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intelligence enterprise' with a new information sharing model where, for instance the generally accepted, but outdated 'need-to-know principle' is substituted by the principle of 'responsibility to provide', reflected in the *United States Intelligence Community: Information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.