusted information environment, which was also pointed at as a crucial element for intelligence cooperation on the national level.

The most important elements of Europol intelligence cooperation were identified as joint cross-border operations and Joint Investigation Teams, coordinated by Europol and supported by a Joint Experts Network, which produced a manual for the setting up of JITs and for joint operations. Examples were pointed out where Member States of the EU have relinquished some degree of sovereignty in order to enhance their joint capacity to combat cross-border/international crime. The harmonisation of the roles of police officers in the respective Member States is a future goal identified for the EU. Reference was also made to civilian and military intelligence cooperation in the EU where the expansion of the EU led to a higher degree of mistrust, especially with the inclusion of erstwhile East bloc states with a legacy of repressive intelligence services. The role of NATO in coordinating intelligence with respect to joint military operations against international crimes such as terrorism and piracy was discussed. It was pointed out that the establishment of a "regional FBI" is highly

improbable. Proposals were discussed to overcome distrust. The ASEANAPOL model of crime intelligence cooperation was discussed, as well as intelligence cooperation in ASEANAPOL.

Civilian intelligence cooperation in Africa was subsequently discussed with reference to the ACSRT. The interaction with the Member States of the AU with the ACSRT through national focal points is one of the most important aspects of the ACSRT's role. In respect of civilian intelligence cooperation, the role of the CISSA in Africa was addressed as well as regional police intelligence cooperation in Africa. Mistrust and self-interest/sovereignty were identified as the most important stumbling blocks for intelligence cooperation on the regional level.

(g) In Chapter 8 of the study, models for intelligence cooperation on the international level were discussed with reference to INTERPOL and the UN, in particular the use of UN commissions of inquiry and the investigations performed by the prosecutors of the respective UN tribunals and the ICC into war crimes, genocide and crimes against humanity. It was pointed out that intelligence cooperation on international level is far more advanced in respect of crime intelligence as opposed to positive intelligence, with no institution in respect of positive intelligence that could be compared to INTERPOL. The independence of INTERPOL, which is able to add value to intelligence to the extent that individual Member States are unable to do, was discussed. This independence is identified as the *crux* of INTERPOL's successful role in crime intelligence cooperation (Gerspacher, 2002: 24). This independence is enhanced by INTERPOL's links with other international organisations dealing with crime intelligence. INTERPOL's intelligence cooperation role is on the strategic as well as the operational level and covers intelligence cooperation in respect of all international crimes discussed in this study. The convergence between international crimes was shown, as a result of which so-called watch-

points, serving as focus points for intelligence cooperation is discussed (US, 2005(d). The intelligence activities of the UN are discussed, with reference in particular to the combating of terrorism, the proliferation of WMD and war crimes. The need for the independence of international organisations to properly fulfil their obligations and not to be viewed as extensions of national intelligence agencies was underlined. The respective UN tribunals have been able to gather crime intelligence on war crimes successfully, but needs intelligence support from positive intelligence, especially in relation to IMINT and COMINT (ICTY-UNICRI, 2009) (Shanker, 1996).

2. TESTING OF ASSUMPTIONS ON WHICH THE STUDY WAS BASED

Assumption: Although the events of 11 September 2001 have led to increased emphasis on intelligence cooperation at the various levels, certain factors such as sovereignty and mistrust are still preventing more effective cooperation between crime intelligence agencies and positive intelligence agencies.

It is clear from the study that, despite various drivers for intelligence cooperation, such as common threats posed by international crimes such as terrorism, piracy, crimes related to the proliferation of WMD and transnational organised crime, sovereignty is the single most important factor inhibiting intelligence cooperation (Aldrich, 2004: 737). Intelligence lies at the core of national sovereignty (Herzberger, 2007: 101). This is true on the national level in terms of the 'independence' of intelligence agencies as well as the independence and focus on self-interest of states on the regional as well as the international level. On the national level this factor is evident from interagency rivalry and mistrust, as well as the difference in approach between crime intelligence and positive intelligence in respect of methodology, objectives and what is referred to as 'organisational

cultures' (US, 2005(c): 288). Especially within international organisations such as INTERPOL and the UN, sovereignty is a major factor to be dealt with in respect of intelligence cooperation, where such organisations need to be seen to be objective and not to be 'spying' on their Member States. In order to fulfill their roles, such international organisations need to obtain some independence in even the gathering of intelligence even if it is just open source intelligence (Gerspacher, 2002: 24). Some UN established institutions need to act fully as intelligence gatherers, for example the prosecutors and their investigators attached to the criminal tribunals established by the UN Security Council to investigate war crimes.

Mistrust is indeed, as is shown in the study, even after the 11 September 2001 events, still one of the major stumbling blocks in intelligence cooperation. The issue of mistrust is the most notable on the regional level within the EU, where huge strides have already been made in respect of both positive intelligence cooperation and crime intelligence cooperation (Walsh, 2006: 625, 638). Formal and informal agreements on intelligence cooperation are valuable tools to overcome mistrust in intelligence cooperation. It is shown in the study that there are also other factors having a profound effect on international intelligence cooperation, such as corruption and the phenomenon of failed or dysfunctional states, as is evident from the examples mentioned in respect of the combating of piracy and drug trafficking and terrorism with reference to Somalia and Afghanistan respectively (Björnehed, 2004: 309).

It is shown in the study that states have a huge resistance to multilateral pooling of intelligence, especially very sensitive data, as a result of security concerns (mistrust) as well as self-interest (sovereignty). In some cases states are prevented from sharing intelligence as a result of constitutional constraints. It is pointed out that states are also reluctant to become dependent on other states for intelligence (Aldrich, 2004: 237, 741).

The greatest risk of intelligence cooperation is the increased threat of espionage and counterespionage. At the heart of a reluctance to share 'hot' intelligence, is often the lack of political will to do so, as is also evident in the EU (Herzberger, 2007: 1). Intelligence sharing on the regional or international level is most frequent where there are clear incentives in terms of political or other gains from such sharing, or where states know that they share the same policies; that they desire the same outcomes from the intelligence sharing; and where they have confidence in the accuracy of the shared intelligence (Fagersten, 2007: 14).

The different organisational cultures amongst intelligence agencies may lead to distortion or withholding of information; turf battles; agencies taking credit for successes derived from intelligence received from another agency without recognition given; and competition as a result of fragmentation. Through competitive intelligence gathering intelligence agencies effectively undermine each other (Boardman, 2006). The non-sharing of intelligence on the other hand may lead to mistrust and refusal of future cooperation. The classification and in particular over-classification of information by agencies is a factor that may severally hamper the sharing of intelligence. The transfer of police data is described as a 'legal minefield' as a result of different structures of protection accorded to personal information in respectively the US and Europe, with strict data protection laws in the latter.

Despite being aware of the problem of institutional differences between law enforcement and positive intelligence and interagency rivalry, it is one of the most difficult issues to address and some form thereof will probably always be experienced.

Whilst the different intelligence agencies must therefore relinquish some authority for the sake of joint planning, but retain operational responsibility, it is clear that mistrust and self-interest- in the case of national agencies linked to so-called

institutional culture and unhealthy competition between agencies, and on regional level, sovereignty, remain inhibiting factors.

The assumption that sovereignty and mistrust still prevent more effective cooperation between crime intelligence agencies and positive intelligence agencies can therefore be verified.

Assumption: Broad intelligence cooperation and sharing in respect of covert action and covert operations are highly unlikely.

Covert action includes assassination, propaganda, political interventions in the political process of the target nation, the use of covert economic measures against a state, the instigation of a *coup* in another country, support of paramilitary actions and secret participation in combat (Jansen van Rensburg, 2005: 22). Covert action by nature is highly controversial and different opinions exist as to whether it could indeed be regarded as part of intelligence (Shulsky & Schmitt, 2002: 96). The use of covert action to combat crime remains a controversial issue.

The exercising of extraterritorial powers by one state may not only may be illegal in another state, but may also cause a loss of trust where intelligence cooperation or intelligence sharing lead to extraterritorial actions which are controversial and sometimes regarded as unethical or inconsonant with international law, relating for example to torture.

The practice of the US to perform so-called ‘renditions’ which could include any extra-judicial transfer of persons from one jurisdiction or country to another, for a variety of purposes, from prosecution to interrogation and extraordinary rendition which may include torture, as well as detention in special military facilities, is an example of covert action with negative consequences for future intelligence cooperation (Wilkinson, 2006: 164) (UK, 2007(a)).

The negative effect of covert or clandestine operations, such as extralegal rendition and sometimes assassination of terrorist targets is one of the most significant threats to international intelligence cooperation. Although such actions may result in successes for the countries executing them, it in numerous instances led to embarrassment for countries that cooperated and to subsequent policy decisions on the highest level not to further allow cooperation in respect of such actions. This is true even amongst the closest partners in intelligence cooperation, such as the US and the UK (UK, 2007(a)). Intelligence cooperation aimed at pure law enforcement actions seems to have the best chance for success. It is, however, in many instances imperative to be able to utilise the intelligence support of civilian and even military intelligence in order to ensure successful investigation of, or the prevention of international crimes.

Military action is in some instances the only option to act in respect of for example war crimes, piracy and terrorism, in which case action should preferably be based on resolutions of the UN Security Council. Covert action will always remain controversial, especially assassinations. The innovative use of military force in an overt manner by means of direct action, which is in line with international law, is supported (Berkowitz, 2003: 133). Even the interrogation programme through which some suspects were detained for months or years in Guantánamo, carried out by the CIA, has been condemned by US courts and had a negative effect on future intelligence cooperation which could lead to incarceration and interrogation or torture (Piret, 2008: 102).

The assumption that broad intelligence cooperation and sharing in respect of covert action and covert operations are highly unlikely is therefore verified.

Assumption: Intelligence cooperation needs to be very focused in terms of methodology, mainly clandestine intelligence gathering methods, especially human intelligence, within the context of special investigative

techniques of controlled deliveries; undercover operations; and surveillance, including electronic surveillance.

Due to the differences between the methodology used respectively by civilian and crime intelligence, the focus of intelligence cooperation should be on special investigative techniques.

As a result of the concept of intelligence-led policing, police services are viewed as part of the broader IC. The importance of positive intelligence keeping law enforcement informed is gradually realised.

Police undercover operations can be regarded as being 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. 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 identification of opportunities for controlled deliveries, or to identify targets for further court-directed attention through special investigative techniques.

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 possible intelligence capabilities and available information could on

national, regional and international level be pooled (fused) to ensure that the most appropriate and effective action in the circumstances is taken against international crime (US, 2006(c): 1 – 4). The intelligence available through law enforcement investigations might be critical for use in respect of military operations.

The Netherlands and Belgium were identified as countries using the 'full panoply of special investigative techniques' and legislation in those countries can be regarded as model legislation in this regard (De Koster, 2005: 16).

It is pointed out in the study that it was realised that US intelligence, despite its technological capabilities regarding imagery and interception, needs to be assisted by smaller intelligence agencies with HUMINT capabilities. The US even experienced a lack of interpreters in foreign languages The US realised it could provide training and other assistance to foreign agencies, in exchange for HUMINT, intelligence sharing or being allowed to use foreign territory for surveillance, rather than relying only on their own HUMINT capabilities (Reveron, 2006: 454 – 455).

The assumption that intelligence cooperation needs to be focused in terms of methodology is therefore verified.

Assumption: By operating in an incremental fashion, and on a project basis, trust can be built between the respective actors in order to promote future intelligence sharing.

The study clearly shows that excellent successes have been achieved in combating international crimes especially transnational crime, through joint investigative teams focusing on crime threats identified through bilateral and multilateral cooperation arrangements. This is the case in the EU through

Europol, with its JITs, the ASEAN region through ASEANAPOL and in Southern Africa through the SARPCCO arrangement.

Regional law enforcement organisations do play an important role on both the operational and strategic level through multilateral crime threat analysis, identifying projects to address such joint crime threats and then operationally supporting such operations. It has been shown in the study that there is usually more trust between agencies where joint threats are addressed.

Within a regional community, joint operations to combat transnational crime are of huge importance, and tend to be highly successful in sharing operational intelligence. In this case it is also important for effective intelligence cooperation that agreements are concluded to allow a degree of flexibility for the law enforcement officers of the respective states to operate in each others' countries. The establishment of JITs, as provided for in the EUROPOL model, is of particular importance for regional intelligence cooperation within the context of the investigation of international crime (Europol, 2009(a): 18, 19, 24, 25).

The assumption that future intelligence sharing can be promoted through an incremental building of trust on a project basis is therefore verified.

3. CONCLUSION

Sovereignty and distrust still hamper intelligence cooperation in combating international crime. Much can be done on national, regional and international level to improve intelligence cooperation to combat international crime. The solution to better intelligence cooperation between positive intelligence and crime intelligence implies the implementation of a combination of proposals. The intelligence culture of a 'need to know' needs to be substituted by a culture of a 'need to be informed' on the national, regional and international levels.

The following proposals are made to enhance intelligence cooperation on the national level, namely that an ideal or model national interagency intelligence system should have the following elements:

— A comprehensive framework for intelligence should be established, including an office with overall power in respect of the whole IC, inclusive also of law enforcement (crime) intelligence. There must be a national coordination mechanism on which all agencies are represented. Duplication of intelligence structures with overlapping mandates must be avoided by integrating such structures into a single unit. Policies to delineate the respective role of the agencies in the positive IC and crime intelligence spheres, as well as to address attitudes in relation to intelligence must be in place. 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). There should be a similar if not the same accountability or review system in respect of the activities of the whole IC. There must be a reward system in place to award sharing of information or intelligence.

— Policing must be community based and intelligence-led and information gathering should be closely linked to communities, involving civil society. Fusion of intelligence should take place on the local as well as regional and national levels. 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. Cooperation should also take place between law enforcement and the prosecution, from an early stage of the investigation. Legacy teams should continuously review previous operations for identification and follow-up of leads that might have been overlooked.

— There should be the maximum degree of fusion or integration of intelligence efforts between crime intelligence and positive intelligence on

the national level as such cooperation is difficult on the regional and international levels.

— States need to provide in their national laws for powers for law enforcement for the use of special investigative techniques such as undercover operations, controlled deliveries and surveillance, including electronic surveillance as well as the use of evidence obtained through those techniques in prosecutions, even where the evidence is obtained in different jurisdictions.

— The safeguards developed for MI5 and MI6 in the UK can be viewed as best practices to counter the negative effects of cooperation in respect of covert action such as extralegal renditions. These safeguards are aimed at the prevention of cooperation which may culminate in the use of torture or mistreatment.

— Intelligence support to crime intelligence by positive intelligence must focus primarily on COMINT and SIGINT, in view of the wide-ranging powers and capacity of positive intelligence in that regard. Such support need not be for court purposes, but could be used to identify opportunities for interdiction of huge shipments of contraband, the location of wanted suspects and in general to provide intelligence leads that could be followed up through special investigative techniques in a court-directed manner.

— Institutional differences between intelligence agencies could be overcome through structural changes and by promoting a culture of a need to share rather than need to know.

In order to improve intelligence cooperation on the regional and international level, the following guidelines are proposed:

— International organisations should focus on collection and analysing open-source intelligence in order to enhance their independence, without endangering their objectivity and impeding on the sovereignty of their member states. International organisations need to cultivate an improved

sense of information security in dealing with sensitive information in order to build trust with national intelligence agencies to provide them with more detailed and sensitive intelligence.

— Further development of the international legal framework, especially in respect of international obligations to combat mercenary activities is required. National intelligence and law enforcement agencies should improve their assistance in respect of intelligence such as intercepts and also satellite imagery, to the ICC and other UN criminal tribunals investigating war crimes. The manual developed by the ICTY for intelligence gathering, analysis and use can be regarded as a comprehensive and useful model for the ICC.

— Trust can be built on an incremental basis within an international and regional context through joint crime threat analyses and joint operations supported operationally by regional and international organisations.

— The focus for intelligence cooperation on the international level should be on bilateral level where the level of trust is the highest.

— International law in respect of defining mercenary crimes must be improved to address the extensive use of private military and security companies by governments in conflicts.

— States which have not yet become parties to major international instruments relating to international crimes need to be encouraged through multilateral fora to become party to such instruments and to incorporate the crimes required to be adopted in terms of those international instruments in their national laws.

— Covert action should, however, not be regarded as a priority area for regional or international intelligence cooperation.

— Regional intelligence cooperation organisations should establish networks with international institutions such as INTERPOL, and the UN, providing the benefit of both regional and international cooperation. This to some extent provides a basis for military intelligence, crime intelligence and civilian intelligence cooperation.

— The placement of personnel from member states of the respective countries stationed at the regional and international organisations is identified as a good practice to provide a spectrum of expertise and access to national agencies and their databases, through established protocols. The practise of placing police liaison officers or legal attachés in cooperating countries to promote crime intelligence cooperation also largely enhances crime intelligence cooperation.

— The African model of regional police cooperation with INTERPOL providing secretariat services, to and CISSA enhancing intelligence cooperation between the civilian intelligence services of most countries on the African Continent, can serve as a model for other regions.

— The independence of regional and international organisations involved in crime intelligence should be promoted, as well as the building of capacity in such organisations to collect and analyse OSINT. These international organisations can play a huge part on the policy and strategic level by having additional sources of information, independent of the individual member states. Such independence is also important for transparency and avoiding abuse of the powers vested in international organisations through the manipulation of intelligence, or withholding of intelligence or disinformation. INTERPOL has established an unrivalled status for crime intelligence cooperation on regional and international level, capitalising on a network of cooperation agreements. It is clear that INTERPOL should further build on its relations to become totally inclusive of all countries globally, strengthen its ties with regional police organisations, and even to play an active role in establishing more such regional police cooperation organisations. It is, however, important that Member States should maximally use the secure communications network of INTERPOL for the exchange of crime intelligence, and contribute to and use INTERPOL's databases and systems such as the MIND/FIND system.

— There is a need for an international instrument on intelligence cooperation to combat international crime. A draft document in this regard is proposed

and attached as an Annexure. Aspects of intelligence cooperation and in particular information exchange, are captured in various international instruments, such as the *United Nations Convention against Transnational Organized Crime* and various counter-terrorist Conventions. The forming of joint investigation teams, for example is also covered in the *UN Convention against Transnational Organized Crime.* (UN, 2004(a): Article 19). The usefulness of the provision for such joint investigation teams is, however, then confined only to transnational organised crime, whilst the concept would be made applicable to all international crimes if included in a general intelligence cooperation convention. The proposed draft convention may also serve to consolidate intelligence cooperation in respect of all international crimes related to security. The concept of international joint investigations is relatively new and is not reflected in most international instruments on international crimes.

The convergence of international crimes and the watch-points developed to focus intelligence cooperation must be taken into account. There should therefore on both the national and the international level be an all-crimes approach to intelligence collection and analysis.

ANNEXURE

DRAFT INTERNATIONAL CONVENTION ON INTELLIGENCE COOPERATION TO COMBAT INTERNATIONAL CRIME

THE STATES PARTIES TO THIS CONVENTION,

BEARING IN MIND THAT international crimes present a common threat to security and stability globally;

RECALLING that various international instruments and Resolutions of the United Nations Security Council obligate States Parties to cooperate in combating the respective international crimes;

NOTING THAT military and civilian intelligence agencies can largely contribute to assist crime intelligence agencies and law enforcement in general with the prevention of international crime, the interdiction of contraband, the identification of intelligence targets and the execution of special investigative techniques such as controlled deliveries, as well as assisting peace support and peace enforcement operations sanctioned by the United Nations Security Council;

REALISING THAT international cooperation is imperative for the successful combating of international crimes;

RECOGNISING the importance of intelligence-led policing in combating international crime;

ALSO NOTING the convergence of and common areas between international crimes which provide focus areas for regional and international intelligence cooperation to combat international crimes,

HAVE AGREED AS FOLLOWS:

Article 1: Use of terms

For the purposes of this Convention:

1. **"Crimes against humanity"** means the crimes as defined in Part 2 of the *Rome Statute of the International Criminal Court*;
2. **"Crimes relating to the proliferation of weapons of mass destruction'** means the contravention of prohibitions enacted in national laws by States prohibiting any non-state actor to manufacture, acquire, possess, develop, transfer or use nuclear, chemical or biological weapons and their means of delivery, interpreted within the context of the Treaty on the Non-Proliferation of Nuclear Weapons, the Convention on the Development, Production, Stockpiling, and the Use of Chemical Weapons and their Destruction, and the Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and their Destruction;
3. **"Fusion"** means the management of the flow of information and intelligence across levels and sectors of government and private industry, in order to establish an intelligence center or creating a computer network, in order to support-
   (a) the implementation of risk-based, information-driven prevention, response, and consequence management programs;
   (b) efforts to address immediate or emerging threat-related circumstances and events;
   (c) the exchange of information from different sources, including law enforcement, public safety, and the private sector;
   (d) the turning of information into meaningful and actionable intelligence and information;
   (e) the identification of emerging crime threats; and

(f) ongoing efforts to address criminal activities.

3. **"Genocide"** means the crime defined in Part 2 of the Rome Statute of the International Criminal Court;

5. **"ICPO-INTERPOL"** means the International Criminal Police Organisation;

6. **"International crimes"** means crimes against humanity, crimes relating to the proliferation of weapons of mass destruction, mercenary crimes, genocide, organised crime, mercenary crimes, piracy, terrorist crimes, and war crimes;

7. **"Mercenary crimes"** means the recruitment, use, financing or training of mercenaries as well as the direct participation by a mercenary as defined in Article 1 of the International Convention against the Use, Financing and Training of Mercenaries in hostilities or in a concerted act of violence[1];

8. **"Organised crime"** means the planned commission of criminal offences determined by the pursuit of profit and power which, individually or as a whole, are of considerable importance and involve more than two persons, each with his/her own assigned tasks, who collaborate for a prolonged or indefinite period of time-

   (a) by using commercial or business-like structures,

   (b) by using force or other means of intimidation; or

   (c) by exerting influence on politics, the media, public administration, judicial authorities or the business sector.

9. "**Piracy"** means the crime defined in section 101 of the United Nations Convention on the Law of the Sea, committed by an individual or a group of individuals;

10. **"Terrorist crimes"** means any acts or omissions that are committed in whole or in part with the intention of intimidating the public, or a segment of the public, with regard to its security, including its economic security, or compelling a person, government or a domestic or an international organisation to do or refrain from doing any act, whether the public or the

[1] The developments to regulate the issue of private military and private security companies may be factored into this definition See UN, 2008(b).

person, government or organisation is in or outside the country where the crime is committed, and that intentionally-

(a) Causes death or serious bodily harm to a person by the use of violence;
(b) endangers a person's life;
(c) causes a serious risk to the health, or safety of the public or any segment of the public;
(d) causes substantial property damage, whether to public or private property, if causing such damage is likely to result in the conduct or harm referred to in any of paragraphs (a) to (c); or
(e) causes serious interference with or serious disruption of an essential service, facility or system, whether public or private, other than as a result of advocacy, protest, dissent or stoppage of work that is not intended to result in the harm referred to in paragraphs (a) to (c); and

any conspiracy, attempt or threat to commit an act or omission described above; and

11. **"War crimes'** means the crimes defined in Part 3 of the Rome Statute of the International Criminal Court.

Article 2: Scope and objects

1. The scope of this Convention is to promote intelligence cooperation between-

(a) Intelligence agencies on an interagency level (inclusive of military, civilian and crime intelligence agencies) within States Parties;
(b) States Parties on a bilateral level;
(c) States Parties and relevant regional and international organisations involved in the combating of international crime; and
(d) regional and international organisations.

2. The object of the intelligence cooperation referred to in Article 2 is to prevent and investigate international crime and not in support of covert action.

Article 3: Measures against abuse of Convention

1. States Parties undertake, in respect of intelligence cooperation in terms of this Convention-
   (a) not to condone the use of torture or mistreatment;
   (b) to use caveats and assurances in cases where torture or mistreatment is foreseen, in order to prevent torture or mistreatment;
   (c) when such caveats and assurances are not enough to minimise the risk of abuse or torture, senior management or ministerial approval must be obtained;

2. States Parties shall consider the establishment of similar reporting and oversight mechanisms in respect of civilian, crime and military intelligence agencies.

Article 4: Legal framework for combating international crimes

1. States Parties undertake to, where it has not yet been done yet, consider becoming Parties to all international instruments pertaining to the prevention and combating of international crime and to take the required steps to effectively implement such international instruments in their national territories.
2. States Parties shall in particular consider enacting laws to empower law enforcement agencies to apply special investigative techniques of

undercover operations, surveillance, including electronic surveillance and controlled deliveries in order to combat international crimes.

3. States Parties shall consider promoting the conclusion of bilateral agreements on police cooperation, and the exchange of information based on the INTERPOL Model Police Cooperation Agreement with countries sharing common international crime threats.

Article 5: Management, use and exchange of criminal information

1. States Parties shall develop policies, structures and methods for the fusion of intelligence between civilian, military and crime intelligence agencies from the local to regional and national levels, the coordination of intelligence activities and the dissemination and use of intelligence to combat international crime.
2. The fusion of intelligence shall not only be focused on international crimes, but an all-crimes approach shall be followed, in order to also serve the local communities' interest and to detect shared illicit nodes between different crimes.
3. States Parties shall consider the closest possible cooperation between civilian, military and crime intelligence agencies, as well as customs, immigration and revenue services in respect of the identification of suspected criminals, the tracing of fugitives, the identification of opportunities for controlled delivery, and the interdiction of contraband.
4. For the purposes of this Article States Parties shall develop a trusted information environment to develop trust between agencies, and also to promote an attitude of cooperation between agencies.
5. States Parties shall consider to fully participate in regional civilian, crime and military intelligence organisations, including contributing to joint databases, the development of regional crime threat analyses and identification of matters for joint investigation.

6. States Parties shall assist with the establishment of, participate in, and cooperate with joint investigation teams set up to address mutual international crime threats identified through regional and international crime threat analysis and subject to the coordination of relevant regional and international crime combating organisations.
7. States Parties shall use the secure INTERPOL communications network for the exchange of crime information and contribute and maximally use INTERPOL databases in particular the MIND/FIND system.
8. Joint investigation teams must respect the sovereignty of States Parties, which through their best endeavours must facilitate the investigations of joint investigation teams.
9. The focus of intelligence activities related to this Convention shall be on the common areas and convergence of international crimes, including-
   (a) Travel information, mail and courier services, customs transactions and documents and companies or legal entities which could possibly serve as front companies;
   (b) illicit nodes which can be shared by criminals including obtaining forged passports, drivers' licences and fraudulent documents, obtaining the assistance of dishonest accountants and bankers for money laundering or money transfers, illegally obtaining firearms and explosives; and setting up training camps and safe houses;
   (c) communications, including cryptology used by criminals involved in international crime;
   (d) the shared use of technology by criminals involved in international crimes;
   (e) violence and corruption as indicators of common areas between the respective international crimes;
   (f) financial transactions and money-laundering;
   (g) organisational structures and goals of criminal organisations;
   (h) cultural links between suspected criminals;
   (i) acts to gain popular support; and

(j) typical trust gaining actions committed by criminals.

Article 6: Regional and international intelligence cooperation

1. States Parties shall contribute crime intelligence to relevant regional organisations and to ICPO-INTERPOL and cooperate in the analysis thereof in order to develop regional and international crime threat analysis.
2. States Parties shall consider the granting of immunities and privileges to INTERPOL officials of the INTERPOL General Secretariat and INTERPOL Regional Bureaus to protect information in their possession, to protect them against search, seizure and arrest where they act in the scope of their duties on behalf of INTERPOL. Such immunity shall not include members of national police and law enforcement agencies attached to INTERPOL National Central Bureaus of States Parties.

3. States Parties undertake to provide information to the United Nations and the specialised agencies thereof-
   (a) in support of peacekeeping and peace support missions approved by the United Nations Security Council;
   (b) to enforce United Nations Security Council Chapter 7 Resolutions in respect of the combating and prevention of terrorism, and the proliferation of weapons of mass destruction; and
   (c) to enforce sanctions of the United Nations, including sanctions in respect of travel bans, the supply of arms and asset freezing in terms of Chapter 7 Resolutions of the United Nations Security Council.
4. ICPO-INTERPOL, Regional economic integration organisations and agencies of the United Nations involved in the combating of international crimes, undertake to, subject to the Constitutive rules applicable to them-
   (a) Conclude bilateral and multilateral agreements between each

other in respect of intelligence cooperation and coordination;

(b) the development of Regional, and where applicable, international crime threat assessments in respect of international crimes;

(c) the development of strategies to address those threats;

(d) the identification of projects which could be investigated by Joint Task Teams formed in collaboration with the national police and law enforcement agencies of the States Parties directly affected by the particular international crimes.

Article 7: Good practices to protect human rights

States Parties, when reviewing their legal and institutional frameworks for intelligence services and their oversight, will consider the good practices proposed by the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism (Human Rights Council Document A/HRC/14/46)[2], dated 5 May 2010, in order to ensure respect for human rights by intelligence agencies while countering terrorism.

Article 8: Settlement of disputes

States Parties shall endeavour to settle disputes concerning the interpretation or application of this Convention through negotiation.

[2] UN, 2010.

Article 9: Signature, ratification, acceptance, approval and accession[3]

1. This Convention shall be open to all States for signature from ……..until……at the United Nations Headquarters in New York.
2. This Convention shall also be open for signature by regional economic integration organisations, ICPO-INTERPOL, and agencies of the United Nations involved in the combating of international crimes.
3. This Convention is subject to ratification, acceptance or approval.
4. This Convention is open for accession by ICPO-INTERPOL, any agency of the United Nations involved in the combating of any international crime or any any State or any Regional economic integration organisation of which at least one member State is a Party to this Convention. At the time of its accession, any organisation referred to above shall declare the extent of its competence with respect to the matters governed by this Convention. Such organisation shall also inform the depository of any relevant modification in the extent of its competence.

Article: 10: Entry into force

1. This Convention shall enter into force on the ninetieth day after the date of deposit of the fortieth instrument of ratification, acceptance, approval or accession. For the purpose of this paragraph, any instrument deposited by a regional economic integration organisation shall not be counted as additional to those deposited by any Member State of such organisation.
2. For each State or regional economic integration organisation ratifying or accepting, approving or acceding to this Convention after the deposit of the fortieth instrument of such action, this Convention shall

[3] Articles 8 to 12 are based on the wording of the United Nations Convention Against Transnational Organised Crime. Some provisions such as those related to amendment have been omitted for purposes of this study.

enter into force on the thirtieth day after the deposit by such State or organisation of the relevant instrument.

Article 11: Denunciation

1. A State Party may denounce this Convention by written notification to the Secretary-General of the United Nations. Such denunciation shall become effective one year after the date of receipt of the notification by the Secretary-General.
2. A regional economic integration organisation shall cease to be a Party to this Convention when all of its Member States have denounced it.

Article 12: Depository

1. The Secretary-General of the United Nations is designated the depository of this Convention.
2. The original of this Convention shall be deposited with the Secretary-General of the United Nations.

IN WITNESS WHEREOF, the undersigned plenipotentiaries, being duly authorised thereto by their respective Governments, have signed this Convention.

SUMMARY

TITLE: Intelligence and intelligence cooperation in combating international crime: selected case studies.
by
Philippus Christoffel Jacobs.
SUPERVISOR: Prof. M. Hough.
DEPARTMENT: Political Sciences, University of Pretoria.
DEGREE: Doctor Philosophiae (International Relations).

This study firstly focuses on the response to the post-Cold War era with the shift of the focus of intelligence to terrorism, proliferation of weapons of mass destruction, and transnational organised crime. Intelligence cooperation in respect of international crimes, including mercenary crimes, piracy and war crimes, crimes against humanity and genocide is analysed, as well as peacekeeping intelligence. Secondly the focus is on intelligence cooperation in response to the events of 11 September 2001 in the United States of America, and intelligence failures in respect of weapons of mass destruction in Iraq. Intelligence cooperation on the national level is analysed with reference to the United Kingdom and the United States of America; on regional level, with reference to the African Union, the European Union and South East Asia; and on international level with reference to INTERPOL and the United Nations. International and regional obligations in respect of intelligence cooperation are described and analysed and both the drivers of intelligence cooperation and the challenges to intelligence cooperation are analysed. Best practices are identified and proposals made to improve intelligence cooperation on the mentioned levels, in combating international crimes, including a high degree of cooperation between crime intelligence and positive intelligence.

Key terms: Intelligence, intelligence cooperation, intelligence coordination, intelligence fusion, crime intelligence, law enforcement cooperation, positive intelligence, regional intelligence cooperation, international crime.

OPSOMMING

ONDERWERP: **I**ntelligensie en intelligensiesamewerking ter bekamping van internasionale misdaad: geselekteerde gevallestudies.

deur

Philippus Christoffel Jacobs.

STUDIELEIER: Prof. M. Hough.

DEPARTEMENT: Politieke Wetenskappe, Universiteit van Pretoria.

GRAAD: Doctor Philosophiae (Internasionale Verhoudinge).

Hierdie studie fokus eerstens op die reaksie in die tydperk na die Koue Oorlog met die verskuiwing van die fokus van intelligensie na terrorisme, proliferasie van wapens van massavernietiging, en georganiseerde misdaad. Intelligensiesamewerking ten opsigte van internasionale misdade, insluitende ook huursoldatemisdade, seerowery en oorlogsmisdade, misdade teen die mensdom en volksmoord is geanaliseer, asook intelligensie oor vredesbewaring. Tweedens is die fokus op intelligensiesamewerking ‘n reaksie op die gebeure van 11 September 2001 in die Verenigde State van Amerika, en intelligensiemislukkings ten opsigte van wapens van massavernietinging in Irak. Intelligensiesamewerking op die nasionale vlak is geanaliseer met verwysing na die Verenigde Koninkryk en die Verenigde State van Amerika; op streeksvlak met verwysing na die Afrika Unie, die Europese Unie en Suid-Oos Asië, en op internasionale vlak met verwysing na INTERPOL en die Verenigde Nasies. Internasionale-en streeksverpligtinge ten opsigte van intelligensiesamewerking is beskryf en geanaliseer en beide die faktore wat intelligensiesamewerking bevorder en strem is geanaliseer. Modelpraktyke is geïdentifiseer en voorstelle gemaak om intelligensiesamewerking op vermelde vlakke te verbeter ten einde internasionale misdade te bekamp, insluitende ‘n hoë vlak van samewerking tussen misdaadintelligensie en positiewe intelligensie.

Sleutelterme: Intelligensie, intelligensiefusie, intelligensiekoördinering, intelligensie-samewerking, internasionale misdaad, misdaadintelligensie, positiewe intelligensie, streeks-intelligensiesamewerking, wetstoepassingssamewerking.

BIBLIOGRAPHY

1. PRIMARY SOURCES

1.1. INTERNATIONAL INSTRUMENTS

AU. 1977. *OAU Convention for the Elimination of Mercenarism in Africa.* [online]. Available at: http://www.africaunion.org/root/AU/Documents/Treaties/Text/Convention_on_Mercenaries.pdf [Accessed 20 March 2008].

AU. 1999. *OAU Convention on the Combating and Prevention of Terrorism.* [online]. Available at: http://www.africa-union.org/root/au/Documents/Treaties/Text/Algiers_convention%20on%20Terrorism.pdf [Accessed 2 March 2009].

AU. 2004(a). *Protocol to the OAU Convention on the Combating and Prevention of Terrorism.* [online]. Available at: http://www.africaunion.org/root/au/Documents/Treaties/Text/The%20Protocol%20on%20Terrorism%2026July2004.pdf [Accessed 2 March 2008].

AU. 2005(a). *African Union Non-Aggression and Common Defence Pact.* [online] Available at: http://www.africaunion.org/root/au/Documents/Treaties/text/Non%20Agression%20Common%20Defence%20Pact.pdf [Accessed 2 March 2009].

Europol. 2008(a). *Europol Convention: Consolidated version.* [online]. Available at: http://www.europol.europa.eu/legal/EuropolConventionConsolidated_version.pdf [Accessed 18 September 2007].

IAEA. 1959. *The Texts of the Agency's Agreements with the United Nations.* Information Circular. Reference: INFCIRC/11. 30 October.

International Committee of the Red Cross. 1989. *International Convention against the Recruitment, Use, Financing and Training of Mercenaries.* 4 December. [online] Available at: http://www.icrc.org/ihl.nsf/FULL/530?OpenDocument [Accessed 26 March 2008].

INTERPOL. 2001. *Co-operation Agreement between INTERPOL and Europol.* [online]. Available at: http://www.interpol.int/Public/ICPO/LegalMaterials/cooperation/agreements/Europol2001.asp [Accessed 11 November 2008].

INTERPOL. 2007(a). *ICPO-INTERPOL Constitution.* [online]. Available at: http://www.interpol.int/Public/ICPO/LegalMaterials/constitution/constitutionGenReg/constitution.asp [Accessed on 11 November 2008].

INTERPOL. 2008(a). *Agreements with Other International Organizations* [online]. Available at: http://www.interpol.int/Public/ICPO/LegalMaterials/cooperation/AgrList.asp [Accessed 23 September 2008].

INTERPOL. 2009(a). *The United Nations and the International Criminal Police Cooperation Organization (INTERPOL).* [online]. Available at: http://www.interpol.int/Public/ICPO/LegalMaterials/cooperation/agreements/UN1997.asp [Accessed 12 October 2009].

INTERPOL. 2009(b). *Agreement Concerning Access by UNMIK to INTERPOL's Telecommunications Systems and Databases* [online]. Available at: http://www.interpol.int/Public/ICPO/LegalMaterials/cooperation/agreements/UNMIK.asp [Accessed 12 October 2009].

INTERPOL. 2009(c). *Cooperation Agreement between the International Criminal Police Organization –INTERPOL and the Special Court for Sierra Leone.* [online]. Available at: http://www.interpol.int/Public/ICPO/LegalMaterials/cooperation/agreements/SierraLeonecourt.asp [Accessed 12 October 2009].

INTERPOL. 2009(d). *Interim Agreement between the Special Tribunal for Lebanon and the International Criminal Police Organisation–INTERPOL.* [online]. Available at: http://www.interpol.int/Public/ICPO/LegalMaterials/cooperation/agreements/ TSL-OIPC.pdf [Accessed 12 October 2009].

INTERPOL. 2009(e). *Co-operation Agreement between the Office of the Prosecutor of the International Criminal Court and the International Criminal Police Organization – INTERPOL* [online]. Available at: http://www.interpol.int/Public/ICPO/LegalMaterials/cooperation/agreements/ICC2005.asp [Accessed 12 October 2009].

INTERPOL. 2009(f). *Co-operation Agreement between the National Atomic Energy Agency and the International Criminal Police Organization- INTERPOL.* [online]. Available at: http://www.interpol.int/Public/ICPO/LegalMaterials/cooperation/agreements/INTERNATIONALATOMICENERGYAGENCY200604. asp [Accessed 12 October 2009].

INTERPOL. 2009(g). *Agreement of Co-operation between the International Maritime Organization and the International Criminal Police Organization* [online]. Available at: http://www.interpol.int/Public/ICPO/LegalMaterials/cooperation/agreements/InternationalMaritimeOrganization.pdf [Accessed 17 October 2009].

OPBW. 2006. *Convention on the Prohibition of the Development and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on Their Destruction 1972.* [online]. Available at: http://www.opbw.org/convention/documents/btwctext.pdf [Accessed 25 October 2009].

OPCW. 2005. *Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and Their Destruction 1993.* [online].

Available at: http://www.opcw.org/chemical-weapons-convention/download-the-cwc/ [Accessed 25 October 2009].

Organisation of American States. 1933. *Montevideo Convention on the Rights and Duties of States.* Adopted by the Seventh International Conference of American States. OAS Law and Treaty Service, No. 37.

RSA. 1997. *Agreement in Respect of Cooperation and Mutual Assistance in the Field of Crime Combating.* [online]. Available at: http://www.saps.gov.za/docsubls/legislation/mou/_mutual_assistanc.pdf [Accessed 2 March 2009].

SADC. 2002(a). *Protocol on Mutual Assistance in Criminal Matters.* [online]. Available at: http://www.sadc.int/index/ save/page/156 [Accessed 20 September 2009].

SADC. 2002(b). *Protocol on Extradition.* [online]. Available at: http://www.sadc.int/index/save/page/148 [Accessed 20 September 2009].

UN. 1982. *United Nations Convention on the Law of the Sea.* [online]. Available at: http://www.un.org/Depts/los/conventionagreements/ texts/unclos/closindx. htm [Accessed 26 July 2008].

UN. 1988. *Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (*[online]. Available at: http://www.unodc.org/pdf/convention_1988_en.pdf [Accessed 18 August 2007].

UN. 1999 - 2003. *Rome Statute of the International Criminal Court*. [online]. Codification Division: Office of Legal Affairs. Available at: http://untreaty.un.org/cod/icc/statute/romefra.htm [Accessed 1 May 2008].

UN. 2000. *Non-proliferation Treaty.* [online]. Available at: http://www.un.org/events/npt2005/npttreaty.html [Accessed 31 May 2008].

UN. 2001(a). *International Instruments related to the Prevention and Suppression of International Terrorism.* New York. US.

UN. 2004(a). *United Nations Convention against Transnational Organized Crime and the Protocols thereto.* E-Book. UN Office on Drugs and Crime. Vienna. UN. New York. US.

UN. 2005(a). *Draft Comprehensive Convention against International Terrorism.* Letter dated 3 August 2005 from the Chairman of the Sixth Committee addressed to the President of the General Assembly. Document A/59/894 12 August. New York. US.

UN. 2007(a). *International Instruments to Counter Terrorism* [online]. Available at: http://www.un.org/terrorism/ instruments.html [Accessed 18 August 2007].

1.2. RESOLUTIONS OF INTERNATIONAL ORGANISATIONS

AU. 2004(b). *Decision of the Executive Council and Assembly at Summit dated 30 June to 3 July.* ASS/AU/Dec.36 and EX,CL/Dec.145, Decision: DOC.EX.CL/106(V). Addis Ababa. Ethiopia.

AU. 2005(b). *Decisions and Declarations: Fourth Ordinary Session.* Assembly of the AU. Document No. Assembly/AU/Dec.55-72(IV)/ Assembly/AU/Dec.1-2)(IV). 30 - 31 January. Abuja. Nigeria.

UN. 2001(b). *Resolution 1373(2001).* Adopted by the UN Security Council at its 4385th Meeting on 28th September. Security Council. Document No. S/RES 1373(2001). New York. US.

UN. 2004(b). *Resolution 1540(2004).* Adopted by the UN Security Council at its 4956th Meeting on 28 April. Security Council. Document **S**/RES1540(2004). New York. US.

UN. 2006. *Measures to Eliminate International Terrorism.* General Assembly. Document A/61/210, 1 August. New York. US.

UN. 2008(a). *Resolution 1851(2008).* Security Council. Document No. S/Res. 1851(2008). 16 December. New York. US.

UN. 2008(b). *Resolution by the General Assembly on the Report of the 6th Committee.* Document Reference: A62/455A/RES61/72. 8 January. New York. US.

UN. 2008(c). *UN Action to Counter Terrorism.* [online]. Available at: http://www.un.org/terrorism/instruments.shtml [Accessed 31 May 2008].

UN. 2008(d). *Montreux Document on Pertinent International Humanitarian Legal Obligations and Good Practices for States related to Operations of Private Military and Security Companies during Armed Conflict.* General Assembly and Security Council. Document No. A/63/467-S/2008/636. 6 October. Washington. US.

UN. 2009(a). *Resolution 1874(2009).* Security Council. Document Res. 1874. 12 June. New York. US.

1.3. LEGISLATION AND EXECUTIVE ORDERS

US. 1968. *Omnibus Crime Control and Safe Streets Act. Title III. Public Law 19 – 351.* [online]. Available at: http://www.fcc.gov/Bureaus/OSEC/library/legislative_histories/1615.pdf [Accessed 6 February 2010].

US. 2002(a). *Title 18: Crimes and Criminal Procedure, Part 1, Chapter 45: Foreign Relations, Section 951.* Available online at: http://www.wais.access.gpo.gov [Accessed 21 December 2008].

US. 2009. *Executive Order - Review and Disposition of Individuals Detained at the Guantánamo Bay Naval Base and Closure of Detention Facilities.* [online]. Available at: http://www.whitehouse.gov/the_press_office/ClosureOfGuantanamoDetention Facilities/ [Accessed 9 February 2009].

1.4. PROGRAMMES, POLICIES AND STRATEGIES

ASEAN. 2002. *Work Programme to Implement the ASEAN Plan of Action to Combat Transnational Crime.* [online]. Available at: http://www.aseansec.org/5953.htm [Accessed 25 October 2008].

ASEAN. 2006. *ASEAN-Canada Joint Declaration for Cooperation to Combat International Terrorism.* [online]. Available at: http://www.aseansec.org/18596.htm [Accessed 18 June 2007].

Canada. 2007. *Foreign Affairs and International Trade Canada: 32-Point Action Plan.* [online]. Available at: http://geo.international.gc.ca/can-am/main/border/32_point_action_-en.asp [Accessed 18 September 2007].

EU. 2004. *Communication from the Commission to the Council and the European Parliament towards Enhancing Access to Information by Law Enforcement*

Agencies (EU Information Policy). Commission of the European Communities. Document Reference: COM(2004)429 final. 16 June. Brussels. Belgium.

EU. 2005. *Joint Investigation Teams- Proposal for Designation of National Experts.* Council of the European Union. Document No. 11037/05 of 8 July. Brussels. Belgium.

NATO. 1999. *The Alliance's Strategic Concept.* [online]. Available at: http://www.nato.int/cps/en/natolive/officialtexts_27433.htm?selectedLocale=en [Accessed 23 September 2009].

SADC. 2001. *Strategic Indicative Plan for the Organ on Politics, Defence and Security Cooperation.* Gaborone. Botswana.

UK. 2006(a). *Countering International Terrorism: The United Kingdom's Strategy.* The Stationery Office. Norwich. UK.

UK. 2008(a). *The National Security Strategy of the United Kingdom: Security in an Interdependent World.* The Stationery Office. Norwich. UK.

UK. 2009(a). *The United Kingdom Strategy for Countering International Terrorism.* The Stationery Office. Norwich. UK.

US. 2003(a). *The National Criminal Intelligence Sharing Plan.* Department of Justice. Global Justice Information Sharing Initiative. [online]. Available at: http://it.ojp.gov/documents/NCISP_Plan.pdf [Accessed 13 June 2007].

US. 2005(a). *Intelligence–led Policing: The New Intelligence Architecture.* Department of Justice. Office of Justice Programs. Bureau of Justice Assistance. Washington, DC. US.

US. 2005(b). *The National Intelligence Strategy of the United States of America.* Office of the Director of National Intelligence. Washington, DC. US.

US. 2007(a). *National Strategy for Information Sharing: Successes and Challenges in Improving Terrorism-Related Information Sharing.* The White House. Washington, DC. US.

US. 2007(b). *Department of Defence Information Sharing Strategy.* US. Department of Defence Information Sharing Executive. Office of the Information Officer. Washington DC. US.

US. 2008(a): *United States Intelligence Community: Information Sharing Strategy.* Office of the Director of National Intelligence. Washington, DC. US.

US. 2008(b). *Department of Homeland Security Information Sharing Strategy.* Information Sharing Governance Board. Department of Homeland Security. Washington, DC. US.

1.5. COMMISSIONS, INQUIRIES AND REPORTS

Asia-Pacific Economic Cooperation. 2003. *ASEAN Efforts to Combat Terrorism.* Report of Asian-Pacific Economic Cooperation Secretariat on Counter Terrorism Task Force Meeting. Document No. 2003/SOMIII/CTTF/038. August 2003. Phuket. Thailand

AU. 2008. *Meeting the Challenge of Conflict Prevention in Africa: Towards the Operationalisation of the Continental Early Warning System.* Conflict Management Division of the Peace and Security Department of the African Union (ed.). Addis Ababa. Ethiopia.

Canada: Solicitor-General. (No date). *Alternative Approaches to Combating Transnational Crime.* Canada. Schneider, S.; Beare, M.; & Hill, J. in Report of the Federal Transnational Crime Working Group. [online]. Available at: http://www.ncjrs.gov/nathanson/ etranscrime.html [Accessed 3 June 2007].

Canada. 2006(a). *Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar. A New Review Mechanism for the RCMP's National Security Activities.* Publishing and Depository Services. Public Works and Government Services. Canada. Ottawa. Canada.

Europol. 2006. *Europol Annual Report 2006.* Europol Corporate Communications. The Hague. The Netherlands.

Europol. 2007(a). *EU Terrorism Situation and Trend Report.* Europol Corporate Communications. The Hague. The Netherlands.

Europol. 2007(b). *EU Organised Crime Threat Assessment 2007.* Corporate Communications. The Hague. Netherlands.

Europol. 2008(b). *EU Organised Crime Threat Assessment: 2008.* The Hague. The Netherlands.

Europol. 2009(a). *Europol Annual Report 2008.* The Hague. The Netherlands.

Europol. 2009(b). *EU Terrorism Situation and Trend Report.* Europol. The Hague. The Netherlands.

ICC-International Maritime Bureau. 2009(a). *Piracy and Robbery against Ships.* Annual Report: 1 January – 31 December 2008. London. UK.

ICC-International Maritime Bureau. 2009(b). *Piracy and Robbery against Ships.* Period: 1 January – 30 June 2009. London. UK.

RSA. 1999. *Project 105: Report: The Interception and Monitoring Prohibition Act, 1992 (Act 127 of 1992).* South African Law Reform Commission. Pretoria. RSA.

Sweden. *2006.* The Weapons of Mass Destruction Commission (WMDC). *Weapons of Terror: Freeing the World of Nuclear, Biological and Chemical Weapons.* [online]. Stockholm. Available at: http://www.wmdcommission.org. [Accessed 24 May 2008].

UK. 2004. *Report of a Committee of Privy Councilors: Review of intelligence on Weapons of Mass Destruction.* [online]. Available at: http://www.butlerreview.org.uk/ [Accessed 20 July 2007].

UK. 2006(b). *Report into the London Terrorist Attacks on 7 July 2005.* Intelligence and Security Committee. The Stationery Office. Norwich. UK.

UK. 2007(a). *Rendition.* Intelligence and Security Committee. Her Majesty's Stationery Office. Norwich. UK.

UK. 2008(b). *Privy Council of Review of Intercept as Evidence: Report to the Prime Minister.* The Stationery Office. Norwich. UK.

UK. 2009(b). *SOCA Annual Report 2008/2009.* Serious Organised Crime Agency [online]. Available at: http://www.soca.gov.uk [Accessed on 21 July 2009].

UK. 2009(c). *Could 7/7 Have Been Prevented? Review of the Intelligence on the London Terrorist Attacks on 7 July 2005.* Intelligence and Security Committee. The Stationery Office. Norwich. UK.

UN. 2005(b). *Report of the International Commission of Inquiry on Darfur to the United Nations Secretary General.* 25 January. Geneva. Switzerland.

UN. 2007(b). *Report of the Ad Hoc Committee Established by the General Assembly Resolution 51/210 of 17 December 1996.* General Assembly. Document A/62/37. 5, 6 and 15 February.

UN. 2007(c). *Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism.* Martin Scheinin: Mission to the United States of America. General Assembly Human Rights Council. Reference Number: A/HRC/6/17/Add.3. 22 November. New York. US.

UN. 2008(e). *Report of the Working Group on the Use of Mercenaries as Means of Violating Human Rights and Impeding the Exercise of the Right of People to Self-determination*. Human Rights Commission. Doc/A/HRC/7/7, 9 January. New York. US.

UN. 2008(f). *Report of the Committee Established Pursuant to Resolution 1540 (2004)*. Security Council. Document Reference: S/2008/493. 30 July. New York. US.

UN. 2008(g). *Report of the Meeting of the UN Open-ended Intergovernmental Expert Working Group on Money-laundering and Judicial Cooperation Held in Vienna from 30 June 2008 to 1 July 2008.* Office for Drugs and Crime. Reference No. UNODC/CND/2008/WG2/3. 9 July.

UN. 2009(b).*Tenth Report of the Analytical Support and Sanctions Implementation Monitoring Team submitted pursuant to Resolution 1822(2008), Concerning Al-Qaida and the Taliban and Associated Individuals and Entities.* Security Council. Document Reference: S/2009/502. 2 October.

UN. 2009(c). *Report of the United Nations Fact Finding Mission on the Gaza Conflict.* Human Rights Council. Document Reference No. A/HRC/12/48. 15 September. Geneva. Switzerland.

UN. 2010. *Report of the Special Rapporteur on the Promotion and Protecting of Human Rights and Fundamental Freedoms, while Countering Terrorism: Martin Scheinin: Compilation of Good Practices on Legal and Institutional Frameworks and Measures that Ensure Respect for Human Rights by Intelligence Agencies while Countering Terrorism.* UN. Human Rights Council. Document A/HRC/14/46. 5 May.

US. 2001. *Report for Congress: Intelligence and Law Enforcement: Countering Transnational Threats to the U.S.* Congressional Research Service. Library of Congress. Order Code. RL30252. 3 December. Washington D.C.

US. 2003(b). *Report for Congress: Domestic Intelligence in the United Kingdom: Applicability of the MI-5 Model to the United States.* Document RL. 31920. Congressional Research Service. Library of Congress. 19 May Washington DC. US.

US. 2003(c). *Report for Congress: The Intelligence Community and 9/11: Congressional Hearings and the Status of the Investigation.* Congressional Research Service. Library of Congress. Order Code RL31650. 16 January. Washington, D.C.

US. 2004(a). *Report for Congress: Disarming Libya: Weapons of Mass Destruction.* Order Code RS21823. Congressional Research Service. Library of Congress. 22 April. Washington, DC. US.

US. 2004(b). *Report of the National Commission on Terrorist Attacks upon the United States.* [online]. Available at: http://fli.findlaw.com/news.findlaw.com/hdocs/docs/911report.pdf [Accessed 30 June 2007].

US. 2005(c). *Report to the President of the United States: Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction*. [online]. Available at: http://govinfo.library.unt.edu/wmd/report/index.html [Accessed 12 August 2009].

US. 2005(d) *Methods and Motives: Exploring Links between Transnational Organized Crime & International Terrorism*. Department of Justice. Office of Justice Programs. Report by Project Team, Shelley L.I., *et al.* Washington DC. US.

US. 2006(a). Report for Congress: *9/11 Commission Recommendations: Implementation Status.* Congressional Research Service. Library of Congress. Order Code. RL 33742. 4 December. Washington, DC. US.

US. 2006(b). *Report for Congress: Homeland Security Intelligence: Perceptions, Statutory Definitions and Approaches.* Congressional Research Service. Library of Congress. Order Code RL33616. 18 August. Washington D. US.

US. 2007(c). *The CIA's Family Jewels* [online]. Available at: http://www.gwu.edu~nsarchiv/NSAEBB/NSAEBB222/family_jewels_full_ocr.pdf [Accessed 13 July 2007].

US. 2008(c). *World at Risk. The Report of the Commission on the Prevention of WMD Proliferation and Terrorism.* Vintage Books. New York. US.

1.6. OFFICIAL HANDBOOKS, MANUALS, CODES OF PRACTICE AND GUIDELINES

ACPO. 2005. *Guidance on the National Intelligence Model.* Centrex, Association of Chief Police Officers Wyboston, Bedford. United Kingdom (UK).

ICTR. 2008. *Best Practices Manual for the Investigation and Prosecution of Sexual Violence Crimes in Situations of Armed Conflict: Lessons from the International Criminal Tribunal for Rwanda.* Arusha. Tanzania.

ICTY-UNICRI. 2009. *ICTY Manual on Developed Practices.* International Criminal Tribunal for Yugoslavia – United Nations Inter-regional Crime and Justice Research Institute. UNICRI Publisher. Turin. Italy.

UK. 2002(a). *Covert Human Intelligence Source Code of Practice.* The Stationery Office. Norwich. UK.

UK. 2002(b). *Covert Surveillance Code of Practice.* The Stationery Office. Norwich. UK.

UK. 2002(c). *Interception of Communications Code of Practice*. The Stationery Office. Norwich. UK.

UK. 2007(b). *Acquisition and Disclosure of Communications Data Code of Practice.* The Stationery Office. Norwich. UK.

UK. 2007(c). *Investigation of Protected Electronic Information Code of Practice.* The Stationery Office. Norwich. UK.

US. 2002(b). *The Attorney General's Guidelines on Federal Bureau of Investigation Undercover Operations.* Department of Justice. 30 May. Washington, DC. US.

US. 2006(c). *Fusion Centre Guidelines: Developing and Sharing Information and Intelligence in a New Era* [online]. Available at: http://it.ojp. gov/documents/ fusion_center_executive-summary.pdf [Accessed 12 June 2007].

US. 2008(d).*The Attorney General's Guidelines.* [online]. Available at: http://epic. org/privacy/fbi [Accessed 17 March 2009].

US. 2008(e). *The Attorney General's Guidelines for Domestic FBI Operations.* Department of Justice. Attorney General. 29 September. Washington DC. US.

1.7. COURT JUDGEMENTS

Canada. 2006(b). Superior Court of Justice. *Case between Her Majesty the Queen and MM Khajawa* Court file No. 04-G30282 11 - 14 December.

ICJ. 2006. *Legality of the Threat or Use of Nuclear Weapons. (Advisory Opinion)*. 8 July. International Court of Justice. The Hague. The Netherlands.

US. 2007(d). *American Civil Liberties Union, et al versus National Security Agency et al.* US Court of Appeal, Sixth Circuit. Case No. 06-2095/2140. 6 July.

US. 2008(f). *Complaint filed in class action in the case of Electronic Foundation and Others versus NSA and Others.* Case No. C 08 4373 CRB. US District Court. Northern District of California. Filed 18 September.

2. SECONDARY SOURCES

2.1. BOOKS

Aid, M.A. 2006. *SIGINT and Peacekeeping: The Untapped Intelligence Resource.* In Rudner, M. *Peacekeeping Intelligence.* Routledge. New York.

Amnesty International. 2001. *Universal Jurisdiction: The Duty of States to Enact and Implement Legislation.* International Secretariat. London. (CD).

Berkowitz, B. 2003. *The New Face Of War: How Wars Will Be Fought In the 21st Century.* The Free Press. New York.

Carter, D.L. 2004. *Law Enforcement Intelligence: A Guide to State, Local and Tribal Agencies.* Michigan State University.

Clark, R.M. 2004. *Intelligence Analysis: The Target-centric Approach.* CQ Press: Congressional Quarterly Inc. Washington.

Carment, D. & Rudner, M. 2006. *Peacekeeping Intelligence: New Players, Extended Boundaries.* Routledge, New York.

Deflem, M. 2004. *Policing World Society: Historical Foundations of International Police Cooperation.* Second Edition. Oxford University Press. Oxford. New York.

De Koster, P. 2005*. Terrorism: Special Investigation Techniques.* Council of Europe Publishing. Strassbourg.

Dillon, M. 1994. *The Enemy Within: The IRA's War against the British.* Doubleday. London.

Eisenberg, D., Dan, U. & Landau, E. 1979. *The Mossad: Israel's Secret Intelligence Service.* Corgi, Transworld Publishers Ltd. London.

Frantz, D. & Collins, C. 2007. *The Nuclear Jihadist: The True Story of the Man Who Sold the World's Most Dangerous Secrets…and How We Could have Stopped Him.* Hatchette Book Group. New York.

Herman, M. 1999. *Intelligence Power in Peace and War.* University Press, Cambridge.

Hulnick, A.S. 1999. *Fixing the Spy Machine: Preparing American Intelligence for the Twenty-First Century.* Praeger Publishers. Westport.

Johnson, L.K. 1991. "Strategic Intelligence: An American Perspective". In Farson, A.S., Stafford, D.E. Wark, W.K. (Eds). *Security and Intelligence in a Changing World: New Perspectives for the 1990's.* Frank Cass Ltd. Oregon.

Johnson, L.K. & Wirtz, J.J. 2004. *Strategic Intelligence: Windows Into a Secret World, An Anthology.* Roxbury Publishing Company, Los Angeles, California.

Kent, S. 1966. *Strategic Intelligence for American World Policy.* Princeton University Press, Princeton, New Yersey.

Klass, P.J. 1971. *Secret Sentries in Space: The First Report on the Secret Satellites Orbited by the United States and the Soviet Union and Their Contribution to International Stability.* Haddon Craftsmen. Scranton Pennsylvania.

Kreijen, G. 2004. *State Failure, Sovereignty and Effectiveness.* Marthinus Nijhoff Publishers. Leiden.

Lowenthal, M.M. (2006). *Intelligence: From Secrets to Policy.* (3rd Edition), CQ Press, Washington D.C.

Nadelmann, E.A. 1993. *Cops Across Borders: The Internationalization of US Criminal Law Enforcement.* Pennsylvania State University Press. Pennsylvania.

Richelson, J.T. 1989. *The U.S. Intelligence Community.* Ballinger. New York.

Reismann, W.M. & Baker, J.E. 1992. *Regulating Covert Action: Practices and Policies of Covert Coercion Abroad in International and American Law.* Yale University Press, New Haven and London.

Scahill, J. 2007. *Blackwater, The Rise of the World's Most Powerful Mercenary Army*. Nation Books, New York.

Settle, R. 1995. *Police Informers.* The Federation Press. Annandale, NSW.

Shulsky, A.N. & Schmitt, G.J. (2002) *Silent Warfare: Understanding the World of Intelligence* (3rd Edition). Brassey's Inc. Washington, D.C.

Stevenson, W. 1976. *Ninety Minutes at Entebbe.* Bantam Books. Keter Publishing House. New York.

Todd, P. & Bloch, J. 2003. *Global Intelligence: The World's Secret Services Today.* Zed Books, London. UK. New York.

Treverton, G.F. 1987. *Covert Action: The CIA and the Limits of American Intervention in the Postwar World.* I.B. Taurus & Co Ltd, Publishers, London.

Van den Wyngaert, C. (ed.) 1996. *International Criminal Law.* Kluwer Law International. The Hague.

Wane, E.G. in AU. 2008. *Meeting the Challenge of Conflict Prevention in Africa: Towards the Operationalisation of the Continental Early Warning System.* Conflict Management Division of the Peace and Security Department of the African Union (ed.). Addis Ababa.

Wilkinson, P. 2006. *Terrorism Versus Democracy.* (2nd Edition). Routledge, Taylor and Francis Group. London, UK and New York.

2.2. THESES, DISSERTATIONS, PAPERS, LECTURES AND SPEECHES

Acharya, A. 2003. *Asian Security after September 11: A View from South-East Asia.* Paper Prepared for the Asia Pacific Foundation of Canada's Roundtable on the Foreign Policy Dialogue and Canada-Asia Relations Nanyang Technological University and York University.

Boardman, C.H. 2006. *Organizational Culture Challenges to Interagency and Intelligence Community Communication and Interaction.* Paper submitted to the Joint Advanced Warfighting School for a Master of Science Degree in Joint Planning and Strategy. Department of Defence, US.

Born, H. 2007. *International Intelligence Cooperation: The Need for Networking Accountability.* Geneva Centre for Democratic Control of Armed Forces (DCAF). [online]. Available at: http://www.dcaf.ch/handbook_intelligence/born-international-intelligence-cooperation-networking-accountability-071006.pdf [Accessed 8 January 2009].

Cave, L. 2002. *The Role of the South African Intelligence Community in Combating Crime with Specific Reference to Organised Crime.* Dissertation for Master of Security Studies. University of Pretoria. Pretoria.

Champagne, B. 2006. *The United Nations and Intelligence.* [online]. Paper Submitted to the United Nations Institute for Training and Research for Certificate-of-Training; United Nations Peace Support Operations. [online]. Available at: http://www.unitarpoci.org/media/champagne.pdf [Accessed 13 July 2007].

Cleary, C.J. 2006. *Strategy for Local Law Enforcement Agencies to Improve Collection, Analysis and Dissemination of Terrorist Information.* Thesis: Submitted for Master of Arts in Security Studies (Homeland Security and Defense) Naval Post-Graduate School. Monterey, California.

Črnčec, D. 2009. *A New Intelligence Paradigm and the European Union*. Paper. [online]. Available at: http://www.fvv.uni-mb.si/varstvoslovje/.../Crncec_VS_2008-4_ang.pdf [Accessed 23 September 2009].

Gerspacher, N. 2002. *International Police Cooperation Institutions as a Response to Transnational Crime: A Study of Institutionalised Effectiveness.* Dissertation for Doctor of Philosophy in Political Science. Graduate University of Illinois, Chicago.

Green, A.W. 2005. *Its Mine! Why the Intelligence Community Does not Share Information.* Research Report. School of Advanced Air and Space Studies. Air University. Maxwell Air Force Base. Alabama.

Herzberger, E.R. 2007. *Counter-terrorism Intelligence Cooperation in the European Union.* UNICRI. European Foreign and Security Studies Policy Program. [online]. Available at: http://www.unicri.it/wwd/security/docs/Intelligence_cooperation_EU.pdf [Accessed 30 October 2008].

Hui, K.B. 2009. *29th ASEANAPOL Conference: Opening Remarks by Mr. Khoo*

Boon Hui, INTERPOL President. 13 May. [online]. Available at: http://www.interpol.int/Public/ICPO/speeches/2009/SpeechKhooASEANAPOL20090513.asp [Accessed 7 September 2009].

Jansen van Rensburg, P.F.B. 2005. *Covert Action as an Option in National Security Policy: A Comparison Between the United States of America and South Africa (1961-2003).* Dissertation for Master of Security Studies. University of Pretoria.

Kasrils, R. 2008. Address by South African Minister for Intelligence Services at Committee of Intelligence and Security Services of Africa (CISSA): Fifth Annual Conference. Cape Town. South Africa. [online]. Available at: http://www.intelligence.gov.za/Speeches/2008/CISSA%20Speech%2022%20May%202008.doc [Accessed 5 November 2008].

Nenneman, M. 2008. *An Examination of State, and Local Fusion Centers and Data Collection Methods.* Thesis for Master of Arts in Security Studies. Naval Postgraduate School. Monterey. California.

Ohr, B.G. 2001. *Effective Methods to Combat Transnational Organized Crime in Criminal Justice Processes. 116th International Training Course Visiting Expert's Papers.* UNAFEI. Resource Material Series. No. 58. Tokyo.

Rimington, S. 1994. *Intelligence, Security and Law.* James Smart Lecture. [online]. Available at: http://www.mi5.gov.uk/output/Page380.html [Accessed 22 June 2008].

Ryan, K.J. 2006. *Criminal intelligence in the European Union: Evaluating the Process Efficiencies of Cooperation and Coordination.* Dissertation for Doctor of Philosophy. Washington University, St. Louis, Missouri.

Saccone, A. 2006. *Combating International Crime in an Enlarging European Union: What is the Role of Europol?* Head of the Crime Analysis Unit of Europol. Lecture in the International Seminar for Experts. 15 December.

Venzke, N.C. 1983. *Statement by Rear-Admiral Norman C. Venzke, Chief Office of Operations US Coast Guard Before the House Judiciary Committee, Sub-Committee on Crime.* July 28. US. [online] Available at: http://testimony. ost.gov/test/ passtest/83testvenkel.pdf [Accessed 28 May 2009].

Walsh, J.I. 2009. *Security Policy and Intelligence Cooperation in the European Union.* Paper prepared for the biennial meeting of the European Union Studies Association. Los Angeles. US. [online]. Available at: http://www.unc.edu/euce/ eusa2009/papers/walsh_12C.pdf [Accessed 20 September 2009].

Wetzling, T. 2006. *The Democratic Control of Intergovernmental Intelligence Cooperation.* DCAF. Working Paper No. 165. Geneva.

2.3. JOURNAL ARTICLES, PERIODICALS, MONOGRAPHS AND REFERENCE WORKS

Acharya, A. 1991. “The Association of Southeast Asian Nations: ‘Security Community’ or ‘Defence Community’?” *Pacific Affairs.* Vol. 64. No. 2. pp. 159 - 178.

Aldridge, R.J. 2004. “Transatlantic Intelligence and Security Cooperation.” *International Affairs.* Vol. 80. No. 4. pp. 731 – 753.

Aqua, J.A. 2007. “National Security Evidence and Terrorism Prosecutions: Cooperation Between the United States and the United Kingdom”. *United States Attorneys’ Bulletin*. Vol. 55. No. 2. pp. 32 – 40.

Baker, T. 2007. *Biometrics for Intelligence-led Policing.* [online] Baker Associates. International Consultants. Available at: http://www.parl.gc.ca/37/1/parlbus/commbus/senate/com-e/defe-e/pdf/18issue.pdf [Accessed 10 June 2008].

Bassiouni, M.C. 1996. "International Crimes; Jus Cogens and Obligation Erga Omnes". *Law and Contemporary Problems.* Vol. 59. No. 4. pp. 63 – 74.

Benyon, J. 1994. "Policing the European Union: The Changing Basis of Cooperation on Law Enforcement". *International Affairs.* Vol. 70. No. 3. pp. 497 – 517.

Berman, J. & Flint, L. 2003. "Guiding Lights: Intelligence Oversight and Control for the Challenge of Terrorism". *Criminal Justice Ethics.* Winter/Spring. Pp. XXX - ZZZ.

Björnehed, E. 2004. "Narco-Terrorism: The Merger of the War on Drugs and the War on Terror". *Global Crime.* Vol. 6. No. 3 & 4. pp. 305 - 324.

Brady, H. 2008. "Europol and the European Criminal Intelligence Model: A Non-state Response to Organized Crime". *Policing*. Vol. 2. No. 1. pp.103 -109.

Bradberry, D. 2006. Civilian and *Military Intelligence: A Necessary Dichotomy.* Commentary *and Analysis.* AmericanDiplomacy.org [online] Available at: http://www.unc.edu/deptws/diplomat/item/2006/0406/brad/bradberry_civil.html [Accessed 28 May 2008].

Brodeur, J.P. 2007. "High and Low Policing in Post- 9/11 Times". *Policing.* Vol. 1. No. 1. pp. 25 – 37.

Burch, J. 2007. "A Domestic Intelligence Agency for the United States? A Comparative Analysis of Domestic Intelligence Agencies and their Implications for Homeland Security". *Homeland Security Affairs*. Volume 3. No. 2. pp.1 - 26.

Choo, A.L-T. & Mellors, M. 1995. "Undercover Police Operations and What the Suspect Said (or Didn't Say)". *Web Journal of Current Legal Issues.* [1995] 2. [online]. Available at: http://www.ncl.ac.uk/~nlawwww/articles2/choo2.html [Accessed 17 March 2009].

Cline, L.E. 2002. "Operational Intelligence in Peace Enforcement and Stability Operations". *International Journal of Intelligence and CounterIntelligence.* Vol. 15. No. 2. pp. 179 -174.

Clough, C. 2004. "Quid Pro Quo: The Challenges of International Strategic intelligence Cooperation". *International Journal of Intelligence and CounterIntelligence.* Vol. 17. No. 4. pp. 601 - 613.

Cole, D. & Lederman, M.S. 2006. "The National Security Agency's Domestic Spying Program: Framing the Debate". *Indiana Law Journal.* American Constitution Society for Law and Policy. Vol. 81 (May). pp. 1356 – 1424.

Coalition for the International Criminal Court. 2007. *The ICC and the Crime of Aggression*. 17 May [online]. Available at: http://www.iccnow.org/documents/CICCFSCrime_of_Agression_Factsheet_FINAL_Eng_1May07 [Accessed 1 May 2008].

Cutting, P.D. 1983. "The Technique of Controlled Delivery as a Weapon in Dealing with Illicit Traffic in Narcotic Drugs and Psychotropic Substances". *UNODC- Bulletin on Narcotics.* Issue 4. No. 002. pp. 15 - 22.

Das, D.K. & Kratcoski, P. 1999. "International Police Cooperation: A World Perspective". *Policing: An International Journal of Police Strategies and Management .* Vol. 22. No. 2. pp. 214 - 242.

Deflem, M. 2006. "Global Rule of Law or Global Rule of Law Enforcement? International Police Cooperation and Counter-terrorism". *The ANNALS of the American Academy of Political and Social Science.* Vol. 603. pp. 240 – 251.

Dorn, A.W. 1999. "The Cloak and the Blue Beret: Limitations on Intelligence in U.N. Peacekeeping". *International Journal of Intelligence and Counter-Intelligence.* Volume 12. No. 4. pp. 414 – 447.

Fagersten, B. 2007. *Multilateral Intelligence Cooperation: An Institutional Approach.* [online]. Available at: http://owww.essex.ac.uk.innopac.up.ac.za/ecpr/events/generalconference/pisa/papers/PP1734.pdf [Accessed 29 October 2008].

Gaston, E.L. 2008. "Mercenarism 2.0? The Rise of the Modern Private Security Industry and Its Implications for International Humanitarian Law Enforcement". *Harvard International Law Journal.* Vol. 49. No. 1. pp. 221 – 239.

Gerspacher, N. 2005. "The Roles of International Police Cooperation Organization". *European Journal of Crime, Criminal Law & Criminal Justice.* Vol. 3. pp. 413 - 434.

Gill, P. 2004. "Securing the Globe: Intelligence and the Post-9/11. Shift from 'Liddism' to 'Drainism'". *Intelligence and National Security.* Vol. 19. No. 3. pp. 467 - 489.

Hanson, S. 2009. *Combating Maritime Piracy.* East Africa Forum. [online]. Available at: http://www.eastafricaforum.net/2009/02/21/combating-maritime-piracy/ [Accessed 24 May 2009].

Hager, N. 1996. *Secret Power: New Zeeland's Role in the Spy Network.* [online]. Available at: http://ftp.fas.org/irp/eprint/sp/sp_c2.htm [Accessed 20 May 2009].

Heide, R.L., Phillips, J. & Perreault, A. D. 2004. *Peacekeeping Intelligence: New Players, Extended Boundaries.* Conference report. Centre for Security and Defence Studies, Charleton University.

Hindle, G. 2007. "Policing Terrorism in the UK." *Policing.* Vol. 1. No. 1. pp. 38 - 42.

Hough, M. 2004. "Warning Intelligence and Early Warning with Specific Reference to the African Context". *Strategic Review for Southern Africa.* Vol. XXVI. No. 2. pp. 23 – 38.

Johnston, R.J. 1998. *Barriers to Transnational Policing.* Jane's Strategic Advisory Services. [online]. Available at: http://www.janes.com/security/law_enforcement/news/ipi/ipi0261.shtml [Accessed 29 October 2008].

Khan, Z. 2006. "The National Security Agency (NSA): Eavesdropping on Americans: A Program that is neither Legal nor Necessary". *Utrecht Law Review.* Vol. 2. Issue 2. pp. 61 – 80.

Lander, S. 2004. "International Intelligence Cooperation: An Inside Perspective". *Cambridge Review of International Affairs.* Volume 17. No. 3. pp. 481 – 493.

Lefebvre, S. 2003. "The Difficulties and Dilemmas of International Intelligence Cooperation". *International Journal of Intelligence and CounterIntelligence.* Volume 16. No. 4. pp. 527 - 542.

Lejeune, P. 1999. "Open Source Intelligence: The Interpol Experience*". Eurointel '99.* The Hague.

Le Roux, L. 2007. "Commentary: 30 May 2007: Piracy in Somali Waters hits Food Aid: The Star 22 May 2007*". ISS Today*. [online]. Available at: http://www.iss.co.za/index.php?link_id=28&slink_id=4523&link_type=12&slink_type=12&tmpl_id=3 [Accessed 22 May 2009].

Makarenko, T. 2002. *Terrorism and Transnational Organised Crime: The Emerging Nexus.* Centre for the Study of Terrorism and Political Violence. University of St. Andrews.

Michaels, J.D. 2008. "All the President's Spies: Private-Public Intelligence Partnerships in the War on Terror". *California Law Review.* Vol. 96. pp. 901 – 967.

McFarlane, J. 2005. "Regional and International Cooperation in Tackling Transnational Crime, Terrorism and the Problems of Disrupted States". *Journal of Financial Crime.* Vol. 12. No. 4. 301 – 309.

Nagan, W.P. & Hammer, C. 2004. "The Changing Character of Sovereignty in International Law and International Relations". *Columbia Journal of International Law.* Vo. 43. No. 1. 141 – 188.

Ngoma, N. 2004. "Coups and Coup Attempts in Africa: Is there a Missing Link?" *African Security Review*. Vol. 13. No. 3. pp. 85 – 94.

Nicoll, A. & Delaney, J. (Eds). 2007. "US Intelligence Reform: Improvement in Counter-terrorism?" *IISS Strategic Comments.* The International Institute for Strategic Studies. Vol 13. Issue 09. pp. 1 - 2.

Permal, S. 2006. *Indonesia's Efforts in Combating Piracy and Armed Robbery in the Straits of Malacca. Maritime Institute of Malyasia* (MIMA). [online]. Available at: http://www.mima.gov.mymima/htmls/papers/pdf/sumathy/sumathy/%20%20Indonesia's%20effort%20in%20combating%20piracy%20and%20armed%20robbery%20in%20the%20Straits%20of%20Malacca.pdf [Accessed 24 May 2009].

Pike, J. 1997. *National Crime Intelligence Service: NCIS.* [online]. Available at: http://www.fas.org/irp/world/uk/ncis/index.html [Accessed 22 July 2009].

Pike, J. 2003(a). *GCHQ Government Communications Headquarters.* [online]. Available at: http://www.fas.org/irp/world/uk/gchq/ [Accessed 13 May 2009].

Pike, J. 2003(b). *Menwith Hill Station*. UK. [online]. Available at: http:// ftp.fas.org/ irp/facility/menwith.htm [Accessed 9 February 2009].

Piret, J-M. 2008. "Boumediene v. Bush and the Extraterritorial Reach of the U.S. Constitution: A step towards cosmopolitanism?" *Utrecht Law Review.* Volume 4. Issue 3. pp. 81 – 103.

Orlova, A.V. & Moore, J.W. 2005. "'Umbrellas' or 'Building Blocks'? Defining International Terrorism and Transnational Organized Crime in International Law". *Houston Journal of International Law.* Vol. 27. No. 2. pp. 267 - 310.

Reagan, B. 2006. "Public Defenders." *Popular Mechanics.* July. pp. 22 – 29. Cape Town.

Reveron, D.S. 2006. "Old Allies, New Friends: Intelligence-sharing in the War on Terror." *Orbis.* Summer. pp. 453 – 468.

Rosenau, W. 2007. *Liaisons Dangereuses? Transatlantic Intelligence Cooperation and the Global War on Terrorism.* Published in Cooperating Against

Terrorism: EU-US Relations Post 9/11. [online]. Available at: http://www.rand.org/pubs/external_publications/EP20070002/- [Accessed 23 September 2009].

SaferAfrica. 2006. *Pax Africa.* Vol. 3. No. 1. February – May. Letlhokwa Graphic Designs. Pretoria.

Sandoval, K. 2007. "The USA PATRIOT Act and Bilateral Information Sharing". *United States Attorneys' Bulletin*. Vol. 55. No. 2. pp. 23 – 26.

Segell, G.M. 2004. "Intelligence Agency Relations between the European Union and the US". *International Journal of Intelligence and CounterIntelligence.* Vol.17 No.1. pp. 81 - 96.

Segell, G.M. 2005. "Intelligence Methodologies Applicable to the Madrid Train Bombings". *International Journal of Intelligence and CounterIntelligence*. Vol. 18. No. 2. pp. 221 - 238.

Segell, G.M. 2007. "Reform and Transformation: The UK's Serious Organised Crime Agency". *International Journal of Intelligence and Counterintelligence*. Vol. 20. No. 2. pp. 217 - 239.

Shanker, T. 1996. *Behind the War Crimes Investigation in Bosnia.* Encarta Yearbook. September.

Sunnucks, M. 2006. "Corruption Seen as Major Hurdle to Imroving US-Mexico Border Cooperation". *Phoenix Business Journal.* 5 May. [online]. Available at: http://www.bizjournals.com/phoenix/stories/2006/05/01/daily62.html?t+printable [Accessed 5 January 2009].

Symeonidou-Kastinadou, E. 2007. "Towards a New Definition of Organised Crime in the European Union". *European Journal of Crime, Criminal Law and Criminal Justice.* Vol. 15. Issue 1. pp. 83 - 103.

Turner, M.A. 2005. "Intelligence Reform and the Politics of Entrenchment". *International Journal of Intelligence and CounterIntelligence.* Vol. 18. No. 3. pp. 383 – 397.

UNAFEI. 2001(a). *Special Investigative Tools to Combat Transnational Organised Crime (TOC*) [online]. pp. 228 - 239. Available at: http://www.unafei.or.jp/english/pdf/PDF_rms/no58/58/58-19.pdf- [Accessed 2 April 2009].

UNAFEI. 2001(b). *Current Situation, Problems and Solutions for Special Investigative Tools in Combating Money Laundering. Special Investigative Tools to Combat Transnational Organised Crime (TOC*). [online]. pp. 466 - 476. Available at: http://www.unafei.or.jp/english/pdf_rms/no58/58-36.pdf- [Accessed 2 April 2009].

Van der Spuy, E. 2009. "Police Cooperation in the Southern African Region: Politics and Practicalities". *Crime, Law and Social Change.* Vol. 51. No. 52. pp. 243 - 259.

Vervaele, J.A.E. 2005. "Terrorism and Information Sharing Between the Intelligence and Law Enforcement Communities in the US and the Netherlands: Emergency Criminal Law?" *Utrecht Law Review.* Volume1. No. 1. pp. 1 – 27.

Vetter, S.M. 1995. *Military Intelligence Support to Law Enforcement Agencies: Rethinking the Way Defense Intelligence Combats Emerging Perils.* [online]. Available at: http://www.globalsecurity.org/intell/library/reports/1995/VSM.htm [Accessed 24 June 2007].

Villadsen, O.R. 2007. *Prospects for a European Common Intelligence Policy.* [online]. Available at: https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/summer00/art07.html [Accessed 25 October 2008].

Warner, M. Undated. *Wanted: A Definition of "intelligence": Understanding Our Craft.* [online]. Available at: https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-st [Accessed 2 April 2008].

Walsh, J.I. 2006. "Intelligence-sharing in the European Union: Institutions are not Enough". *Journal for Conflict Management and Resolution (JCMR)*, Vol. 44. No. 3. pp. 625 - 43.

Watt, DC. 2002. "The War Against Terror and the Need for Institutional Innovation. *The Political Quarterly.* Vol. 73. Issue 3. pp. 288 – 298.

Watts, L.L. 2001. "Intelligence Reform in Europe's Emerging Democracies". *Studies in Intelligence.* Vol. 48. No. 1. pp. 11 – 25.

2.4. MEDIA REPORTS, PRESS RELEASES AND COMMUNIQUES

Abuggao, M. 2009. *Somali Pirates Controlled by Syndicates- INTERPOL.* [online]. Available at: http://www.google.com/hostednews/afp/article/ALeqM5hPsfTb5 MwUq0regWvnBc74PNdj3g [Accessed 14 October 2009].

African National Congress (ANC). 2006. *ANC Daily News Briefing.* [online]. Available at: http://70.84.171.10/~etools/newsbrief/2006/news0210.txt [Accessed 5 September 2009].

Afrol News. 2009. *African Police Chiefs to Strengthen Collaboration with INTERPOL.* 3 September. [online]. Available at: http://www.afrol.com /articles/34074 [Accessed 15 September 2009].

Allvoices. 2009. *Police Chiefs to Address Piracy in East Africa*. [online]. Available at: http://www.allvoices.com/contributed-news/3540201-police-chiefs-to-address-piracy-in-east-africa [Accessed 15 September 2009].

ASEAN. 2008(b). Joint *Communiqué of the 28th ASEAN Chiefs of Police Conference: Brunei Darussalam, 25-29 May.* [online]. Available at: http://www. aseansec.org/21619.htm [Accessed 28 October 2008].

Bali News. 2005. *Region's Top Cops gather in Bali: 3-Day Meeting among ASEAN and Regional Police Officials Discussed New Forms of Cooperation in Fighting Crime.* 23 May.

Begawan, B.S. *Creation of Aseanapol Secretariat Office Discussed.* The Brunei Times. [online]. Available at**:** http://www.bt.com.bn/en/home_news/2009/03/20/ creation_of_aseanapol_secretariat_office_discussed [Accessed 9 July 2009].

Boot, M. 2008. "Pirates, Terrorism and Failed States". *The Wall Street Journal.* 9 December. New York. US.

Dodd, V. & Norton-Taylor, R. 2007. *Britain Failing to Check Migrants on Terror Database, Says Interpol Chief. Guardian.* [online]. Available at: http://www. guardian.co.uk/terrorism/story/0,,2121808,00html [Accessed 16 July 2007].

Grossman, E.M. 2009. *Boost in IAEA Intelligence Capability Looks Unlikely in Near Term.* Global Security Newswire. 22 June. [online]. Available at: http://www.nti. org/gsn/nw_20090622_4368.php [Accessed 22 October 2009].

HSDailyWire.com. 2009. *Growing Questions About US. UAV Attacks Inside Pakistan.* A.W. News Group Inc. [online]. 21 February. Available at: http://hsdaily wire.com/single.php?id=7408 [Accessed 21 February 2009].

INTERPOL. 2009(h). *INTERPOL Media Release: INTERPOL Maritime Piracy Working Group Aims to Enhance International Police Cooperation.* [online]. Available at: http://www.interpol.int/public/ICPO/PressReleases/PR2009/ PR 200981.asp [Accessed 17 October 2009].

INTERPOL. 2009(i). *INTERPOL Media Release: Landmark INTERPOL-United Nations Ministerial Meeting Sets Course for Boosting Police's Vital Role in Peacekeeping.* [online]. Available at: http://www.interpol.int/Public/ICPO/Press Releases/PR2009/PR200992.asp [Accessed 10 October 2009].

Mazzetti, M. & Glaberson, W. 2009. *Obama issues Directive to Shut Guantánamo.* New York Times. 21 January. [online] Available at: http://www. nytimes.com/2009/01/22/us/politics/22gitmo.html?_r=1 [Accessed 28 May 2009].

Othman, A. 2009. Commissioner of Police at Aseanapol Meeting. Brunei News. 21 May. [online]. Available at: http://news.brunei.fm/2009/05/21/commissioner-of -police-at-aseanapol-meeting/ [Accessed 7 September 2009].

Rhodes, F. (2007). *Namibia: Illegal Weapons Destroyed. New Era.* 27 November. Windhoek. Namibia.

SARPCCO. 2009. *Communique of the Council of Ministers for the Southern African Regional Police Chiefs Cooperation Organisation (SARPCCO)* at the 14th Annual General Meeting held at Emperors Palace and Conference Centre, Kempton Park, South Africa. 4 September.

Vanezis, P. 1999. *The Forensics of Investigating War Crimes.* BBC News. 21 January. [online]. Available at: http://www.nes.bbc.co.uk/olmedia/255000/audio_259995_venesis_all.ram [Accessed 23 October 2009].

UN. 2009(d). *Africa, United Nations Should Improve Strategies for Countering Terrorism, Experts Say at Addis Ababa Meeting.* Department of Public Information. Press Release: AFR/1861, dated 15 June.

2.5. INTERNET SOURCES

ASEANAPOL (No date]. [online]. Available at: http://www.pnp.gov.ph/pcr/content/aseanapol/aseanapol.html [Accessed 30 October 2008].

ASEAN. 2008(a). *Overview: Association of South East Asian Nations.* [online]. Available at: http://www.aseansec.org/64.htm [Accessed 25 October 2008].

AU. 2009. *Committee of Intelligence and Security Services of Africa (CISSA).* [online]. Available at: http://cissa-au.org/root/en/aboutus.asp [Accessed 8 August 2009].

Australia. 2008. *Department of Foreign Affairs and Trade. ASEAN Regional Forum (ARF).* [online]. Available at: http://www.dfat.gov.au/arf/ [Accessed 28 October 2008].

CERI-Sciences Po. 2008. *Intelligence, Borders and Surveillance.* [online]. Available at: http://www.libertysecurity.org/IMG/pdf_Challenge_-_Intelligence_Borders_and_Surveillance_-_21.04.2008_-_en.pdf [Accessed 4 April 2009].

EU. 2008(a). *European Police Chiefs (EPCTF) for Better Operational Cooperation Between Police Forces.* [online]. Available at:

http://www.eu2008.si/en/News_and_Documents/Press_Releases/May/0522EPCTF.html [Accessed 5 September 2009].

EU. 2008(b). *Cooperation with the African Centre for Study and Research of Terrorism.* [online]. Available at: http://europa.eu/legislation_summaries/development/african_caribbean_pacific_states/index_en.htm [Accessed 27 July 2009].

Europol. 2009(c). *Europol and Eurojust Concluded New Agreement.* [online]. Available at: http://www.europol.europa.eu/index.asp7.page=news&news=pr09/005htm [Accessed 13 October 2009].

Foreign Policy. 2008. *The Failed States Index, 2008: The Rankings.* [online]. Available at: http://www.foreignpolicy.com/story/cms.php?story_id=4350&page=1 [Accessed 20 December 2008].

Frontex, 2009. *More about Frontex.* [online]. Available at: http://www.frontex.europa.eu/more_about_frontex/ [Accessed 27 September 2009].

Global Security. 2006. *IMINT Overview.* [online]. Available at: http://www.globalsecurity.org/space/systems/imint-overview.htm [Accessed 22 May 2009].

IAEA. 2009(a): *The "Atoms for Peace" Agency.* [online]. Available at: http://www.iaea.org/About/index.html [Accessed 23 October 2009].

IAEA. 2009(b). *Safeguards Statement for 2008 and Background to the Safeguards Statement.* [online]. Available at: http://www.iaea.org/OurWorks/SV/Safeguards?es2008.html [Accessed 23 October 2009].

ICRC. 2003. *Use of Nuclear, Biological or Chemical Weapons: Current International Law and Policy Statements.* [online]. Available at: http://www.icrc.org/Web/Eng/siteengOnsf/htmlall/5KSK7Q [Accessed 18 August 2008].

ISS. 2006 - 2009. *Profile of African Union.* [online]. Available at: http://www.iss.co.za/index.php?link_id=3893&slink_id=3070&link_type=12&slink_type=12&tmpl_id=3 [Accessed 5 September 2009].

INTERPOL. 2007(b). *INTERPOL and Aseanapol Sign Historic Agreement.* [online]. Available at: http://www.interpol.int/public/News/2007/Aseanapol20070607.asp [Accessed 28 October 2008].

INTERPOL. 2007(c). *List of Police Cooperation Agreements Mentioning Interpol.* [online]. Available at: http://www.interpol.int/public/ICPO/LegalMaterials/cooperation/AgrListPolice.asp [Accessed 30 October 2008].

INTERPOL, 2008(b). *The Command and Coordination Centre.* [online]. Available at: http://www.INTERPOL.int/Public/CCC/default.asp [Accessed 3 October 2009].

INTERPOL. 2008(c). *Operational Data Services and Databases for Police.* [online]. Available at: http://www.interpol.int/Public?ICPO/CoreFunctions/Databases.asp [Accessed 3 October 2009].

INTERPOL. 2008(d). *Southern African Regional Police Cooperation Organisation (SARPCCO).* [online]. Available at: http://www.interpol.int/public/Region/Africa/Committees/SARPCCO.asp [Accessed 4 October 2008].

INTERPOL. 2008(e). *INTERPOL Notices.* [online]. Available at: http://www.interpol.int/Public/Notices/default.asp [Accessed 3 October 2009].

INTERPOL. 2008(f). *Fusion Task Force.* [online]. Available at: http://www.interpol.int/Public/FusionTaskForce/default.asp [Accessed 17 October 2009].

INTERPOL. 2008(g). *Public Safety and Terrorism.* [online]. Available at: http://www.interpol.int/Public/Terrorism/default.asp [Accessed 17 October 2009].

INTERPOL. 2008(h). *Criminal Organizations.* [online]. Available at: http://www.interpol.int/Public/OrganisedCrime/default.asp [Accessed 17 October 2009].

INTERPOL. 2008(i). *Interpol Anti-Money-Laundering Unit.* [online]. Available at: http://www.interpol.int/Public/FinancialCrime/MoneyLaundering/Unit.asp [Accessed 17 October 2009].

INTERPOL. 2008(j). Home Website. *Interpol Notices: MIND/FIND.* [online]. Available at: http://www.interpol.int/default.asp [Accessed 28 August 2008].

INTERPOL. 2009(j). *Regional Bureaus*. [online]. Available at: http://www.interpol.int/public/ICPO/SRB/default.asp [Accessed 15 September 2009].

INTERPOL. 2009(k). *OASIS Africa.* [online]. Available at: http://www.interpol.org Accessed 15 September 2009].

INTERPOL. 2009(l). *Regional Bureau Nairobi.* [online]. Available at: http://www.interpol.int/Public/ICPO/SRB/nairobi.asp [Accessed 15 September 2009].

INTERPOL. 2009(m). *Regional Bureau Abidjan.* [online]. Available at: http://www.interpol.int/Public/ICPO/SRB/abidjan.asp [Accessed 15 September 2009].

INTERPOL. 2009(n). *Regional Bureau Yaoundé.* [online]. Available at: http://www.interpol.com/Public/ICPO/SRB/YaoundeFr.asp [Accessed 15 September 2009].

ISS. 2009(a). *Profile: African Centre for the Study and Research on Terrorism (ACSRT).* [online]. Available at: http://www.issafrica.org [Accessed 27 July 2009].

ISS. 2009(b). *ISS Organised Crime Watch.* July. Issue 2. [online]. Available at: http://www.iss.co.za/dynamic/administration/file_manager/file_links/ISS2JUN09.HTML?link_id=3&slink_id=7916&link_type=12&slink_type=12&tmpl_id=3 [Accessed 15 September 2009].

National Security Agency. 2009. *About NSA.* [online]. Available at: http://www.nsa.gov/about/Index.shtml [Accessed 11 May 2009].

NATO. Undated(a). *Counter-Piracy Operations.* [online]. Available at: http://www.nato.int/cps/en/natolive/topics_48815.htm [Accessed 23 September 2009].

NATO. Undated(b). *NATO Operations and Missions.* [online]. Available at: http://www.nato.int/cps/en/natolive/topics_52060.htm [Accessed 23 September 2009].

NATO. 2009. *NATO-EU Strategic Partnership.* [online]. Available at: http://www.nato.int/cps/en/natolive/topics_49217.htm [Accessed 23 September 2009].

Privacy International. 2005. *UK Introduces 'E Borders' Programme, Proposing More Surveillance and Profiling All.* [online]. Available at: http://www.privacyinternational.org/article.shtml?cmd%5B347%5D=x-347260609 [Accessed 16 March 2009].

Smith, M. [No date]. *Private Intelligence Companies: How the Spooks moved in on Big Business.* [online]. Available at: http://www.michaelsmithwriter.com [Accessed 21 February 2009].

Sourcewatch. 2004. *Coup Attempt in Equatorial Guinea.* [online]. Available at: http://www.sourcewatch.org/index.php?title=Coup_Attempt_in_Equatorial_Guinea [Accessed 6 September 2009].

T.C.M. Asser Instituut. 2009. *EUROPOL and EUROJUST: Their Role in EU Police and Judicial Cooperation.* Brochure. [online]. Available at: http://www.europeanpolice.net/sites/europeanpolice.net/files/EUROPOL%20and%20EUROJUST%20Brochure%202009.doc [Accessed 23 December 2009].

UN. 2002. *The International Criminal Court.* [online]. Available at: http://www.un.org/news/facts/iccfact.htm [Accessed 3 February 2010].

UN. 1949 – 2009. *UNOSAT: Satellite Imagery for All.* [online]. Available at: http://www.unspecial.org/UNS621 T32.html [Accessed 20 November 2009].

UN. 2005(c). *United Nations Department of Peacekeeping Operations Situation Centre.* Peace and Security Section. Department of Public Information. [online]. Available at: http://www.un.org/Depts/dpko/sitcen/sitcentre.html [Accessed 26 September 2007].

UN. 2008(h). *UN Action to Counter Terrorism.* [online]. Available at: http://www.un.org/terrorism/instruments.shtml [Accessed 31 May 2008].

UN. 2008(i). *Security Council Committee Established Pursuant to Resolution 1267 (1999) Concerning Al-Qaida and the Taliban and Associated Individuals and Entities.* [online]. Available at: http://www.un.org/sc/committees/1267/index.shtml [Accessed 28 October 2008].

UN. 2008(j). *The Consolidated List Established and Maintained by the 1267 Committee with Respect to Al-Qaida, Usama bin Laden, and the Taliban and*

Other Individuals, Groups, Undertakings and Entities Associated with Them. [online]. Available at: http://www.un.org.sc/committees/1267/pdf/consolidated list.pdf [Accessed 28 October 2008].

UN. 2009(e). *UNOSAT Joins Hands with UNICRI in Applied Research for Security.* [online]. Available at: http://www.cern.ch/unosat/asp/news.asp?id=452 [Accessed 29 November 2009].

UN. 2009(f). *Counter-Terrorism Technical Assistance Programmes*. [online]. Available at: http://www.un.org.org/sc/ctc/directory/doa/INTERPOL.html [Accessed 3 October 2009].

Von Lampe, K. *Definitions of Organised Crime.* [online]. Available at: http://www.organized-crime.de/OCDEF1.htm#standards [Accessed 6 April 2008].

2.6. YEARBOOKS

Ahlström, C. 2007. *SIPRI Yearbook 2007.* Stockholm International Peace Research Institute (SIPRI). Oxford University Press. Solna. Sweden.