# INTELLIGENCE COOPERATION TO COMBAT TERRORISM AND SERIOUS ORGANISED CRIME: THE UNITED KINGDOM MODEL

***P C Jacobs***
**Division Legal Services**
**South African Police Service**

***M Hough***
**Department of Political Sciences**
**University of Pretoria**

***ABSTRACT***

*The 11 September 2001 terrorist attacks in the United States of America (US), the terrorist attacks on the transport system in the United Kingdom (UK) during July 2005, as well as official commissions of inquiry into how intelligence on weapons of mass destruction (WMD) was dealt with in the UK and the US respectively, profoundly affected intelligence cooperation in the UK. International and regional imperatives, as well as the utility of effective intelligence cooperation, demands of all states to review and improve their intelligence structures to combat terrorism, organised crime and the proliferation of weapons of mass destruction. This article explores the UK's response to identified intelligence failures and with reference to intelligence strategies, policies and practices in the UK, proposes principles for intelligence cooperation, and looks at the UK intelligence cooperation model's suitability as a benchmark for other countries, in order to comply with international and regional imperatives for intelligence cooperation. The conclusion is that the well-developed UK model in certain respects provides a benchmark for intelligence cooperation. The positive elements of the UK model include the establishment of a comprehensive business model for intelligence; community-based and intelligence-led policing; a national coordination mechanism representative of all agencies; the functioning of law enforcement on a multi-disciplinary basis, with powers of police, immigration and customs synchronised into the same agency; cooperation between investigators and prosecutors, nationally and internationally, from an early stage of investigation; and the establishment of a trusted information environment for the exchange of intelligence between civilian and crime intelligence. On the negative side, the UK model without a counter-terrorism mandate in respect of the Serious Organised Crime Agency can be criticised for not adequately addressing the linkages between organised crime and terrorism. Furthermore, effective intelligence sharing in the UK is said to remain hampered by the intelligence community's fractured organisational structure and disconnected way of work, the lack of standardised information technology and uniform procedures between different agencies. The non-utilisation of intercepts as evidence is also not conducive to crime combating.*

## INTRODUCTION

The 11 September 2001 terrorist attacks in the United States (US), the terrorist attacks on the London transport system in July 2005, and official inquiries into how intelligence on weapons of mass destruction (WMD) in Iraq was dealt with, hugely influenced the approach to intelligence cooperation in the United Kingdom (UK). Intelligence failures were identified in the US through inquiries into how the

intelligence community in the US dealt with intelligence on WMD in Iraq and the intelligence available before the 11 September 2001 attacks. These failures include the lack of intelligence cooperation between crime intelligence and civilian intelligence and the duplicity of intelligence structures, not properly coordinated, without a single structure with overall command over all intelligence structures (Gill, 2004; United States of America, 2004; United States of America, 2005). This article analyses crime intelligence and civilian intelligence practices and cooperation in the UK to identify elements of intelligence cooperation in the UK intelligence model, which could serve as a benchmark elsewhere. Universal and regional obligations in respect of the combating of terrorism (United Nations Resolution 1373, 2001), organised crime (United Nations Convention against Transnational Organized Crime, 2000), and the proliferation of WMD (United Nations Resolution 1540, 2004), requires from all states to find ways to intensify and accelerate the exchange of information, including operational information, to combat the above phenomena, which are experienced as present day threats to global and national security.

In addition, factors such as the effects of globalisation, the needs of individual countries, shared crime threats, the sheer advantages or utility of effective international and regional intelligence cooperation, the huge volumes of intelligence available and the huge costs of technology, are drivers for intelligence cooperation on all levels. Effective international intelligence cooperation presupposes effective domestic or national intelligence structures. Countries such as the US and the UK, which have experienced first-hand the effects of terrorism, for example, have since 2001 reviewed and hugely restructured their intelligence structures. In the pursuit to be compliant to international imperatives, countries which have not yet done so, need to review and improve their structures for intelligence cooperation. The objective of this paper is to describe and analyse the UK model for intelligence cooperation as a benchmark for an ideal model for intelligence cooperation for other countries.

## POLICY FRAMEWORK FOR INTELLIGENCE COOPERATION

Intelligence cooperation involves the sharing of intelligence products ranging from intelligence based assessments, including assessments from single-source reports, to sharing of pre-emptive intelligence such as plans or intentions, sharing of raw intelligence products; and operational cooperation, which may include surveillance (joint intelligence collection), joint agent handling, sharing of linguists, exchanges of technical know-how and equipment, common training, and sharing of analytical staff (Lefebvre, 2003; Lander, 2004). International intelligence cooperation can take place at various levels, from complete visibility of the source and product that provides the greatest detail, but carries the most risk; to exposing all or part of the raw product, without exposing the source; sharing only a summary of the data; sharing analysis of the data only; and sharing policy conclusions resulting from the intelligence (Clough, 2004). Similar intelligence cooperation may take place on local, national and international level, each with its own challenges and modalities.

## INTELLIGENCE COOPERATION: STRATEGIES AND POLICIES IN THE UNITED KINGDOM

The overarching strategy governing intelligence cooperation in the UK is the National Security Strategy of the UK, analysed below.

***The National Security Strategy of the United Kingdom***

The National Security Strategy (NSS) of the UK identifies terrorism, the proliferation of nuclear weapons and other WMD; and transnational organised crime as being amongst the main threats to the UK (United Kingdom, 2008a). It is stated that in addition to the police, border police, armed forces and civilian intelligence agencies, there must be a greater involvement with business and local authorities and communities to plan for emergencies and to counter extremism (United Kingdom, 2008a). According to the NSS, there is a common thread among international crimes as threats to security, namely the transnational nature thereof, the role of non-state actors and the effect of dysfunctional states (United Kingdom, 008a). The international instruments dealing with the proliferation of WMD (namely the Treaty on the Non-Proliferation of Nuclear Weapons, 1968; the Convention on the Prohibition of the Development and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on Their Destruction, 1972; and the Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and Their Destruction, 1993) were drafted with the primary objective of preventing the proliferation of WMD among states. It placed WMD as an issue on the international political (foreign policy) agenda to be dealt with mainly by civilian and military intelligence agencies.

After the 11 September 2001 events and the revelation in 2003 of the existence of a private network of suppliers of sensitive nuclear technologies, led by the Pakistani scientist Abdul Qadeer Khan, it was realised that the focus should be widened to include non-state actors as recipients as well as suppliers of sensitive goods and technologies (Frantz and Collins, 2007). In respect of law enforcement, it means a renewed focus on the enforcement of laws relating to the control of materials relating to WMD and their delivery systems, in order to "deny access to WMD and the equipment, technology and expertise while promoting commerce and technological development for peaceful purposes" (United Kingdom, 2008a, p. 29). The main aim of the NSS is to ensure integration of government efforts and to this end, it calls for the strengthening of initiatives such as the Joint Terrorism Analysis Centre (JTAC); SOCA; the Office for Security and Counter-terrorism; the new border agency; the new Cabinet Committee on National Security, and an envisaged National Security Forum (United Kingdom, 2008a).

***The National Intelligence Model***

The National Intelligence Model (NIM) was implemented from April 2003 (in England and Wales) until November 2005 (nationally), on a compulsory basis by police forces and provides a common framework for police intelligence to all police forces of the UK. Her Majesty's Inspectorate of Constabulary is responsible for monitoring and ensuring the compliance of police forces with the NIM (United Kingdom, 2005). The NIM complies with minimum standards in respect of all areas of policing and is captured in the Police Reform Act of 2002, and further statutorily complemented by the NIM Code of Practice, issued in 2005 by the Home Secretary under the said Act. It is described as a "business model" for law enforcement and is aimed at crime prevention rather than simply responding to crime incidents (United Kingdom, 2005). The NIM furthermore envisages cooperation on local, national and international levels to address local crimes as well as serious and organised crime through targeted operations by dedicated units. It has been adopted by agencies such as the Serious Organised Crime Agency (SOCA) and the UK Immigration Services

(United Kingdom, 2005). Analytical options in the NIM include crime pattern analysis; demographic/social pattern analysis; network analysis; market profiles; criminal business profiles; risk analysis; target profile analysis; operational intelligence assessment; and results analysis (United Kingdom, 2005). The NIM represents an intelligence-led policing approach, which includes maximum access to all intelligence sources, a proper analytical process and capacity and the following intelligence products: Strategic assessments, that is, current and long-term issues affecting police; tactical assessments, relating to the day-to-day business of policing; target profiles to have a better understanding of an individual (victim or suspect) or a group; and problem profiles, to better understand emerging crime or incident series, priority locations and other identified high risk issues, and to recommend opportunities for tactical resolution in line with control strategy priorities (United Kingdom, 2005).

Interagency sharing of intelligence, through established protocols, is regarded as an important element of the NIM (United Kingdom, 2005). The NIM requires standardisation of processes and equipment, the integration of databases of partner intelligence - and police agencies, and the availability of technical resources and expertise of other agencies, to each other (United Kingdom, 2005). The NIM requires closer links between police services and external partners in the wider intelligence community, even including wardens and rangers (responsible for, *inter alia*, enforcing wildlife conservation in national parks), traffic wardens, parish special constables, and volunteer associations such as neighbourhood and farm watches, as well as the establishment of permanent joint intelligence units comprising of police, customs, immigration and other agencies, in the police force (United Kingdom, 2005). In practice, the joint agency function is performed mainly through the Special Branches, of which each police force has its own (United Kingdom, 2004). Special Branches have established Special Branch Ports Units, coordinated by the National Co-ordinator of Ports Policing, who is appointed by the Home Office to co-ordinate Special Branch activities at ports.

It is for example stated in respect of the Suffolk Special Branch Ports Unit that: "The unit is primarily an intelligence gathering unit…The unit works closely with other agencies, in particular the UKBA (United Kingdom Border Control Agency) (ex Customs and Immigration)" (UK, 2010). The National Co-ordinator of Ports Policing reports to the National Co-ordinator of Special Branch (United Kingdom, 2004). Security Branch staff are posted at Special Branch units at airports, seaports and international rail termini and works very closely with colleagues in the UK Immigration Service, the Home Office, Her Majesty's Customs and Excise, the Department of Transport, the travel industry, the Security Service and other intelligence agencies, thereby providing national coverage (United Kingdom, 2004b).

A particular strategy to combat terrorism has been adopted and is described below.

***United Kingdom's Strategy for Countering International Terrorism***

The UK's Strategy for Countering International Terrorism is based on four principles, of which two, namely 'PURSUE' and 'PROTECT', relate to intelligence cooperation (United Kingdom, 2009a). 'PURSUE' refers to the gathering of intelligence regarding the terrorist threat; disrupting terrorist activities through prosecution and other means; and international cooperation with partners and allies overseas to strengthen the

intelligence effort and disrupt terrorists outside the UK. 'PROTECT' covers issues such as strengthening border control; working with the private sector to protect key utilities and to protect against attacks by means of technological advances and protection of persons going about their daily activities (United Kingdom, 2009a). The Border Management Programme aims, amongst other things, to improve intelligence sharing in support of border operations and includes the issue of e-borders and the use of biometrics in identifying suspect travellers (United Kingdom, 2009a). An overall business model to deal with intelligence in policing was also developed, namely the National Intelligence Model.

The role of civilian and crime intelligence agencies in the UK is discussed below.

## CIVILIAN AND CRIME INTELLIGENCE AGENCIES TO COMBAT TERRORISM AND ORGANISED CRIME IN THE UNITED KINGDOM

As an introduction to the role of civilian and crime intelligence agencies in the UK, a brief background to intelligence structures in the UK is required.

### *Intelligence structures in the United Kingdom*

The role of both civilian and crime intelligence agencies in the UK in respect of the combating of serious organised crime and terrorism is in a gradual process of development and restructuring. The civilian intelligence community in the UK consists of the Security Service (MI5), established in terms of the Security Services Act of 1989; the Secret Intelligence Service (SIS or MI6), established by the Intelligence Services Act, 1994, and the signals arm - the Government Communications Headquarters (GCHQ) (Todd & Bloch, 2003). In addition, the Joint Terrorism Analysis Centre (JTAC) is a loose-standing structure consisting of representatives of 11 agencies and departments and serves as the UK's "centre of excellence and expertise on assessing the threat from international terrorism".

### *The role of the Security Service*

MI5, as a civilian domestic intelligence agency, is responsible for protecting the UK against covertly organised threats against national security, including terrorism, espionage and the proliferation of WMD. In 1992, MI5 took over the overall intelligence coordination relating to the combating of the terrorist threat to the UK from Northern Ireland. The problems experienced at the time and which led to the new role of the MI5 included "rivalry and squabbling within the security apparatus, which included the Army, MI5, MI6, the Anti-Terrorist Squad at Scotland Yard and regional police forces", and a lack of coordination of anti-terrorist policy (Dillon, 1994, p. 178). MI5 imposed strict rules on the other intelligence services about the handling of agents and the security of information provided by those sources, and to guard against using agent provocateurs. The Task Co-ordinating Group was set up to coordinate all operations and use of agents (Dillon, 1994).

There is also a special relationship between MI5 and Police Special Branches. The function of the Police Special Branches is to gather intelligence about security threats by various means and to assess this with a view to improving the functioning of local police and assisting MI5 in countering terrorist threats. MI5 determines the priorities of Special Branches to gather national security-related intelligence and may request Special Branches to run checks for MI5 without giving the Special Branches the

background to the request (United Kingdom, 2009a). MI5, in addition to playing the leading role in respect of setting priorities for the Special Branches, closely supports the Special Branches of the 56 police agencies in the UK in combating terrorism. It gathers clandestine and open source intelligence information about the covert activities of suspected terrorists; assesses the threats emanating from such activities; takes appropriate actions to prevent or deter terrorist acts; and where appropriate, shares information with other agencies and law enforcement. The police forces are responsible to pursue counter-terrorism investigations by collecting evidence for use in legal proceedings, with a view to criminal prosecutions (United States of America, 2003). The practical working arrangement between MI5 and the police is implemented through Executive Liaison Groups (ELGs). The ELGs provide a secure forum to safely share secret, sensitive and raw intelligence exchange with the police. This intelligence forms the basis for decisions on how to best gather evidence to prosecute suspects in court. In this partnership, MI5 takes the lead in collecting, exploiting and assessing intelligence, while the police take the responsibility for the gathering of evidence, obtaining arrests and preventing crime. ELGs meet regularly and are kept abreast of developments in the investigation in order to coordinate responses to developments, for example, when to execute arrests or when to transfer the overall responsibility from MI5 to the police (United Kingdom, 2009a).

***The Serious Organised Crime Agency***

The establishment of the Serious Organised Crime Agency (SOCA), through the Serious Organised Crime Act of 2005, reflects a total new approach in respect of crime intelligence and law enforcement in the UK, in reaction to the multitude of intelligence agencies in the UK. The erstwhile National Criminal Intelligence Service (NCIS), the National Crime Squads and investigators of the Customs and Immigration Services were amalgamated into SOCA, which commenced operations in 2006. The NCIS was one of the first services in Europe to deal with crime intelligence on a national scale. The NCIS gathered intelligence on drug traffickers, money-launderers, organised criminal groups, paedophiles and soccer hooligans. It focused on the highest echelons of crime and assisted police and other agencies in the UK and elsewhere (Pike, 1997). The National Crime Squad (NCS) was launched in 1998 by the amalgamation of six regional crime squads and was an investigative capacity in respect of mainly organised crime. The NCIS housed the UK National Central Bureau of INTERPOL, and its 500 strong staff complement was drawn from the police, Customs and Excise and the Home Office.

The need for secrecy and fear of compromise also stifled any move towards centralised databases, standardisation and interoperability of electronic communications systems, all of which are requirements for effective sharing of information (Segell, 2007). The mindset of what constitutes intelligence and analysis thereof has changed from the over-emphasis of secrecy towards "openness, transparency, civic consultation and participation in the political debate" (Segell, 2007, p. 219). By the end of 2008, SOCA had established mutually beneficial relationships with hundreds of businesses, trade associations and regulatory bodies (United Kingdom, 2009b). A major catalyst for the establishment of SOCA is the ongoing transformation of the European Union (EU) and its organisations, and the openness of borders in the EU, which necessitate closer cooperation between the respective countries of the EU to combat crimes committed across international borders. SOCA has a limited counter-terrorism role in respect of the financing of

terrorism, resulting from the fact that 60 percent of members of 'paramilitary organisations' in Northern Ireland turned to organised crime (Segell, 2007).

SOCA has been established in addition to the existing intelligence agencies as well as the existing police services and military intelligence units in the UK, but at the same time consolidated intelligence activities and law enforcement and is therefore described as the UK's first non-police law enforcement body (Segell, 2007). SOCA is also the UK's National Financial Intelligence Unit, which receives suspicious transaction reports. In addition, it acts as the gateway for UK law enforcement for a wide range of specialised services through the International Criminal Police Organization (ICPO-INTERPOL), the European Police Office (Europol) and Schengen. As such, in 2008/2009, it channelled 155,000 messages, in turn generating 27,000 cases (United Kingdom, 2009b).

To fulfil its national and international roles, SOCA has established Regional Intelligence Cells (RICs) in the UK and at the same time strengthened cooperation with the Europol; the EU Joint Situation Centre; the Intelligence Division of the EU military staff; and the EU Satellite Centre (Segell, 2007). SOCA took over some of the liaison functions of the Foreign Office; has 120 liaison officers based in 40 countries around the world; and is involved in the G8 countries' Lyon Group. The Lyon Group is responsible for the "improvement of cross-border sharing of intelligence information; to prevent and disrupt terrorist activity and prosecute terrorists; for effective use of advanced investigative techniques such as interception and undercover agents; an enhanced legal framework with states criminalising and prosecuting terrorist activities…; tackling passport fraud; faster operational action to tackle attacks on computer networks; and faster cooperation in tackling Internet related crimes such as child pornography" (Segell, 2007, pp. 217, 224).

SOCA investigators closely cooperate with specialist prosecutors, who are answerable to the National Prosecution Service, and are available when required to provide "comprehensive, practical and specialist advice to help shape investigations and develop strong and well-presented cases for prosecution" (Segell, 2007, p. 226). These prosecutors are expected to become involved in cases from an early stage and to work alongside investigators until conclusion of the prosecution "wherever it would make good operational sense" (Segell, 2007, p. 226). SOCA differs from MI5 in that MI5 officers do not have powers of arrest. The intelligence mandate of SOCA, like that of traditional police forces, is limited to investigative powers such as surveillance, interception and the use of covert human intelligence sources, as provided for in the Regulation of Investigatory Powers Act of 2000 (RIPA). SOCA officers have the multiple powers of police, immigration and customs, and is further supported through the use of statutory deals for immunity and reduced sentences by prosecutors; the use by courts of long-term orders to force criminals to provide bank statements; and disclosure notices by courts to force suspects by threat of prosecution to provide documents (provided such documents may not be used for court purposes) (Segell, 2007).

The importance of cooperation with prosecutors is also vital on international level, as early involvement of prosecutors from different countries may assist to develop a case strategy; to share information about the facts of the case; and to share key evidence and 'any other information'. Involvement of prosecutors may solve jurisdictional

issues such as where and how the investigation may most effectively be prosecuted; whether prosecutions should be initiated or discontinued; and how aspects of the case could be pursued more appropriately in each jurisdiction. An example of such cooperation is between the UK and the US, on the strength of a document entitled *Guidance for Handling Criminal Cases with Concurrent Jurisdiction between the United Kingdom and the United States of America*, signed in January 2007 by the Attorney Generals of the two countries (Aqua, 2007).

The personnel of SOCA include detectives, specialist civilian investigators, financial analysts and computer experts. SOCA is subdivided into four directorates, each respectively responsible for gathering, assessing and using intelligence; enforcement, i.e. for an operational response to threats and basically investigating, or building court cases; intervention, in order to disrupt criminal activities through particularly the freezing and seizing of criminal assets; and corporate services, to support, facilitate and develop the capabilities of SOCA (Segell, 2007).

SOCA has no components in Scotland, where policing functions are devolved to the Scottish government. In Scotland, the Scottish Drug Enforcement Agency, the Strathclyde Police Forensic Department, the Scottish Money-Laundering Unit, the Scottish Witness Liaison Unit and the National High-Tech Centre have been moved to one location at Gartosh, in response to the establishment of SOCA in the rest of the UK (Nelson, 2004).

The success or not of SOCA will certainly form the basis of further transformation. The problem has already been identified that despite the growth in numbers of the RICs established with the aim to collect information from the communities in which potential terrorist extremists can receive support and sympathy, there currently exists no nationwide database for the sharing of counter-terrorism intelligence.

It had been proposed that in the longer run, the counter-terrorism role of SOCA could be extended from counter-terrorist financing only to using its 'revolutionary' broad nationwide mandate to "build intelligence networks and investigative and disruptive capabilities with an international reach and presence" (Hindle, 2007, pp. 40, 41). The independence of civilian and crime intelligence agencies is becoming increasingly irrelevant and potentially obstructive in the conduct of counter-terrorism investigations (Hindle, 2007).

## REVIEW OF INTELLIGENCE ACTIVITIES

The manner in which intelligence agencies in the UK dealt with intelligence relating to WMD in Iraq led to a formal inquiry, the results of which are set out below.

### *Report on the Review of Intelligence on Weapons of Mass Destruction*

The Review Committee was tasked in February 2004 to investigate the intelligence coverage on WMD programmes in countries of concern; on the global trade in WMD; to investigate, with hindsight, what was known about Iraqi WMD until March 2003; and to evaluate discrepancies between the intelligence gathered, analysed and used before March 2003 and the findings of survey teams later on, with a view to improve future intelligence gathering, evaluation and use (United Kingdom, 2004). The Review Committee recommended an improved contribution from the International

Atomic Energy Agency (IAEA) and the UN Special Commission (UNSCOM) in addition to the capacity of national intelligence sources.

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

Following the terrorist attacks on the transport network in London on 7 July 2005 (explosions of improvised explosive devices in the underground train system and one on a bus), the *Report into the London Terrorist Attacks on 7 July 2005* was compiled by the Intelligence and Security Committee (ISC), an independent parliamentary civilian intelligence oversight body. The ISC examined the possibility that intelligence which could have prevented the attacks may have been overlooked; the reasons and effect of lowering the threat assessment level before the attacks; and the lessons learnt as a result of the attacks (United Kingdom, 2006). The report refers to the interaction between the respective agencies, taking into account the diverse sources of intelligence on terrorism, such as intercepts by the GCHQ; intelligence from agents controlled by MI6 inside overseas terrorist cells with links to the UK; intelligence from foreign liaison services; and intelligence products of physical surveillance by MI5 or from agents run by the police within terrorist networks in the UK or of extremist activity in the UK (United Kingdom, 2006). The overwhelming volume of intelligence and limitations such as the impossibility of knowing everything, intercepting all communications, or correctly prioritising every issue, is acknowledged in the report (United Kingdom, 2006).

A major recommendation in the report is to increase coverage of terrorist threats overseas and domestically in the UK, by ensuring a regional presence of MI5 (United Kingdom, 2006). A key lesson from the 7 July 2005 attacks is the value of close cooperation between MI5 and the police, without the police being "removed from their local roots" (United Kingdom, 2006).

***Review of the Intelligence on the London Terrorist Attacks on 7 July 2005***

The report entitled *Review of the Intelligence on the London Terrorist Attacks on 7 July 2005* followed the previous report, but with focused attention on the fact that two of the 7 July 2005 bombers featured in a previous investigation, codenamed Operation Crevice. Operation Crevice was a successful investigation that led to one of the longest terrorist trials in the UK, in which five men were convicted for planning to explode a fertiliser bomb in the UK. At the time when MI5 was investigating the Operation Crevice suspects, they were in contact with two then unidentified men - later identified as two of the London (7 July 2005) bombers. The ISC investigated why MI5, with prior knowledge of these persons, were not able to prevent them from committing the attacks (United Kingdom, 2009c). Operation Crevice was extensive, with 45,000 man hours devoted to monitoring and transcription, and 34,000 man hours to surveillance, in addition to other investigative methods, causing a massive overload of work (United Kingdom, 2009c). An attack was also imminent, leading to arrests at a stage when MI5 would have preferred to gather more intelligence.

From intelligence gained from Operation Crevice, the police were successful through Operation Rhyme to arrest further suspects who planned coordinated attacks by parking limousines packed with gas canisters in underground parking areas and exploding them. The plan was to put radiological material in the devices to form crude "dirty bombs" (United Kingdom, 2009c). Numerous follow-up operations were

launched without uncovering new plots (United Kingdom, 2009c). The report shows that the intelligence community did what they could within their constraints and with the intelligence that was available at the time. A solution to prevent the recurrence of suspects 'getting lost' in an investigation or not being prioritised, is the establishment of what is referred to as 'legacy teams', to reflect on previous operations and the suspects in those operations, and to assess what must be followed up. This method has already enhanced the intelligence agencies' ability to ensure the best deployment of their resources during operations (United Kingdom, 2009c).

The improvement of storing and accessing of information to ensure effective exploitation of intelligence; better identification of targets from fragmentary information and analysing their activities; the establishment of connections between people; and focusing of limited resources are recommended in the review (United Kingdom, 2009c). MI5 has implemented the recommendation of establishing regional offices. This, along with the establishment by the police of three additional counter-terrorist units with a combined intelligence- and investigative capacity, have improved intelligence coverage, response capabilities and coordination with police investigations (United Kingdom, 2009c).

## PRACTICE OF INTELLIGENCE METHODOLOGY IN THE UNITED KINGDOM

The intelligence methodology to investigate terrorism and serious organised crime, as applied in the UK, is set out below. The UK has provided for a comprehensive and well regulated framework through the RIPA and various codes of practice, to ensure that law enforcement and civilian intelligence agencies may fully utilise intelligence tools:

- The *Covert Human Intelligence Source (CHIS) Code of Practice* was issued to regulate the use of covert human intelligence sources inside or outside the UK, and in support of both (United Kingdom, 2002a). According to the *CHIS Code of Practice*, authorisation can be granted for the use of a source by civilian and crime intelligence agencies inside or outside the UK, and in support of both domestic and international investigations (United Kingdom, 2002a).

- The *Covert Surveillance Code of Practice* regulates the authorisation of 'directed surveillance' (non-intrusive covert surveillance undertaken for the purpose of a particular investigation or operation), which may result in obtaining private information on an individual and 'intrusive surveillance' (covert surveillance in relation to events on any residential premises or in any private vehicle carried out by means of a surveillance device) (United Kingdom, 2002b).

- The Secretary of State may authorise the interception of communications upon an application setting out the grounds for the application, the manner of interception, the identification of the targeted person, description of communications to be intercepted, the necessity of the interception, and proportionality. Oral, postal, courier-carried or electronic communications, whether by means of radio, satellite, telephone or the Internet may be intercepted in the interests of national security and for preventing or detecting serious crime. The procedures laid down in the *Interception of*

*Communications Code of Practice* are the same for law enforcement and civilian intelligence agencies (United Kingdom, 2007c).

- Terrorists and criminals use information security technologies to protect their electronic data and the privacy of their communications (cryptology). RIPA, supplemented by the *Investigation of Protected Electronic Information Code of Practice*, provide for access to such technology to ensure that the effectiveness of public authorities is not undermined by the abuse of cryptology (United Kingdom, 2007a).

- RIPA and the *Acquisition and Disclosure of Communications Data Code of Practice* provides for access to telecommunications traffic data from postal or telecommunications operators (service providers). Traffic data includes information on the origin or destination of a communication, including incoming calls; the location of equipment, such as the location of a mobile phone; information identifying the sender or recipient; routing information identifying the equipment being used; web browsing information; addresses or markings on postal items; and online tracking of communications such as postal items and parcels (United Kingdom, 2007b).

***The use of intercepted communications as evidence***

In some jurisdictions, such as the US, intercepted communications have been used as evidence in court for decades. In the UK, intercepts in terms of a UK interception warrant may not be used as evidence in a UK court of law, but such material intercepted in a foreign country under the laws of that country may be used as evidence in a UK court of law. The Privy Council, which reviewed the use of intercepts as evidence, pointed out that the use of intercepts as evidence is curtailed by the danger that such use could compromise the capabilities of intelligence agencies and could thus reduce the effectiveness thereof (United Kingdom, 2007c). The Privy Council recommended that the *status quo* not to use intercepts as evidence, should be retained (United Kingdom, 2007c).

## INTERNATIONAL INTELLIGENCE COOPERATION

In order to identify how civilian intelligence may assist law enforcement through intelligence cooperation, a brief overview of international intelligence cooperation involving the UK is provided.

***The United Kingdom's international cooperation on signals intelligence collection***

The UKUSA signals intelligence (SIGINT) collection agreement between the UK, US, Canada, New Zealand and Australia is an example of the most comprehensive SIGINT cooperation globally. In 1996, the veil was lifted on the extent of this cooperation, and in particular on the global system code-named 'Echelon'. Through the Echelon system, the interception stations of all the allies are interconnected and computers are used to search, in accordance with pre-programmed dictionaries of keywords and fax, e-mail and telex addresses, bulk communications to locate, automatically collect and relay the intercepts to the specific user country. Out of millions of communications, the actual intercepts that are needed to be read by intelligence personnel are reduced by this computerised 'funnel' to a manageable few hundred or thousand (Hager, 1996). The Menwith Hill facility in the UK is an element

of the above cooperation and is capable of carrying two million intercepts per hour. It sifts international messages, telegrams and telephone calls of citizens, corporations or governments to select information of political, military or economic value (Pike, 2003).

Positive intelligence (civilian and military intelligence) clearly has a massive capacity for interception of communications globally. Law enforcement may benefit from SIGINT on an operational level - the pre-empting of terrorist attacks; planning for the interdiction of shipments of drugs, firearms or other goods being illegally trafficked; the unravelling of criminal networks; and targeting of persons or criminal entities for other court-directed investigative technology. Such intelligence could also be used for the tracing of suspects or fugitives.

## PROBLEMS IDENTIFIED IN THE UNITED KINGDOM MODEL

Despite the explanations on what happened with the London bombing suspects who 'slipped the net', the events are regarded as an intelligence failure symptomatic of problems within the UK intelligence community, relating to different institutional priorities and responsibilities that encourage "a disjointed and inconsistent approach to the investigation of terrorist suspects" (Field, 2009, p. 999); over-reliance on techniques (technology) at the expense of basic investigative methods; a lack of interfacing information technology systems and procedures between individual agencies; lack of cooperation and integration of intelligence between the police and MI5; and different tasking and co-ordination processes of the respective intelligence agencies and police forces (Field, 2009, pp. 1008, 1009).

## CONCLUSION

The UK response to the challenges to intelligence cooperation to combat terrorism and serious organised crime is exemplary, with specific reference to the development of intelligence and law enforcement structures and policy; providing the necessary powers to law enforcement and intelligence agencies for collection of intelligence; and the use of special investigative techniques through legislation and formal codes of practice. International intelligence cooperation by the UK and cooperation between civilian intelligence and crime intelligence agencies are indeed well-developed.

The establishment of SOCA in the UK is evidence of the importance of integrating some structures rather than proliferating intelligence and law enforcement structures, and also of having an intelligence capacity in law enforcement structures. Establishment of legacy teams is a best practice to prevent a suspect being 'lost'.

In evaluating the suitability of the UK intelligence model as a benchmark, positive aspects are: the established comprehensive community-based and intelligence-led business model for intelligence in NIM; a national coordination mechanism on which all agencies are represented, namely the Joint Terrorism Coordination Centre and the Joint Terrorism Analysis Centre; in respect of the combating of organised crime - a multi-disciplinary basis with powers of police, immigration and customs integrated into the same agency, namely SOCA, with cooperation between law enforcement and the prosecution on national and international level from an early stage of the investigations; and a trusted information environment, namely the RICs established

by SOCA and ELGs established by MI5 for the exchange of information between civilian intelligence and crime intelligence.

On the negative side, despite the recognition in the National Security Strategy of the UK of the linkages between terrorism and organised crime, it is obvious that terrorism and organised crime are dealt with by separate structures. A bold step of real reform and integration would be to incorporate the intelligence capability in respect of terrorism (MI5) with SOCA and to mandate SOCA to also combat terrorism and to capitalise on the intelligence links between terrorism and organised crime. The practice of not using intercepted communications as evidence is also a negative aspect of the UK intelligence model. Furthermore, in so far as the UK intelligence model seems to be ideal in theory, it is clear that key aspects of the NIM needs to be fully implemented in order to address the problems of a lack of interface on technology and procedures, and to fully utilise basic policing methods instead of over-reliance on technology.

## REFERENCES

Aqua, J.A. (2007). National security evidence and terrorism prosecutions: Cooperation between the United States and the United Kingdom. *United States Attorneys' Bulletin*, 55(2): 32–40.

Clough, C. (2004). Quid pro quo: The challenges of international strategic intelligence cooperation. *International Journal of Intelligence and Counter Intelligence*, 17(4): 601-613.

Convention on the Prohibition of the Development and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on Their Destruction (1972). Retrieved on October 25, 2009 from http://www.opbw.org/convention/documents/btwctext.pdf

Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and Their Destruction (1993). Retrieved on October 25, 2009 from http://www.opcw.org/chemical-weapons-convention/download-the-cwc/

Field, A. (2009). Tracking terrorist networks: problems of intelligence sharing within the UK intelligence community. *Review of International Studies*, 35: 997.

Frantz, D. & Collins, C. (2007). *The nuclear Jihadist: The true story of the man who sold the world's most dangerous secrets…and how we could have stopped him*. New York: Hatchette Book Group.

Dillon, M. (1994). *The enemy within: The IRA's war against the British*. London: Doubleday.

Gill, P. (2004). Securing the globe: Intelligence and the post-9/11 shift from 'Liddism' to 'Drainism'. *Intelligence and National Security*, 19(3): 467–489.

Hager, N. (1996). Secret Power: New Zealand's role in the spy network. Retrieved on May 20, 2009 from http://ftp.fas.org/irp/eprint/sp/sp_c2.htm

Hindle, G. (2007). Policing terrorism in the UK. *Policing*, 1(1): 38–42.

Lander, S. (2004). International intelligence cooperation: An inside perspective. *Cambridge Review of International Affairs*, 17(3): 481–493.

Lefebvre, S. (2003). The difficulties and dilemmas of international intelligence co-operation. *International Journal of Intelligence and Counter Intelligence*, 16(4): 527–542.

Nelson, F. Scotland and England go separate ways with own FBI-style agencies. November, 25, 2004. Retrieved on July, 6, 2010 from http://news.scotsman/seriousorganisedcrime agencyplans/Scotland -and-England-go-se...

Pike, J. (1997). National Crime Intelligence Service: NCIS. Retrieved on July 22, 2009 from http://www.fas.org/irp/world/uk/ncis/index.html

Pike, J. (2003). Menwith Hill Station. Retrieved on May 13, 2009 from http://ftp.fas.org/irp/facility/ menwith.htm

Segell, G.M. (2007). Reform and transformation: The UK's Serious Organised Crime Agency. *International Journal of Intelligence and Counterintelligence*, 20(2): 217–239.

Todd, P. & Bloch, J. (2003). *Global Intelligence: The World's Secret Services Today.* London, New York: Zed Books.

Treaty on the Non-Proliferation of Nuclear Weapons (1968). Retrieved on May 31, 2008 from http://www.un.org/ events/npt2005/npttreaty.html.

United Kingdom (2002a). Covert Human Intelligence Source: Code of Practice, Home Office, London: The Stationery Office.

United Kingdom. (2002b). Covert Surveillance Code of Practice. Home Office, Norwich: The Stationery Office.

United Kingdom. (2004a). Report of a Committee of Privy Councillors: Review of intelligence on weapons of mass destruction. Retrieved on July 20, 2007 from http://www.butlerreview.org.uk/

United Kingdom. (2004b). Guidelines on Special Branch Work in the United Kingdom. Home Office, London.

United Kingdom. (2005). Guidance on the National Intelligence Model. Wyboston, Bedford: National Centre for Police Excellence on behalf of the Association of Chief Police Officers.

United Kingdom. (2006). Report into the London terrorist attacks on 7 July 2005. Intelligence and Security Committee, Norwich: The Stationery Office.

United Kingdom. (2007a). Investigation of Protected Electronic Information: Code of Practice. Home Office, London: The Stationery Office.

United Kingdom. (2007b). Acquisition and Disclosure of Communications Data: Code of Practice. Home Office, London: The Stationery Office.

United Kingdom. (2007c). Interception of Communications: Code of Practice. Home Office, London: The Stationery Office.

United Kingdom. (2008). Review of Intercept as Evidence: Report to the Prime Minister. Privy Council, Norwich: The Stationery Office.

United Kingdom (2008a). The National Security Strategy of the United Kingdom: Security in an interdependent world. Cabinet Office, Norwich: The Stationery Office.

United Kingdom. (2008b). Privy Council of Review of intercept as evidence: Report to the Prime Minister. Norwich: The Stationery Office.

United Kingdom. (2009a). The United Kingdom's strategy for countering international terrorism. HM Government, Richmond, Surrey: The Stationery Office.

United Kingdom. (2009b). SOCA Annual Report 2008/2009. Retrieved on July 21, 2009 from http://www.soca.gov.uk

United Kingdom. (2009c). Could 7/7 have been prevented? Review of the intelligence on the London terrorist attacks on 7 July 2005. Intelligence and Security Committee, Richmond, Surrey: The Stationery Office.

United Kingdom. (2010). Special Branch Ports Unit. Retrieved on July 6, 2010 from http://www.suffolk.police.uk/About+Us/Departments+and+Roles/Small+Ports+Unit/

United Nations Convention against Transnational Organized Crime. (2000).

United Nations. (2004). *United Nations Convention against Transnational Organised Crime and the Protocols thereto*. New York: E-book.

United Nations Resolution 1373 (2001). Adopted by the Security Council at its 4385th Meeting on 28th September. Security Council Document No. S/RES 1373. New York: United Nations.

United Nations Resolution 1540 (2004). Adopted by the Security Council at its 4956th Meeting on 28 April. Security Council Document S/RES1540. New York: United Nations.

United States of America. (2003). Report for Congress: Domestic intelligence in the United Kingdom: Applicability of the MI-5 model to the United States. Document RL.31920, 19 May. Washington, DC: Congressional Research Service, Library of Congress.

United States of America. (2004). Report of the National Commission on terrorist attacks upon the United States. Retrieved on June 30, 2007 from http://fli.findlaw.com/news.findlaw.com/hdocs/docs/911report.pdf

United States of America. (2005). The Commission on the intelligence capabilities of the United States of America regarding weapons of mass destruction: Report to the President. Washington, DC: Official Government Edition.