THE ROLE OF INTELLIGENCE IN COUNTERING TERRORISM AND INSURGENCY

Brig Gen G P H Kruys (Ret)
Research Associate: Institute for Strategic Studies
University of Pretoria

ABSTRACT

Operations to counter terrorism and insurgency depend largely on timely accurate intelligence. In order to gain such intelligence it is essential that the various intelligence agencies co-operate effectively irrespective of which objectives of government they serve. This is true of international intelligence co-operation between democratic states as well. Institutions and media aiming to maintain democratic freedoms tend to be critical over intelligence collection methods, but it is of prime importance that it does not lead to the handicapping of intelligence agencies in such a way that it makes them ineffective.

1. INTRODUCTION

Terrorism has been a major component of insurgency campaigns for centuries. Since the end of the Cold War in 1989 it has become so prominent that the two terms, terrorism and insurgency, are often used as if they meant the same thing. Insurgency covers a much wider field of subversive activities than terrorism does. The nature of the post-September 11, 2001 international terrorist campaign, led by al-Qaeda and based on fundamentalist Islamic thinking, has naturally led to the synonymous usage of the terms.

In order to defeat any political terrorist campaign, described as terrorism or insurgency, it is imperative that high quality intelligence be developed.[1] Analysts and practitioners of counter-insurgency have concluded that good intelligence is critical. The United States of Am-

erica (US) National Commission on Terrorism stated that "no other single policy effort is more important for preventing, pre-empting, and responding to attacks than intelligence."[2]

It is clear that the problem of defeating an enemy consists of firstly finding it. In consequence it is easy to recognise that reliable information is of paramount importance.[3] Having confirmed its importance, it is necessary to consider how the intelligence communities of democratic states should perform their functions at strategic and tactical levels to defeat terrorism internally and/or externally.

2. TERRORISM AS A CRIMINAL ACT

There are many definitions of terrorism and there are reasons why 'anti-colonial', 'anti-imperialist' and some communist-inspired 'freedom struggles' had a historical problem in seeing terrorism as a crime during the Cold War. However, it seems to be clearly classified as a crime now.

The Republic of South Africa promulgated the *Protection of Constitutional Democracy Against Terrorist and Related Activities Act, 2004* (Act No 33 of 2004). It was enacted "to provide for measures to prevent and combat terrorist and related activities; to provide for an offence of terrorism and other offences associated or connected with terrorist activities …; to provide for investigative measures in respect of terrorist and related activities; and to provide for matters connected therewith".[4]

To remove any doubt that terrorist activity is a crime in South Africa, the Act states that "terrorist and related activities means any act or activity related to or associated with the commission of the offence of terrorism, or an offence associated with a terrorist activity".[5]

In the Preamble to the Act it is made clear that South Africa regards international terrorism as a crime as well. The South African government is committed to co-operate with the United Nations (UN), the African Union (AU) and the Non-Aligned Movement (NAM) to prevent and combat terrorist and related activities. It has thus become party to a number of instruments of the UN which include *The International Convention for the Suppression of Terrorist Bombings* and *The International Convention on the Suppression of the Financing of Terrorism*. It is also bound by the *Convention for the Pre-*

vention and Combating of Terrorism adopted by the Organisation of African Unity (OAU).[6]

In order to allay any doubt as to the meaning of terrorism in this article, it is defined as "a method to strike with terror those against whom it is adopted".[7] Political terrorism is defined as "the use of murder and destruction in order to terrorise individuals, communities and/or governments into conceding to terrorists' demands".[8]

The immorality of terrorism is clear in the above definitions, but terrorism should also be seen as a crime because when it is defined as terrorist warfare rather than criminal behaviour, the terrorists' status is enhanced. It provides them with the legitimacy they seek. They generally, in the words of a US Federal Bureau of Investigation (FBI) undercover agent, who infiltrated terrorist groups, refer to themselves as soldiers, revolutionaries or holy warriors. Their greatest fear is that they should be labelled as mere criminal gangs.[9]

As is the case with most of the world, European countries face a significant threat from terrorism. The Director General of the Legal Affairs of the Council of Europe stated in April 2005 that the European states did not yet have the ability to contain attacks on the scale of the terrorist attacks launched on Madrid in 2004. In order to co-ordinate European counter-terrorist activities, amongst other things, a Committee of Experts on Special Investigation Techniques in Relation to Acts of Terrorism was instructed to make a study of special investigation techniques. This was to facilitate the prosecution of terrorist offences, and in so doing increase the effectiveness of law enforcement.[10]

The investigating committee came to the conclusion that in combating terrorism, there were two options, namely that of using force or using the law. The European states chose the option of using the law. They took the view that bringing terrorists before a judge was their worst punishment.[11]

The term 'War on Terror' still has an aggressive and hostile ring to it, so as to mobilise anti-terrorist feelings, but the US-led overthrow of the Taliban and al-Qaeda in Afghanistan in 2001 forced the jihadist terrorist network to disperse. This has led to a common insight and conclusion that countering terrorism can best be done by effective law enforcement and intelligence co-operation.[12] This implies intelligence co-operation between key counter-terrorism allies such as the US and Western European countries, and between intel-

ligence agencies such as civilian intelligence, military intelligence and crime intelligence.

3. INTELLIGENCE CO-OPERATION

One of the major reasons for intelligence failure is the difficulty in achieving intelligence co-operation. Co-operation in the form of intelligence sharing between security and crime intelligence is problematic. Interlinking their networks will be achieved with difficulty, assuming that it can ever truly be achieved. The aim of crime intelligence is to arrest and try criminals. The very nature of court proceedings, which includes the cross-examination of witnesses, has the inherent risk of classified information being exposed. Furthermore, the purpose of security intelligence is to forestall anticipated hostile action. In spite of the tendency to conclude that terrorism can best be countered by effective law-enforcement, recourse to the courts remains one among a number of options, and inherently a risky one.[13]

In 2003, long after September 11, 2001, it was reported that information sharing between the FBI, the US Central Intelligence Agency (CIA) and the US National Security Agency (NSA) continued to be highly restricted. The FBI preferred to keep its intelligence to itself and was not inclined to share intelligence with the CIA and other intelligence agencies. As a law enforcement agency the FBI has a domestic security mission, and law enforcement and intelligence are two different functions.[14]

There is the now famous case of FBI special agent Kenneth Williams who in July 2001 sent the *Phoenix Memo* to FBI headquarters which read: "Phoenix believes that the FBI should accumulate a listing of civil aviation universities/colleges around the country". Evidently the recommendation and the intelligence on which it was based was not taken seriously, was not analysed, and was not shared with other intelligence agencies, or even other FBI field offices, except New York's office.[15] A US special investigation commission concluded that the FBI had damaged its intelligence capability by favouring a law enforcement approach to crime, terrorism and counter-intelligence. An agent described as a counter-intelligence veteran, a certain I C Smith, agreed with the finding and stated that it was clear that the FBI had had no interest in being a major player in the intelli-

gence community.[16]

FBI agents in New York were evidently prevented from initiating criminal investigations against two of the September 2001 hijackers, because the managers at FBI headquarters failed to understand their intelligence sharing regulations. It is thus evident that bureaucratic inefficiency was a major cause for the intelligence breakdown. It was not a lack of intelligence and probably not an over-reliance on criminal law enforcement. Restrictions on intelligence sharing caused the failure. Exposure of proactive law enforcement techniques at trials may well have helped to avoid the 9/11 attacks on the World Trade Centre. Protecting the intelligence gleaned did not serve to protect US national security.[17] The extent to which terrorist attacks are frustrated when the terrorist cells have been compromised by their plans becoming known, as a result of the publicity given to trials after the arrests of the terrorists themselves, is debatable.

Studying the pre-September 2001 FBI failures can be insightful, but since the 9/11 terrorist attacks, the intelligence functions of the FBI relating to counter-terrorism and counter-intelligence have grown enormously in importance. The FBI, it is stated in 2006, has reorganised in an effort to ensure that its intelligence function does not suffer from traditional law enforcement occupational methods.[18] Due to the requirements of confidentiality involved in counter-terror operations, FBI successes are not likely to be widely publicised. Should a major intelligence failure occur again it will probably be available for study some time after the event. Due to the difficulty inherent in intelligence work, this is likely to happen somewhere in the future.

The use of information supplied by the public to security forces can also be problematic, possibly because it is too time-consuming to evaluate all of it. In June 2006 Sky News network reported that a certain Martin Gilbertson had warned the police in London, two years prior to the 7 July 2005 London bombings, that he had contact with two persons whose fundamentalist Islamic beliefs led him to believe that they had possible destructive terrorist aims. They were extremely anti-Western and tried to convert Gilbertson, who worked in a bookshop with them, to fundamentalist Islam. They in fact later proved to be two of the suicide bombers who killed and injured innocent members of the public in London.

In June 2006 much publicity was given, also on Sky News amongst other networks, that the police in London had raided a home,

arrested two members of the public and later released them, having found them not to be terrorists at all. Evidently the raid had injured one of the two people arrested and it had been a major inconvenience to the whole neighbourhood. The deputy commissioner of police then publicly apologised for the inconvenience caused by police activity. Clearly the evaluation of information and intelligence used to combat terrorism is not an easy task.

Intelligence sharing between states is best organised by bilateral agreements, and long-standing bilateral relationships remain the primary vehicle for real inter-state intelligence co-operation. Good relations are easily fostered between nations with common political and economic systems, common religious beliefs and common cultures. Nevertheless, national governments are afraid of losing control over their own intelligence. After all, intelligence agencies, even in the same state have difficulty in sharing intelligence. For that very reason, multinational institutions such as the UN, the European Union (EU) and the Association of South East Asian Nations (ASEAN) have not been very successful in the sharing of intelligence among member states.[19]

However, on 8 July 2006, CNN reported that the FBI had made a formal statement, that a terrorist group had been arrested in unspecified countries, with one terrorist being arrested in Lebanon. The aim of the group was to attack the underground railway system in New York. The terrorist group was still in the preparatory phase of their operation, but it confirmed that international intelligence co-operation can be very successful indeed.

A terrorist plot to blow up as many as ten passenger jets, bound from London to the US was foiled in August 2006 with the arrest of 24 suspects. A year prior to the arrests Britain's M15 launched the investigation. Pakistani officials helped track the British suspects, and US intelligence provided intercepts of the group's communications.[20] This was clearly a combined effort.

4. INTELLIGENCE FUNCTIONS AT STRATEGIC LEVEL

Before considering the roles and functions of intelligence at strategic level it is necessary to define strategic intelligence. Strategic intelli-

gence is intelligence concerned with the policies, cultural tendencies, thinking processes, intentions, capabilities, limitations, vulnerabilities and possible courses of action of foreign or enemy nations or international terrorist organisations. It is used in carrying out national security measures, in determining foreign and anti-terror policies or in conducting general security and/or military operations.[21]

In October 2005 the US Office of the Director of National Intelligence (ODNI) released the *US National Intelligence Strategy*. The document states that the strategy will guide the intelligence community's policy, planning, collection, analysis, operational programming, acquisition, budgeting and execution. It further states that the activities will be overseen by the ODNI and that it will be implemented by an integrated intelligence community.[22]

Under the heading "Mission Objectives" the strategic roles of intelligence are further explained as those mission objectives relating to intelligence efforts to predict, penetrate, and pre-empt threats to US national security, and which assist all who make and implement US national security policy, fight the US's wars, and protect and enforce its laws. The mission objectives are listed as defeating terrorists at home and abroad, preventing and countering the spread of weapons of mass destruction (WMD), developing ways to penetrate and analyse difficult targets, anticipating developments of strategic concern and the identification of opportunities and vulnerabilities for decision-makers. Also added is the bolstering of democracy and the sustenance of democratic states.[23]

The mission objectives are a mixture of purely intelligence objectives and objectives of US national strategy. Also listed are objectives under the heading "Enterprise Objectives". They are truly intelligence community objectives set by the ODNI. Summarised they read as follows:[24]

— The building of an 'integrated' intelligence capability which can combat the threats to the US itself, consistent with US laws, and the protection of privacy and civil liberties.

— To improve analytic expertise, methods and practices.

— The 'integration' and optimisation of collection capabilities.

— To attract, employ and 'unify' a results-focused, innovative intelligence community workforce.

— To strengthen foreign intelligence relationships and to establish new ones.

— In order to improve the intelligence agencies' ability to 'work together', clear, uniform security practices and rules are to be created.

— To exploit path-breaking research and scientific advances.

— To eliminate programmes which add little value to the intelligence effort and to direct the savings so accrued to new priorities.

From the above strategic explanations, as well as the mission and enterprise objectives it is clear what strategic intelligence means to the US ODNI, The appointment of a Director of National Intelligence in the US was done to rectify previously experienced weaknesses. It should be noted that of the eight enterprise objectives listed above, four have the element of integration of the intelligence community as a goal.

Many studies on intelligence stress the fact that tactical intelligence takes up too much effort on the part of intelligence agencies, at the expense of strategic intelligence. The point is made that specific centres in the agencies should be tasked to produce strategic intelligence and that analysts in those centres should specialise in it.

It would seem that the US government as a whole did not foresee the collapse of the Iraqi state after the US military's seizure of Baghdad in April 2003, and that Iraq was a type of failed state in an advanced state of decay.[25] It underlines the assumption that strategic intelligence was lacking. In retrospect it is remarkable that the intelligence communities of the Western nations did not predict the insurgency which has taken place in Iraq. The involvement of neighbouring countries, Syria and Iran, as well as the enmity between Sunnis and Shiites, not to mention the involvement of al-Qaeda in the insurgency, should have been anticipated by experienced strategic analysts.

The type of information needed to make the correct forecasts was not secret. It could have been gleaned from open sources which include speeches by officials, Middle Eastern media and the mood of the peoples living in Iraq and its neighbouring states. Analysts who are good observers and who are able to conceptualise what mass

tendencies will bring about, must be given time, facilities and the mission to produce strategic intelligence.

It was estimated by the US government, as result of an appreciation done by a workgroup of the then National Security Advisor, Condoleezza Rice, that the cost of reconstructing Iraq after the war would be about US$50-60 million. However, the US was to spend US$87 billion for military operations and the rebuilding of Iraq and Afghanistan. This evidently included US$20 billion in grants to rebuild Iraq alone. The failure to estimate the costs correctly was caused by two false assumptions namely, firstly, that Iraq's infrastructure was in a reasonable state, and secondly, that the oil exports would pay for reconstruction. Neither have proved feasible. The economic intelligence failures, combined with the WMD intelligence failure, were difficult to explain and were 'catastrophic'.[26]

However, in April 2006, a former CIA senior analyst for the Middle East, Paul R Pillar, who had been the Deputy Chief of the CIA's Counterterrorist Centre, wrote that the Bush Administration disregarded the intelligence community's predictions of a likely sequence of events, if Iraq were to be invaded. He reported that intelligence analysts presented a picture of a country that would have a long, difficult and turbulent transition to democracy. This prediction was made prior to the war when the Administration aimed, by invading Iraq, to destabilise the power structures of the Middle East and in so doing, spread more liberal politics and economics throughout the region.[27]

Evidently intelligence estimates foretold that despite Iraq's oil resources, a massive Marshall Plan-type effort would be needed to restore the country's economy. The violent conflict between Sunnis and Shiites which has developed, was forecast, and it was anticipated that the foreign occupying forces would be the target of resentment and attacks, unless security was established within the first weeks or months after Saddam Hussein was ousted. The intelligence assessment argued that Iraq's value as a democratic example would be minimal, and that foreign occupation would promote fundamentalist political Islam, increase support for terrorist aims and Iraq would then attract extremists from all over the Middle East.[28]

The contradictions in the above reports are obvious. Which is true? Did intelligence misread the future, predict wrongly or not predict at all, or did it predict correctly? The debate will probably con-

tinue for a long time to come.

The senior analyst stated that the official intelligence analysis was not relied on even when the most important national security decisions were made. Furthermore, it was contended that intelligence was misused publicly to support decisions already made, and that ill-will developed between policy-makers and the intelligence officers.[29]

The question that should also be asked is whether the intelligence community did or did not forecast 'all' the possibilities, as it often does? In so doing intelligence is never wrong. There is also a constant debate in intelligence research that operational mistakes are either the fault of the policy-makers, or that of the intelligence operatives. The truth is probably that the fault lies with both camps.

5.   THE ROLE OF INTELLIGENCE AT TACTICAL LEVEL

Tactical or actionable intelligence can be defined as an awareness of the target, timing and type of attack being planned by an enemy.[30] It can also be described as intelligence pertaining to the capabilities, limitations, vulnerabilities or reactions of a hostile force (or terrorist organisation), either air or surface, which is used in carrying out tactical operations.[31]

In the foreword to the European study of special investigation techniques, in order to co-ordinate European counter-terrorist activities (previously referred to), the Director General of the Legal Affairs of the Council of Europe stated that judicial and police authorities have had to adapt their investigative measures. This was necessary in order to contend with the terrorist networks which are often involved with other types of crime such as drug and arms trafficking. The authorities have had to develop special investigation techniques such as undercover operations and electronic surveillance. These he described as techniques used to systematically gather information in such a way that they do not alert the persons being investigated.[32]

The European Committee of Experts on Special Investigation Techniques in Relation to Acts of Terrorism, decided that it should define and draw up a list of the techniques and set standards concerning their use.[33] As part of the investigation, member countries of

the EU were asked to report what special investigation techniques were employed in their respective countries. The techniques are clearly activities at tactical level and include, amongst others, the following:[34]

— Undercover operations which included covert investigations.

— Front store operations, for example, undercover companies.

— The use of informants.

— Observation activities to include cross border observation.

— Electronic surveillance.

— Interception of communications which include telephone, fax, e-mail and monitoring of public and private networks.

— Searches of cars, premises and computers.

— Cross-border (hot) pursuit.

— Agents provocateurs.

As regards standards set for the use of special investigation techniques, the following examples should suffice:[35]

— The laws governing telephone tapping must state the categories of people whose telephones are to be tapped, the types of offences being investigated, and the duration of the tapping operations.

— Normally searches require judicial warrants.

— Recording of personal data needs a strict legal framework which covers the nature of the data, to whom it may be made available, and the supervision by state authorities.

— Infiltrating police officers who passively observe criminal activities do not infringe on the offender's rights.

— The police are not required to reveal the identity of informants. This may of course prove problematical in court.

— Criminal cases based substantially on the testimony of agents provocateurs, may well violate the rights of accused to a fair hearing.

— Police officers may testify anonymously either to ensure that they may be used again, or to ensure their and their family's safety.

Denis Pluchinsky, a US State Department intelligence analyst with more than 25 years experience, has described al-Qaeda as an extremely secretive, dedicated, patient group who are small in numbers and perfectly willing to die for their cause. In his opinion al-Qaeda members will be very difficult to track down and eliminate. He further specifies what he considers to be the five elements of a terrorist operation, namely target selection, surveillance, operational planning, the attack itself, and escape and evasion.[36]

Pluchinsky's experience led him to comment that he had studied about 9 000 anti-US terrorist threats and he could only recall about two dozen reports which provided the key elements of a credible terrorist plot. He saw only two ways to find out if a terrorist group was planning an attack. Firstly, intelligence was needed from a human agent who had access to the plot information or who intercepted conversations detailing the plot. The very nature of al-Qaeda, he felt, would make human intelligence of this calibre unlikely. Secondly, specific attack information could be obtained by analysis of pieces of information. However, he believed it impossible to deduce targets and times through analysis alone.[37]

From the above it can be concluded that detecting terrorist plots and the role of intelligence in combating terrorism is extremely difficult. It was reported that on 15 June 2006, Abu Mousab al-Zarqawi, the Jordanian leader of al-Qaeda in Iraq, was finally eliminated. He, his so-called spiritual adviser and one of his trusted couriers, together with about four other people were killed at 18:12 hours when the first of two guided 227 kilogramme bombs fell on the farmhouse in which they hid. The house lay 50 kilometres north of Baghdad in the countryside, just outside Baqubah.[38]

A US government source said that it had taken years of work to find and eliminate Zarqawi. The fact that the strike was done using F-16 fighter aircraft, one of which dropped two precision bombs, shows that the surveillance team were taking no chances of losing their target. By 18:12 hours darkness was approaching and they also lacked enough forces to storm the house.[39]

Early in 2006, former Baath Party members, some of whom

objected to Zarqawi's vicious attacks on Shiites, began to report on his whereabouts. Evidently a month after the November 2005 suicide attacks on three hotels in Amman, which resulted in the death of 60 people, the Jordanian head of state, King Abdullah II, ordered his intelligence officials to establish a special security branch. The task of the branch, designated the Knights of God, was to launch an offensive against terrorists outside Jordan and to eliminate Zarqawi. A Jordanian official reported that the Jordanians sought sources inside al-Qaeda. One informant, who was neither a Jordanian nor an Iraqi, managed to make contact with three of Zarqawi's couriers. The informant reported spotting one of the couriers in an area outside Baqubah. The Jordanian official is further quoted to have said "Mr X", a courier, "went to Baqubah, so we knew Zarqawi went there".[40]

Concurrently with the Jordanian activities, US intelligence officers were able to find important leads as to Zarqawi's whereabouts. An al-Qaeda operative captured in May revealed the location of Sheik Abdul-Rahman, Zarqawi's spiritual advisor, after which Abdul-Rahman was shadowed. When he was observed in the same place as the Jordanian's Mr X, the US reconnaissance and surveillance team from a so-called Delta Force, moved into a grove of date and palm trees around the house from where they called in the air strike.[41]

US Army Major General William Caldwell told the media that there had been no doubt that Zarqawi was in the house. The Jordanian official confirmed that the courier, the so-called Mr X, Abdul-Rahman and Zarqawi's young wife were also killed in the bombing.[42]

Although no two anti-terrorist operations will be the same, it is clear from the sequence of events in the Zarqawi operation that human intelligence was a major factor. It was possible because Jordanians who are part of the local Middle East population, speaking Arabic, were able to locate a courier. Former Baath Party members gave information, as did a captured al-Qaeda member. All of the information, the result of collaboration between US and Jordanian intelligence, was obviously collated to bring about a highly successful operation.

6. INFRINGEMENT OF HUMAN RIGHTS

In its 'War on Terror', the US government is constantly being criticised for violating fundamental rights and freedoms of its own citi-

zens, and also of alleged terrorists. Since it is an open society, where opposition criticism is given massive publicity, much of it extreme and news headline material, the fault-finding is given prominent news coverage throughout the world. The fact that the US is the world's sole superpower also enhances the news value of the criticism. It is important to note that most of the critique centres on the gathering of information and intelligence.

One of the headline grabbing criticisms is that telephone traffic in the US itself is monitored. Evidently a *Washington Post-ABC News* poll found that 63 per cent of US citizens asked, said they deemed the NSA project to create a database of US phone calls acceptable in the fight against terrorism. As many as 44 per cent said they strongly approved of it, and 51 per cent favoured how the US President was dealing with privacy.[43]

The sensation which this monitoring caused, led to the President himself stating that the intelligence activities he had authorised were lawful. He further added that the Government had been successful in preventing another attack on American soil. The type of comment which caused President Bush to react, was a statement made by a member of Congress that the monitoring of telephone traffic was "a wholesale destruction of the privacy of the American people".[44]

However, a CIA official wrote in 2000 that the intelligence challenges facing the CIA in the period up to the year 2015 included the use of state of the art communication technology by terrorists. He stated that they would use laptop computers, establish their own websites, use sophisticated encryption, reconnaissance, and weaponry which had not been available to their predecessors. This proved to be true as early as 11 September 2001, when the terrorists who planned the attacks in New York, operating in different cities, evidently stayed in contact through computer e-mail.[45]

In order to gather communication intelligence (COMINT), the NSA runs a worldwide surveillance network with its intelligence partners in the United Kingdom (UK), Australia, Canada and New Zealand. The network links supercomputers in various sites around the world, which receive, analyse and sort information beamed down to the computers from satellites, and which capture the information through microwave spillage.

A former NSA director explained that in a typical half hour a

million messages would be intercepted and passed on to the computers. A process known as optical character recognition (OCR), with its OCR dictionary, typically filters out all but 6 500 messages with about 1 000 of these surviving a second filtering process. These 1 000 messages are then sent to the appropriate intelligence agencies every half hour. In order to process all the information a very high standard of information management is required. This according to the former director is "the single most important problem for the US intelligence community".[46]

A White House official reported that the idea of monitoring communications traffic was to collect data, which he described as "a bunch of numbers". The data was then sifted using a process called link analysis, in which a search was done to establish patterns. For example, there could be a large number of calls from pay phones in Detroit to cell phones in Pakistan. Such patterns were cross-checked with other intelligence databases to find some that warranted in-depth investigation. An independent intelligence analyst who monitors the NSA and other intelligence organisations, a certain William Arkin, was of the opinion that link analysis and social analysis led to better understanding of the nature of terrorist networks. He mentioned that the CIA's database of suspected terrorists had trebled in four years to about 190 000 persons.[47]

On 24 June 2006 the Cable News Network (CNN) had a news item that the CIA was monitoring international bank transactions. Although this received prominent coverage, it is obvious that the banking transactions of terrorist groups under various guises must be determined. The transactions are then to be studied to draw further intelligence and to foil the aims of the transactions themselves. The Dutch-Belgian news network, Beste van Nederland en Vlaandere (BVN), reported that the Netherlands Bank had no comment to make. The news item has since received far less attention, but is expected to surface again from time-to-time.

A third item receiving publicity has been the Council of Europe charge that 14 European countries have, to varying degrees, co-operated with the CIA's system of moving suspected terrorists to countries where they were tortured to gain information. This has been termed 'rendition' which means the "surrender of place or person",[48] or "a surrender of fugitives from justice".[49] Based on the phrase "renditions unto Caesar", the US is by inference seen as Caesar.[50]

A Swiss parliamentarian headed the Council's investigation into the rendition charge. He said that the European states involved, provided the CIA with stopover facilities for terrorist suspects *en route* to torture locations, such as Cuba (Guatánamo Bay) or Afghanistan. They may also have co-operated with US intelligence so as to ease the interrogation process. The Swiss leader of the investigation admitted that there was a lack of proof to support the allegations, and numerous European governments have denounced the charges.[51]

However, on 14 February 2007, the EU Parliament approved a report reprimanding the UK, Germany, Italy and 11 other European countries for their alleged complicity in the CIA's so-called 'extraordinary rendition programme'. The European Parliament is motivating its member states to investigate CIA activities in Europe, and to start criminal investigations where violations of their laws occur. Both Italy and Germany have done so early in 2007, where an Italian court indicted 26 Americans, mostly CIA officers, for kidnapping, and German prosecutors issued arrest warrants for 13 CIA officers alleged to have abducted a German citizen.[52]

The terrorist bombings in Madrid (2004) and London (2005) have put a lot of pressure on European governments to ensure that massive terrorist attacks do not occur in Europe again. Obviously this leads to US-EU intelligence co-ordination. If the choice means letting a suspected terrorist run free, or handing him over to US intelligence to gain information so as to prevent another bombing, the latter option is sure to be chosen.[53]

7.   POST-COLD WAR TERRORISM AND CRIMINALITY

The insurgency and terrorism being waged by al-Qaeda in Iraq and Afghanistan, and which has surfaced in the US and Europe, is completely indiscriminate. One bombing can kill and wound as many as 100 and more people at once. Large numbers of victims are innocent women and children.

Al-Qaeda's methods in Iraq have been described as 'netwar' where cells or individuals gravitate towards each other to carry out terrorist armed attacks. They may exchange intelligence, trade

weapons, engage in joint training and carry out an attack with no intention to operate together again. The term 'netwar' is drawn from their method of co-ordination and communication in an 'internetted' manner, with no central command in place.[54]

Whereas Europe and Indonesia have treated terrorists as criminals, South Africa is an example where criminals, many of them foreigners, employ terrorist methods. Their methods may well be based on netwar principles as described above. They have evidently had formal weapon and military or police-type training. As many as 135 armed robberies at shopping centres using large calibre weapons were carried out by criminal gangs in the first six months of 2006. These gangs have the ability to plan attacks after detailed observation of their targets, evaluation of the target's security systems, and appreciation of the best routes to and from the targets. Often they in fact 'outgun' the police.[55]

The Commissioner of the South African Police Service for the Gauteng Province (the Johannesburg/Pretoria area) announced that the province's police management would undertake an investigation into the capacity of the police to carry out its intelligence function. Rightly so, since four police officers had been killed in what was described as an ambush, on 25 June 2006 in Jeppestown, Johannesburg. He further added that closer liaison with the local population may have led to the police having been aware of the criminal gang's whereabouts.[56]

The main difference between criminals and terrorists lie in intent and motivation to carry out their attacks. This influences their methods and it affects the probability of gaining human intelligence in order to combat them. The population is likely to be more forthcoming with information in the case of criminality than it might be in an insurgency, where large numbers of the people may support the insurgents. However, in South Africa criminals are often extremely violent in their rampages, clearly aiming to intimidate. To what extent they are supported by parts of the population is not clear.

8. CONCLUSION

It is concluded that the role of intelligence in countering terrorism and insurgency is absolutely critical. The debate whether to combat terrorism as a 'War on Terror', or whether terrorists should be seen simply

as criminals and fought as such, is important. It is probably best to see it as a 'no holds barred' war against criminals. Accordingly, intelligence can employ a host of special investigation techniques to find the terrorists, and operations can use many methods to capture or destroy them.

The causes of intelligence failure against terrorism are not the same as those against conventional warfare enemies. The problem is often not faulty analysis, because there are normally few tactical intelligence indicators available to analyse anyway. The fault lies primarily in the defective collection of information. Technical sources of intelligence are less useful in counter-insurgency than they are in conventional operations. Probably the only significant type of intelligence in countering terrorism is gained from human sources.[57] The right tactic to defeat post-Cold War terrorism is not conventional warfare but tedious intelligence work done by monitoring telephone calls, tracking financial transactions, shadowing suspects and infiltrating terrorist cells.[58]

A clear conclusion from the many investigations into intelligence failures is that intelligence agencies of all disciplines must co-operate and share intelligence. It remains difficult to formalise systems to ensure the needed co-operation but it is essential. In the 'War on Terror' co-operation between the intelligence agencies of different countries has also proved essential.

The argument of too much emphasis on tactical intelligence at the expense of strategic intelligence is indefensible. Clearly both are needed. Terrorists will not be captured unless it is known when, where and how they intend to carry out attacks, and where they in fact hide out. At the same time strategic intelligence, considering the state of population support, and economic and infrastructure conditions leading to the support or lack of it, is essential as well. Strategic intelligence considers and evaluates the 'sea in which the insurgent swims'. If the surrounding conditions are changed, support may dwindle and an insurgency fail. A good understanding of conditions also gives indications of the likely financial costs involved in combating an insurgency, and which security control measures are likely to succeed.

Open democratic societies allow political parties and the media representing various interest groups, to criticise how their governments and security forces combat terrorism. The intelligence

agencies are roundly criticised for tapping communications, monitoring bank accounts, and the US and EU governments have been attacked for what has been described as 'rendition', namely cooperation with the US, to allow terrorists to be held over in countries other than the US, either for illegal interrogation or for onward transmission. Since the terrorists have no qualms about the methods they use, such criticism should remain within the bounds of reason. The aim is to defeat terrorism not to enhance it. In June 2006 the King of Jordan said in an interview on CNN, that Muslims had to decide whose side they were on. As a prominent Muslim leader, he is fervently against terrorism. An old South African Army adage, born largely out of counter-insurgency operations in Ovamboland (Namibia), namely "scheme against the terrorists, not against your friends" is very applicable at present.

REFERENCES

1. Wilkinson, P, *Terrorism and the Liberal State*, Macmillan Press, London, 1977.
2. United States of America, National Commission on Terrorism, *Countering the Changing Threat of International Terrorism*, Report of the Congressionally mandated commission chaired by L Paul Bremer III, 7 June 2000, p 7, cited in Dahl, E J, "Warning of Terror: Explaining the Failure of Intelligence Against Terrorism", *The Journal of Strategic Studies*, Vol 28, No 1, February 2005, p 35.
3. Kitson, F, *Low Intensity Operations: Subversion, Insurgency, Peace-keeping*, Faber and Faber, London, 1971, p 95, cited in Hoffman, B, Insurgency and Counterinsurgency in Iraq, *Studies in Conflict and Terrorism*, Routledge Taylor and Francis Group, Philadelphia, 2006, p 110.
4. Republic of South Africa, *Protection of Constitutional Democracy Against Terrorist and Related Activities, 2004* (Act No 33 of 2004), p 1.
5. *Ibid*, p 10.
6. *Ibid*, pp 1-2.
7. *The Shorter Oxford English Dictionary*, Oxford University Press, London, 1973, alphabetical.
8. Wilkinson, P, *op cit*, p 49.
9. Owens, D D, Boyne, S, German, M and P R Pillar, *Law vs War: Competing Approaches to Fighting Terrorism*, Strategic Studies Institute, US Army War College, July 2005, pp 2 and 11.
10. De Koster, P, *Terrorism: Special Investigation Techniques*, Council of Europe Publishing, April 2005, pp 5 and 11.

11. *Ibid*, p 41.
12. "CIA – Looking for International Intelligence Partners", *World Security Network Newsletter*, newsletter@worldsecuritynetwork.net, June 2006, p 2.
13. De Koster, P, *op cit*, p 39.
14. Gertz, B, *Breakdown: The Failure of American Intelligence to Defeat Global Terror*, Plume, Penguin Group, New York, June 2003, pp xxiii and 34.
15. *Ibid*, p 85.
16. *Ibid*, p 101.
17. Owens, D D, Boyne, S, German, M and P R Pillar, *op cit*, pp 14 and 15.
18. Best, R A (Jr), Foreign Affairs, Defense, and Trade Division, *Intelligence Issues for Congress*, Congressional Research Service, The Library of Congress, May 2006, p CRS-3.
19. "CIA – Looking for International Intelligence Partners", *World Security Network Newsletter, op cit*, p 3.
20. Ripley, A, "How Much are we Willing to Take", *Time*, Vol 168, No 9, 21 August 2006, p 21.
21. *Military Dictionary*, South African Defence Force, Personnel Division, Director Language Services, Pretoria, 1993, alphabetical (updated by author).
22. United States of America, *US National Intelligence Strategy*, Office of the Director of National Intelligence, October 2005, p 1.
23. *Ibid*.
24. *Ibid*, p 2.
25. International Institute for Strategic Studies (IISS), *Strategic Survey 2004/5*, Routledge, London, 2005, p 181.
26. Elliot, M, "So, What Went Wrong?", *Time*, Vol 162, No 13, 6 October 2003, p 26.
27. Pillar, P R, "Intelligence, Policy, and the War in Iraq, *Foreign Affairs*, March/April 2006, pp 1-2. (http://www.foreignaffairs.org/2006/2.html, accessed 20 July 2006).
28. *Ibid*.
29. *Ibid*, p 1.
30. *Military Dictionary*, SA Defence, *op cit*, alphabetical.
31. Derksen, K M, "Commentary: The Logistics of actionable Intelligence Leading to 9/11", *Studies in Conflict and Terrorism*, Routledge, Taylor and Francis Group, Winnipeg, 2005, p 253.
32. De Koster, P, *op cit*, p 5.
33. *Ibid*, p 11.
34. *Ibid*, p 13.
35. *Ibid*, pp 28-31.
36. Gertz, B, *op cit*, pp 149-150.

37. *Ibid*, pp 150-151.
38. Powell, B and S MacLeod, "How They Killed Him, War on Terror", *Time*, Vol 167, No 25, 19 June 2006, pp 29-31.
39. *Ibid*, p 29.
40. *Ibid*, p 31.
41. *Ibid*.
42. *Ibid*.
43. Tumulty, K, "Inside Bush's Secret Spy Net: America's phone records have been enlisted in the war on terrorism", *Time*, Vol 167, No 21, 22 May 2006, p 25.
44. *Ibid*, pp 25-26.
45. Gannon, JC, "The CIA in the New World Order: Intelligence Challenges Through 2015", cited in Fridell, R, *Spying: The Modern World of Espionage*, Twenty-First Century Books, Brookfield, 2000, p 126.
46. *Ibid*, pp 49-50.
47. Timulty, K, *op cit*, pp 27-28.
48. *The Concise Oxford Dictionary*, Oxford University Press, London, 1954, alphabetical.
49. *Highroads Dictionary*, Thomas Nelson and Sons Ltd, London, 1958, alphabetical.
50. Ledbetter, J, "Renditions unto Ceasar", *Time*, *op cit*, 19 June 2006, p 37.
51. *Ibid*.
52. *Time*, 5 March 2007, Vol 169, No 10, p 9.
53. Ledbetter, J, *op cit*, p 37.
54. Hoffman, B, *op cit*, p 115.
55. *Rapport* (Johannesburg), 2 July 2006.
56. *Ibid*.
57. Dahl, E J, *op cit*, February 2005, p 36.
58. Ferguson, N, "The Nation that Fell to Earth", *Time*, Vol 168, No 12, 11 September 2006, p 21.