To spy or not to spy?

Intelligence and democracy in South Africa

Edited by Lauren Hutton

Monograph 157
February 2009

Contents

Contributors

Ronnie Kasrils was appointed to President Thabo Mbeki's cabinet as Minister for Intelligence Services after the third democratic elections in South Africa on 27 April 2004. Prior to his appointment, Kasrils served as the Minister of Water Affairs and Forestry (1999- 2004) and Deputy Minister of Defence (1994 -1999). The Sharpeville massacre prompted Kasrils to join the African National Congress (ANC) in 1960, serving as the secretary of the ANC-aligned Congress of Democrats in Natal until it was banned in 1962. A member of Umkhonto weSizwe (MK), the ANC's military wing, since its inception in 1961, he was involved in its first operation. In 1963 he became the Commander of the Natal Regional Command of MK. In 1983, Kasrils was appointed Chief of MK Intelligence. He served on the ANC's Politico-Military Council in Lusaka from 1985, on the National Executive Committee from 1987, and on the South African Communist Party's Central Committee from 1985. From 1991 to 1994, Kasrils also headed the ANC's Campaign Section at the organisation's headquarters in Johannesburg, was an active participant in the negotiations between MK and the former South African Defence Force and a member of the Transitional Executive Council 's Sub-Council on Defence.

Sandra Botha is the leader of the opposition party, the Democratic Alliance (DA) in the National Assembly. Her political career includes her appointment as Deputy Director of the Independent Electoral Commission in the Free State in 1998. After the 1999 election she was selected as the Free State Democratic Party Representative to the National Council of Provinces where she was appointed Caucus Leader from 2000-2004. In 2004, the Free State Electoral College of the DA placed Sandra first on the National Assembly list and in the same year she became the first DA MP to be elected as House Chairperson of the National Assembly.

Imtiaz Fazel is a chartered accountant and holds the position of Chief Operating Officer in the Office of the Inspector General for Intelligence.

Barry Gilder joined the ANC's armed wing – Umkhonto we Sizwe – in 1979 and in 1980, the ANC's Intelligence Branch (DIS) in Angola. From 1983 to 1989 he headed DIS in Botswana. In 1994, he was appointed to the South African Secret Service (SASS). In January 2000 he moved to South Africa's domestic intelligence service – the National Intelligence Agency (NIA) – as Deputy Director General Operations. In May 2003 he was appointed as Director-General of the Department of Home Affairs. In March 2005 he was appointed Coordinator for Intelligence, where he served until his retirement in October 2007.

Sam Sole has been a journalist for 20 years. Sole's work has focused on exposing the 'hidden hand' of the state, both during the apartheid era and since 1994. His first major investigation related to circumstances surrounding the Goniwe murders and the activities of the so-called Hammer Unit, a Citizen Force special unit used for undercover military operations in the Eastern Cape. In late 1994 and 1995, Sole and veteran journalist Jean Le May broke the story of the existence of South Africa's Chemical and Biological Warfare programme and the role of Dr Wouter Basson in it. In 2003, he won the Vodacom Journalist of the Year award for breaking the story of the Scorpions investigation of then Deputy President Jacob Zuma. In the same year Sole won the Mondi award for Investigative Journalism with colleague Stefaans Brummer. Sole and Brummer worked together on the Oilgate expose of 2005.

Chantal Kisoon is deputy director at the South African Human Rights Commission. She specialises in monitoring the implementation of the Promotion of Access to Information Act within the South African public service.

Melissa Moore is the head of the Law Clinic at the Freedom of Expression Institute based in Johannesburg, South Africa. The purpose of the FXI Law Clinic is to promote the objectives of freedom of expression and access to information through providing legal services for litigation and precedent setting cases in relation to freedom of expression.

Lauren Hutton was appointed as researcher in the Security Sector Governance Programme at the ISS Tshwane (Pretoria) office in January 2007. She joined the ISS as a consultant for the Southern African Human Security Programme in 2006. She works on the African Security Sector Governance Project and focuses on parliamentary oversight of the security sector, with specific interest in the governance of the intelligence sector. Other fields of interest include gender and defence and broader issues of security sector reform in Africa**.** She initiated a project on the democratic governance of the intelligence sector in January 2007.

Foreword

> The role of the public in stimulating debate on the way intelligence services should function in an open and democratic society is essential…we welcome the public's involvement, which can only strengthen our intelligence services and build the necessary trust and confidence required in a democracy'
>
> *Ronnie Kasrils (MP), Minister for Intelligence Services*
> *4 December 2007, Business Day*

The attitude conveyed by Minister Kasrils in the above statement is a defining characteristic of the current internal environment of the 'secret' sector in South Africa. Since the country's transformation to democracy in 1994, the national intelligence apparatus has been regularly reviewing and reforming its efforts to more fully integrate the ideals of democracy into the governance practices of a sector, which, by its very nature, presents certain challenges to democratic control. The comprehensive intelligence reform that took place after the demise of apartheid resulted in the establishment of key mechanisms for exercising democratic control of the intelligence services. These mechanisms included the Joint Standing Committee on Intelligence and the Office of the Inspector General.

One characteristic of democratic governance generally absent from the discourse on the intelligence sector in South Africa, has been public interaction, engagement and participation. The review processes currently underway within the intelligence community provide a unique opportunity for encouraging public debate on fundamental issues like the nature and character of the intelligence services. Amongst these core issues is the role intelligence services should play in a democratic dispensation, upholding simultaneously both national security requirements and civil liberties.

As one of the key participants in the intelligence governance debate in South Africa, the Institute for Security Studies has, by means of its Security Sector Governance Programme, been playing an increasingly significant role with its objective research on the democratic governance of the intelligence sector. This has included disseminating information on the sector, focusing specifically on the civilian intelligence sector, and offering a platform for public engagement on such issues. The ISS, as a civil society stakeholder, is thus well placed for providing for dialogue between the intelligence community and the public at large.

Accordingly, during July and August of 2008, the Security Sector Governance Programme hosted a series of public seminars in South Africa on the nature and role of the intelligence sector. The objectives of the seminar series can be defined as follows:

- Enhancing understanding of the South African intelligence apparatus;
- Encouraging critical thinking on the role that the intelligence services should play in enhancing the security of the state and its people;
- Providing a platform for interaction between the intelligence community and the public as a mechanism for building the trust and dialogue characteristic of a vibrant democratic state;
- Encouraging civil society to engage in intelligence- related issues and to promote the development of research and discourse on the topic;
- Serving as a confidence-building measure towards African collaborative security.

This report serves as a summary of the series of seminars and includes most of the papers presented. We extend our thanks to all who participated in the events, especially the Minister for Intelligence Services, Mr Ronnie Kasrils, for his participation in and support of this initiative.

(Ms) Lauren Hutton
Researcher
Security Sector Governance Programme
Institute for Security Studies
Pretoria
South Africa
September 2008

REFERENCES

Kasrils, R. 2007. Redefining the boundaries of intelligence, in SA. *Business Day,* 4 December 2007. Available online at: http://www.businessday.co.za/articles/topstories.aspx?ID=BD4A649000 last accessed 3 September 2008.

1 Secrets, spies and security

An overview of the issues

Lauren Hutton

As the title of the series of papers suggests, there are two primary issues for discussion. On the one hand, the question 'To spy or not to spy?' has been posed. This question asks us to consider the nature of the role and function of the South African intelligence community and the role of the secret sector in the security apparatus of the state. On the other hand, the issue of the relationship between intelligence and democracy in South Africa is also brought to the fore. Seeking to establish and maintain democratic control of the intelligence sector is a challenge for even mature democracies. It is therefore important to consider and evaluate how the South African intelligence community is grappling with meeting the democratic demands of openness and accountability while, at the same time, maintaining the secrecy deemed necessary if intelligence is to function effectively.

WHAT ROLE FOR THE SOUTH AFRICAN INTELLIGENCE COMMUNITY?

The issue of the role of intelligence in South Africa lies at the core of any discussions we may have about the intelligence sector. How can we assess whether or

not intelligence is doing its job if we do not understand what that job is? The issue of the role and function of intelligence in South Africa is actually more complex than merely being able to evaluate successes and failures. One could, in fact, argue that in a democratic state it is essential to have some kind of consensus or agreement on the role and function of the security services. I very much doubt the existence of such an agreement in South Africa. Instead, there is the general perception of government's reliance on the intelligence community to obstruct democratic processes, be it through interference in intra-party politics or through spying on institutions of democracy: opposition parties, the media and the judiciary.

In 1994, with the transition to democratic rule, the role and function of the intelligence community was the subject of interrogation and debate. At that time, it was one of the imperatives of democratic transformation to move away from the position in which the intelligence community, broadly speaking, was utilised as a tool of oppression and the maintenance of minority control. The 1994 White Paper on Intelligence serves as the first comprehensive statement on the nature, role and function of democratic intelligence services. It states that the intelligence machinery serves the Constitution and government of the day, implying that intelligence is a tool in the government arsenal to further the aims and objectives of the elected government.

Moreover, the White Paper defines intelligence as:

> The product resulting from the collection, evaluation, analysis, integration and interpretation of all available information, supportive of the policy and decision making processes pertaining to the national goals of stability, security and development.

In this definition of intelligence, we can see the priorities of the intelligence community assuming a focus on the greater national agenda of stability, security and development. Interestingly, this is also an arena of intense debate and contest. Should the national intelligence structures grant attention and priority to issues pertaining only to security (narrowly-defined security), or is there a role for the intelligence community to play in achieving the laudable goals of development and stability?

As the primary policy document establishing the role and functions of the intelligence sector, the White Paper articulates the government's stance on

the role intelligence should play. In this respect, it is clear that the functions of the intelligence community are not limited to issues that could manifest as traditional threats to the security of the state and the Constitutional order. Intelligence is defined as being focused on issues pertaining to the national goals of security, stability and development.

We could debate in much more detail whether or not this should indeed be the focus of the South African intelligence community. On the one hand, a very sound argument could be made for the need to marshal all the tools of state power in the fight against poverty and underdevelopment. Moreover, especially in a transition state, a strong case could be made for the need for the intelligence sector to maintain a strategic interest in state stability in order to prevent an outbreak of the violent conflict so common in emerging democracies and post-conflict environments.

An opposing argument would question whether or not, given the nature of intelligence, the intelligence community could play a successful role in a broader national development policy. One could easily ask when it would no longer be a strategic imperative to employ the coercive and secretive tools of state power domestically. If we could accept that a focus on stability, specifically and exclusively domestic stability, is a justifiable and necessary task of the intelligence community in transitional democracies, when does it become unnecessary and unjustifiable to deploy the intelligence apparatus against potential domestic (political) 'threats' to national stability?

To answer this, we have to step back and understand what constitutes threats to domestic stability. As threat perception generally drives the development of intelligence capacity, understanding domestic threats should provide an indication of (a) the role that the intelligence services can play in countering such threats and (b) the possibility that other state agencies or institutions of democracy ought to be central to countering such potential threats.

In a section of the White Paper detailing internal realities facing the South African intelligence community, the following observations are made:

> Massive socio-economic degradation, with poverty, hunger, homelessness and unemployment being the order of the day, will render the political changes meaningless if they are not accompanied by a significant improvement in the quality of our people's lives. Whilst politically motivated violence is on the decline, there has been an increase in common criminal activities.

> These socio-economic problems call for creativity and commitment in the implementation of the RDP. At the same time, the government and society must be firm in dealing with crime and lawlessness.

When those threats to national stability organise into coordinated efforts to undermine the Constitutional order of the state or the physical security of its citizens, there is no doubt that this should fall within the ambit of legitimate civilian intelligence functions. However, one cannot but wonder about the perceived role of the intelligence sector in response to threats relating to the poverty and socio-economic disparities. Intelligence services are undoubtedly an essential tool in the fight against crime, but should that task be fulfilled by a civilian intelligence service or by a crime intelligence unit contained within the national police structure?

Given that the White Paper, as illustrated above, highlights crime and socio-economic conditions as internal threats to South African stability, what role can be envisaged for the civilian intelligence dispensation? What we have witnessed, especially in the past few years, is that the expanded role for the domestic intelligence service has led to the intelligence apparatus focusing attention on a wide range of non-traditional issues such as potential disruption by labour disputes and the potential instability emerging from the ANC succession debate.

This should, however, be viewed in context. Internationally, the trend is for a limited domestic intelligence function, limited in the light of the threats and issues that receive attention from the intelligence agencies. This is often restricted in terms of legislation on, for example, threats to the constitutional order of the state, or domestic threats that are likely to result in violence. Such a mandate therefore encompasses a wide range of threats and potential threats, including, inter alia, subversion, terrorism and organised crime.

The African context differs in that the intelligence services of African states have followed the democratic development trajectory of the African state. In other words, most African intelligence services have their roots in the security architecture established by the colonial rulers, which was often adopted and maintained by the post-independence authorities. Given that internal instability, political fragmentation and contestation for power were the primary characteristics of many African states; the intelligence sectors have developed alongside the threat perceptions of the authorities. These have largely been threats of an internal nature as well as threats to the authority or power of the ruling regime.

In short, it is not uncommon to find intelligence services in Africa that have been utilised as tools of oppression for the maintenance of group, personal or elite political power.

South Africa emerged from such an environment in 1994, and massive reforms were achieved within the security sector. The mandate, functions and controls on the intelligence sector were transformed into a leading model of democratic governance. Further, in comparison with that in the apartheid period, the intelligence community (civilian and security forces) in the current era has a vastly limited domestic function. This is based largely on the changes in the political environment as well as on the transformation of the function of the state security apparatus into tools serving the interests of the majority of the citizens.

However, we should consider and question whether there is still a need for a domestic intelligence service that has a function of devoting its attention to political intelligence.[1] The main concern with the continued existence of a domestic mandate so broad as to include any item that could cause instability is the potential for abuse. The power to utilise the covert tools of the state should be very carefully controlled and the current open mandate for domestic intelligence activities provides fertile ground for abuse. The domestic intelligence capacity should be the tip of the spear, the point that protects citizens at home. The real issue is to decide whom it will protect and from what.

SECRECY, TRANSPARENCY AND DEMOCRATIC IDEALS

> The development of a more open intelligence community will go a long way towards demystifying and building trust in the national intelligence community. Where legal limits on secrecy, including criteria and time frames for classification and declassification, are clearly understood and accepted by society, the dangers of the intelligence becoming self-serving are averted.
>
> *White Paper on Intelligence 1994*

As the above quotation from the White Paper on Intelligence indicates, a key element in the reform of the South African intelligence sector was the creation of more openness and improved civil-security relations. Linked to this need for more openness and transparency, and therefore less secrecy, is the

issue of the protection of information. As pointed out in the White Paper, the uncontrolled and excessive use of secrecy increases the potential for abuse of the intelligence and security services. In essence, uncontrolled and excessive secrecy undermines the very fabric of democracy; it can be a source of instability and can even be detrimental to countering certain threats to security. Without an adequate legal framework to govern the use of secrecy, the possibility for abuse exists.

Currently the Protection of Information Act 84 of 1982 is the primary statute governing the use of secrecy or rather the protection from disclosure of certain information. Before even opening the legislation, one is cognisant that this is a 1982 act dating back to the pre-democratic era. Considering the importance of this legislation to democratic governance, it is alarming that it remains unchanged after more than 14 years in the democratic order have elapsed. More open and transparent governance could certainly have been created. The Protection of Information Act was amended through other legislation that has come into effect, but the 1982 secrecy regime remains essentially intact.

The Act is problematic in that it is about information that should be protected from disclosure, but it does not identify such information nor does it set out criteria for disclosure. In other words, there is no framework for the classification and declassification of information in the legislation. To illustrate the breadth of the current legislation, consider the following extract:

PROHIBITION OF OBTAINING AND DISCLOSURE OF CERTAIN INFORMATION

Any person who, for the purposes of the disclosure thereof to any foreign State or to any agent, or to any employee or inhabitant of, or any organisation, party, institution, body or movement in, any foreign State, or to any hostile organisation or to any office-bearer, officer, member or active supporter of any hostile organisation–

- Obtains or receives any secret official code or password or any document, model, article or information used, kept, made or obtained in any prohibited place; or
- Prepares, compiles, makes, obtains or receives any document, model, article or information relating to-

- any prohibited place or anything in any prohibited place, or to armaments
- the defence of the Republic, any military matter, any security matter or the prevention or combating of terrorism shall be guilty of an offence and liable on conviction.

Undoubtedly a new framework is needed for the protection of information, including clear and distinct guidelines for its classification and declassification. Inherent in this are the issues of secrecy and transparency and the potential of 'illegitimately' using secrecy (i.e. classification) to manipulate, hide abuse and maladministration, and essentially to curtail democratic participation and accountability.

The new proposed regulatory framework for the protection of information was published in the *Government Gazette* on 18 March 2008. The Protection of Information Bill has been widely debated: in the Ministry for Intelligence Services, in Cabinet, in Parliament, in civil society and in the media. The bill was not well received by the South African public. In the first scathing attacks, the Bill was labelled a sinister proposal, the enemy of democracy and a blatant attempt to gag the media.

Some valid points were made in critique of the Bill. Citizens in a democracy should interrogate and subject to public debate any potential attempt to curtail transparent governance. At the heart of the debate on the Protection of Information Bill was the question: How does the state secure information which, if released, could cause demonstrable harm, while at the same time not reducing the Constitutional right of access to information? Much of the public discourse and debate, however, became extremely skewed. Debate focused primarily on the Bill as an attempt to prevent the media from publishing information that could bring disrepute to the state or those in service of the state. Most particularly, the Bill was seen as an attempt to stop the publication of articles exposing corruption and mismanagement.

Submissions by civil society groups to the Ad Hoc Committee on Intelligence Legislation made further arguments against provisions in the Bill. Such arguments are presented in other papers in this collection of presentations, so this section will not elaborate in detail on the pros and cons of the Bill. Interestingly, this Bill attracted a remarkable amount of public attention. There was a great deal of media coverage as the debate moved through the legislative process,

probably because the media had a vested interest in how some of the clauses could apply to them.

Some very real criticisms can be made of the Protection of Information Bill, and it is going to be interesting to see what changes emerge from the parliamentary process. Even more interesting has been that, by means of this process, discussion on issues of secrecy and transparent democratic governance in South Africa has been energized.

CONCLUDING REMARKS

This chapter is an introduction to the issues to be discussed in more detail in the papers that follow. Some background information on the debates that fill the rest of these pages has been provided. We have not tried to reach any agreement on the points raised. Different perspectives have been offered to encourage others to further interrogate these issues in the hope of stimulating even greater interest and dialogue on the intelligence sector.

NOTE

1 There are obviously other important tasks that the domestic intelligence service fulfils including counter terrorism and counter intelligence duties.

REFERENCES

Protection of Information Act 84 of 1982, Cape Town: Republic of South Africa.

White Paper on Intelligence 1994, Cape Town: Republic of South Africa.

2 To spy or not to spy?*

Intelligence and democracy in South Africa

Ronnie Kasrils

INTRODUCTION

To spy or not to spy? To be or not to be? Can a nation state be what it aspires to be without an effective intelligence service that collects and analyses secret information that enables its leaders to make better informed decisions? I think not. As a fan of John Le Carré, may I point to the advice of one of his most legendary characters, George Smiley, imparted to a group of newly-recruited officers, in which he asks:

> Why spy…For as long as rogues become leaders we shall spy. For as long as there are bullies and…madmen in the world…For as long as nations compete…politicians deceive…tyrants launch conquests…your chosen profession is secure… (Le Carré, cited in Lathrop 2004).

LEARNING FROM HISTORY

The need for intelligence has, in fact, existed since the dawn of time, and the origins of the profession can be traced back to the Old Testament, as evidenced by the reference to Moses despatching his spies across the River Jordan to bring

* Dedicated to the memory of Dr Rocklyn 'Rocky' Williams.

back reports about the land of Canaan. Its genesis is reflected by our prehistoric ancestors, who scanned the environment well beyond the cave, gathering information with which they could ensure the perpetuation of our very species.

As human societies evolved, growing ever more complex and interdependent in their interactions with each other, so the need for intelligence grew, as leaders across the centuries increasingly relied upon the skills of their spies to advise them of threats to their vital interests.

Examples abound among the ancient Greeks, Persians, Moguls and Chinese. The 6th Century Byzantine historian Procopius stated that:

> from time immemorial the [Byzantines]…had maintained a large number of agents who used to travel among our enemies…they would make detailed inquiries of all that was afoot, and…were…able to…report on…the enemy's secret plans to…government, who, forewarned… [were] put upon their guard (Procopius, cited in Lathrop 2004).

Procopius cautions against the neglect of intelligence. This happened under the rule of Emperor Justinian, who, argues Procopius, '…would spend nothing; and…abolished the very name of secret agent…'. Procopius highlights the 'many disasters' that befell the Byzantines arising from this neglect, as they 'had not the remotest idea of…' their enemy's plans or movements 'at the time' (cited in Lathrop 2004).

These developments illustrate how intelligence was viewed as an indispensable adjunct to statecraft, which ultimately gave rise to the establishment of specialised intelligence services with both national and international reach. These remain a permanent feature of nation states today. Given the threats in our unpredictable global world that knows no borders, we cannot afford to discard this age-old craft, and must be ever mindful of Procopius's warning.

Yes, we must collect and analyse unique information, most often under the cloak of secrecy, in order to ensure the security of our state, our people and the country. No responsible government can allow the neglect of intelligence of which Emperor Justinian was guilty.

THREE CONSIDERATIONS

Trusting that I have made the case for why it is essential to establish intelligence services, let me now deal with three considerations relevant to this discussion.

Firstly, it is important to remember that intelligence has been employed in pursuit of very different objectives, depending on the character and nature of the state. Historically, empires used it to advance their imperialist ambitions, laying claim to other's territory, plundering their resources and subjugating their people. Others used it for more noble ends, countering these sinister designs in defence of their territory, as evidenced in the valiant struggles of the indigenous kingdoms of Southern Africa against colonial conquest from the 17th Century. While the intelligence services of today contain many common features, they also contain key differences, whereby their mandate and the manner in which they conduct it, mirrors the priorities and value systems of the societies they serve, ranging from autocratic through authoritarian and imperialist to democratic.

Secondly, it is necessary to appreciate how the emergence, growth and strengthening of democracy effected a decisive shift in intelligence. Services, as was the case in the past, could no longer simply be concerned with preserving the security of the state, its military power and dominance by elites, where they were (and often still are) used as tools of oppression and control. Democracies are expected to protect the security of all their citizens, including their human rights, like the freedom from want, and fundamental freedoms. This is also called human security.

A problem that exists must be rectified. On one hand, too broad a mandate, particularly in socio-economic issues, may be too great an intrusion into public territory, while, on the other hand, it could be raising unrealistic expectations of what the intelligence services should be capable of. For example, there are complaints that the National Intelligence Agency (NIA) is far too intrusive, yet, as seen during the recent outbursts of violence against foreigners, the complaint becomes: Where was NIA? Why did the spooks not predict it? I will return to the question of NIA's mandate in due course.

Thirdly, experience demonstrates that, if they are not subject to specific safeguards, the special powers and capabilities provided to intelligence services could be abused, manipulated or misdirected, thereby undermining the very rights and freedoms that they are expected to protect. Democracies therefore began to realise, in the words of an intelligence commentator: 'that the medicine…if not administered under the very strictest and widest supervision [could]…have the effects which are as damaging as the disease' (Porter, cited in Gill & Phythian 2006).

It was precisely because of such dangers that democracies have, in answer to the age-old quandary *Quis custodiet ipsos custodes? Who shall guard the*

guards?, subjected their intelligence services to laws, controls and oversight – the guardians of the guards; the supervisors of the spies - so as to limit these harmful outcomes, by facilitating their accountability and professionalism, and ensuring a close check on the legality, propriety and effectiveness of their activities.

THE SOUTH AFRICAN CONSTITUTION, LEGISLATION AND REGULATIONS

It is these considerations that informed South Africa's perspective in fashioning a new intelligence dispensation, as enshrined in the provisions of our founding Constitution. It is from this that all subsequent legislation must flow, creating a vast distance between our country's painful apartheid past, when the intelligence agencies were deeply compromised by serving an iniquitous system, and today's democratic aspirations.

The Constitution, by providing for the establishment of the intelligence services, recognises their importance and necessity in building a society based on democratic values, social justice and fundamental rights. In so doing, it envisions them as a credible force for good in protecting the state, its citizens and the democratic order, according the intelligence services special powers and capabilities for that purpose.

Yet these powers and capabilities are by no means unfettered, and whatever fears and misgivings some might have about the intelligence services, as witnessed in the way they are treated in the media, our Constitutional imperatives provide for powerful checks and balances.

In this regard, the Constitution (Chapter 11, Section 198, 209 & 210) clearly spells out the key principles and directives for the intelligence services:

- It sets out their noble purpose, by providing that: 'National security must reflect the resolve of South Africans, as individuals and as a nation, to live as equals, to live in peace and harmony, to be free from fear and want and to seek a better life' (Chap 11 Sect 98a)
- It declares that they are bound by the law - including international law – where no member may obey a manifestly illegal order. It requires them to secure this legitimate conduct by example and by teaching all members to act in accordance with the Constitution and the law.

- It reinforces the need to ensure that they exercise non-partisanship in discharging their mandate, which must be carried out in the national interest of all our people – irrespective of colour, creed or party affiliation - prohibiting members from undertaking their functions in a manner that either prejudices or furthers the interests of any political party
- It asserts that they cannot operate in isolation as a law unto themselves, as they are subject and accountable to the civilian oversight, control and authority of Parliament and the national executive. To this end, it requires them to be established and regulated by national legislation, which must elaborate on their mandate, powers and functions, stipulating that the law must also set out the mechanisms for civilian oversight, control and monitoring of their activities.

But it is not only these high-sounding principles, virtually unsurpassed anywhere in the world, that define the role and function of our intelligence services. We have put in place the legislation and oversight bodies to enforce the necessary Parliamentary and public control. In this we are also amongst the foremost in the world. In fact only a handful of countries have intelligence oversight to begin with – the United States, Norway, Britain, Canada, Australia and New Zealand. However, in many instances, these countries are not as elaborate as South Africa in their control framework and transparency. Incidentally, it should be noted that many intelligence services around the world still reside under the authority of the military (amongst others, France, Belgium, Brazil) rather than under more transparent, accountable civilian control.

The White Paper on Intelligence (1994), the National Strategic Intelligence Act (1994) and the Intelligence Services Act (2002), establish the guidelines and regulate the activities of the intelligence services, providing the framework for effective control and oversight. This is further reinforced by the Intelligence Services Oversight Act (1994), through the establishment of the Office of the Inspector General of Intelligence and the Parliamentary Joint Standing Committee on Intelligence (JSCI), provided for in the Constitution.

Not only do these oversight mechanisms provide for ongoing review of the work of the intelligence services, but members of the public can also submit complaints to them for further investigation, if they feel that their rights are being unlawfully infringed. Beyond the Inspector General and JSCI, it is also important to add that their activities are also subject to the scrutiny of, amongst others, the Human Rights Commission, the Public Protector and the courts.

Coupled with these external oversight mechanisms are internal controls that set out the criteria and processes that inform the operations of the intelligence services. The Minister is required to issue regulations, complemented by internal directives by the Heads of the Services, on matters ranging from security vetting to procedures for placing targeted individuals under surveillance.

These oversight and control mechanisms should not only mitigate against abuse by the intelligence services, but also enable them to work in an effective, efficient and focused manner. For example, the requirement in our law providing that they can intercept an individual's communications only once the necessary judicial authorisation has been obtained ensures that operations are directed against genuine threats; that their powers are appropriately used in proportion to the nature of the threat; and that any evidence of criminal activity arising from the particular interception can then be used in subsequent court proceedings in support of the prosecuting authorities.

The Constitution and the accompanying regulatory framework therefore clearly provide for oversight and control, setting the parameters for the professional, legitimate and lawful conduct of our intelligence services. They provide certainty about the rules, how to follow them and the consequences of non-compliance.

THE INTELLIGENCE MANDATE

The mandates of the national intelligence structure, that is, the National Intelligence Agency (NIA), the South African Secret Service (SASS), the National Intelligence Coordinating Committee (NICOC), Defence Intelligence and Crime Intelligence are set out in the National Strategic Intelligence Act, as required by the Constitution. For the purpose of this paper I will focus on the mandate of the NIA.

The NIA's mandate is to gather domestic intelligence in order to identify any threat or potential threat to the security of the country. Domestic intelligence is defined as intelligence on any internal issue that is detrimental to the national stability of the Republic, as well as threats or potential threats to the constitutional order of the Republic and the safety and wellbeing of its people (National Strategic Intelligence Act 39 of 1994).

Threats to the constitutional order include espionage, terrorism and subversion, those areas traditionally associated with domestic intelligence and

security services. In translating the mandate into operational focus areas, the services defined their functions in the context of the national security philosophy as articulated in the White Paper on Intelligence. This was developed in 1994 as the framework document for the establishment of the democratic intelligence community.

The White Paper argued for a shift away from a state-centric approach to security in favour of a national perspective premised on the notion that the objectives of security policy must go beyond ensuring the security of the state. It should, in fact, encompass the pursuit of democracy, sustainable economic development and social justice. To quote from the White Paper:

> The implication is that security policy should deal effectively with the broader and more complex questions relating to the vulnerability of society. National security objectives should therefore encompass the basic principles and core values associated with a better quality of life, freedom, social justice, prosperity and development.

The White Paper sought to articulate that the intelligence services of the country should perform their functions in defence of the people, in pursuit of democracy, and that security can truly be achieved only in a context where the people of a country are free from political injustice and social inequality. These principles are laudable, especially given our history, when apartheid security services acted to support the interests of a white minority at the expense of the majority.

However, the implication of this very broad interpretation of the NIA's mandate was that it was expected to provide intelligence on a range of social and economic issues affecting the country. In the initial years after amalgamation, NIA established operational components to focus on what was called political and economic intelligence to advise on a broad range of such issues.[1]

The late Dr Rocklyn "Rocky" Williams, a former ANC intelligence operative and later academic of note, cautioned against what he termed the 'securitization' of the state (Williams 2004). What he was warning against was an interpretation of the notion of human security that resulted in the involvement of the intelligence services in all areas of public life. A national security policy informed by a human security perspective cannot mean that the intelligence services should be involved in every aspect of public life. Other government

departments, academics and research institutes are best placed to provide expert advice on, for example, the impact of service delivery issues on the general well-being of people. It can be argued that to expect the intelligence services to expend resources on such issues is inefficient, but could also lead to the perception that the intelligence services are unduly intrusive. Indeed this was seen during the local service delivery protests and provincial border dispute issues of recent years, when trade unionists, political parties, community organizations and the media alike raised a general complaint about the iniquity of NIA members.

The experience of such protests and the more recent eruptions of violence against foreigners in our midst, resulting from socio-economic causes, has led to an internal review of how the NIA mandate should best be applied: to widen it or narrow it? Socio-economic contradictions are located in the very structure of our present social system, and require government's policy interventions. The intelligence services may well monitor developments on the ground and should be part of state institutions advising government. The focus of the intelligence services, however, should be on the "trigger points" where localized outbursts might occur, whether spontaneous or organized. This is of course no easy task. It is well nigh impossible to predict spontaneous outbursts. Not much easier to forecast are those micro-organized actions that can be predicted only by reliable sources on the ground. That is the challenge for the NIA. Without well-placed sources – and, heavens knows, they cannot be everywhere – it is akin to the weather forecaster predicting the time and place where sudden hailstorms will be triggered by inclement conditions.

My contention, in concurring with Rocky Williams, is that the focus of the intelligence services needs to be on the "trigger points" and not on the all-embracing socio-economic climate in the country.

DEALING WITH ABUSE IN A DEMOCRACY

There will always be those officers who attempt to subvert the Constitution and the regulations, as has happened both internationally and in our own country as recently as in 2005. It must be said that our experience, unfortunate as it was, in fact demonstrated the effectiveness of our oversight regime. These transgressions were uncovered shortly after they were carried out by an investigation undertaken by the Inspector General; launched in terms of

the law at the request of the executive on the receipt of a complaint from a member of the public.

Where there are abuses, despite the existence of these measures, the key challenge is to ensure that the subsequent interventions go beyond simply dealing with a few bad apples. The point is to make the barrel as rot-proof as possible by strengthening measures and dealing with weaknesses, so as to counteract the potential for a recurrence. It is for this reason that we embarked on an extensive evaluation process, which has resulted in the introduction of new initiatives and wide-ranging reforms. I would claim that this process demonstrates how keen government is to strengthen the governance and management of intelligence practice. This reform process has involved seven initiatives.

- ***Five Principles of Professionalism***
  Efforts have been directed to enhancing an awareness of the necessity for legality and propriety at all times in our work, based on the Minister's *Five Principles for Professional Intelligence Officers*. These flow directly from the Constitutional provisions referred to earlier and were articulated after the bad experience of 2005: namely that our members acknowledge that they:
  - do not stand above the law;
  - are accountable to the executive and Parliament;
  - accept the principle of political non-partisanship;
  - owe their loyalty to the Constitution, our people and the state;
  - appreciate that they must maintain high standards in the performance of their functions.

- ***Civic Education Programme***
  Central to the attainment of this professional ethos is our Civic Education Programme, which is being developed in a series of seminars that seek to shift mindsets and ensure that all officers have a clear understanding of the Constitution, relevant legislation and their responsibilities to our people. Its implementation is supported by lively internal debates on a range of topics to inculcate a spirit of engagement and critical thinking about the complex challenges confronting the intelligence services of a democracy. Elements of the programme's curriculum are also being integrated into our existing training initiatives, in which our curricula impart tradecraft skills as well as instil discipline, professionalism and ethical work practices. By

these means such imperatives are ingrained as second nature in the actual operational environment.

- ***Strengthening internal policies***
  Also important is the evaluation that we proceeded to conduct of all our internal policies in order to secure greater conformity with our Constitutional framework. In so doing, we have sought to deal with any deficiencies, ensuring at all times that the rule of law is strictly observed; that our capabilities are deployed responsibly in proportion to genuine security threats and are weighted against the potential damage to fundamental rights.

  We have translated these policies into Standard Operating Procedures for each area of work, spelling out the rules by which they must be implemented, so as to provide further guidance for our officers in the course of their management and operational duties, where short-cuts and bending of rules are more likely to occur. We have also established internal assurance bodies to monitor and enforce compliance at the operational coal-face, enabling us to prevent any deviations from regulations or curb these should they arise.

- ***Introducing legislation***
  We are bringing the legislation governing our protection of information regime into harmony with our Constitution, as reflected in our Protection of Information Bill, which seeks to regulate the way in which government information should be secured within an open and democratic society. I do not intend to go into detail here, as this topic will be covered in a later seminar, as part of the Institute for Security Studies (ISS) public dialogue series. Suffice it to say that the Bill is not a 'Kafkaesque' ploy to obstruct the work of journalists and researchers.

  Rather it is aimed at protecting sensitive information, which must lawfully be restricted by criminalising the actions of those who attempt to gain unauthorised access for the purpose of prejudicing our country's national security. In fact, the Bill will facilitate access to government information by ensuring that any decision taken to restrict information is done sparingly, lawfully, legitimately and is justified within the context of our Constitution, making it an offence to use this process as a cloak to hide government corruption, incompetence or abuse. Overall it makes access to government information far easier than before, balancing transparency with the necessary

confidentiality. In a nutshell, it seeks to reconcile demands for transparency in an open society with the necessity for secrecy.

In addition, we have drafted two Amendment Bills, the Intelligence Services Amendment Bill and the National Strategic Intelligence Amendment Bill, which, apart from numerous technical changes, establishes the National Communications Centre as a separate organizational entity and provides for tighter control over its operations.

- ***Ministerial Review Commission***

  All these initiatives are being assessed by the independent Ministerial Review Commission, established to evaluate and make recommendations on all our legislation and mechanisms of internal control in order to ensure better compliance and alignment with the Constitution and the rule of law. The Commission's report should soon be completed and will be made public. It will no doubt provide a basis for introducing further reforms and continuing the public engagement that has already begun.

- ***Public Debate***

  The common thread binding these initiatives is our belief that matters of intelligence policy must be subject, where possible, to informed public debate and scrutiny. While secrecy is necessary for aspects of intelligence, it is certainly not essential for all of them, which is why we welcome this ISS initiative. Such dialogue ensures that the public is party to shaping key decisions on critical issues impacting on their lives. It also allows our citizenry to have a clear understanding of our role, so that they are not misled or intimidated by those who falsely purport to act with our blessing, either overtly or tacitly, in advancing their own or others' agendas.

  Such fraudulent behaviour has been detrimental to the intelligence services in general and in particular to the NIA, which is an easy target, given its potentially intrusive domestic mandate. If I could make a plea, it would be for the press, politicians and public to become better informed so as not to be susceptible to the false assertions of those who claim to be acting in the name of the NIA or any other intelligence organ for that matter. Perhaps at this point I can make it clear that we have not been involved in the succession battles of any party, nor of the forthcoming trial of the President of the African National Congress.

- ***Institutional culture***

  Whilst laws, regulations, controls and oversight mechanisms are critical, they are not sufficient, because so much depends ultimately on the integrity of the men and women of the intelligence community themselves. The single greatest guarantee against any abuse lies with them. Their endeavours are supported by ongoing training and building an institutional culture that respects and understands the Constitution, the law, the implications of the conduct of operations, and their relationship to the state.

  What we aim to achieve is to have all officers abide by the Constitution and the law, not simply because they have to, but because they view this as integral to their professionalism and effectiveness. This will contribute to the improved quality of their work and a deeper sense of personal confidence in their decision-making and actions, informed by a sophisticated world-view, which enables them to set aside any preconceptions and strive to provide objective judgement.

CONCLUSION

It should be borne in mind that ours is a very young democracy, with an intelligence dispensation that was formally created only in 1995. While much progress has been made, much remains to be done. It will take patient and consistent effort to secure the level of sound professionalism that we require and aspire to. I believe we have come a long way in establishing intelligence services working in defence of our Constitution and for our people. As long as we continue along these lines, we will get better still.

In closing, I leave you with the following statement, which I believe underpins what we are attempting to achieve: '…Intelligence is…essential…but it is, being secret...most dangerous. Safeguards to prevent its abuse must be devised, revised and rigidly applied. But as in all enterprises, the character and wisdom of those to whom it is entrusted will be decisive. In the integrity of that guardianship lies the hope of free people to endure and prevail' (Stephenson 1976:xvi)

That is something that Le Carré's George Smiley would surely sign up to. I welcome this series, which provides a platform for much needed public engagement on issues extremely relevant to safeguarding our Constitution and democracy, and the public awareness and academic interest that it will hopefully generate.

NOTES

1 These operational components have subsequently been closed down because of concerns that they contributed to NIA's involvement in political affairs of the country, following the report on the Masetlha Affair by the Inspector General, March 2006.

REFERENCES

Constitution of the Republic of South Africa Act 108 of 1996. Cape Town: Republic of South Africa.

Gill, P. & Phythian, M. 2006. *Intelligence in an insecure world*. Cambridge: Polity.

Lathrop, C.E, 2004. *The literary spy*. New Haven, CT: Yale University Press.

National Strategic Intelligence Act 39 of 1994. Cape Town: Republic of South Africa.

Stephenson, W. 1976. *A man called Intrepid*. New York: The Lyons Press.

White Paper on Intelligence 1994. Cape Town: Republic of South Africa.

Williams, R. 2004. Paper presented at the National Security Strategy Workshop hosted by NICOC, September 2004.

3 Intelligence and democracy in South Africa

Sandra Botha

I would like to thank the Institute for Security Studies (ISS) for hosting this important public discussion series and for affording me the opportunity of imparting the perspective of the Democratic Alliance (DA) on the role of the intelligence services in our democracy.

Mine will undoubtedly be a political perspective, but one which I hope you will find to be a constructive contribution to the ongoing efforts to unpack the important topic of how the functions of an intelligence service and its structures should be pursued in a democratic country like South Africa. This topic is of great importance in view of the important role intelligence services play in ensuring the political and economic stability of democracies around the world.

In South Africa, as Minister Kasrils has on occasion pointed out, it is also important for the purposes so uniquely prescribed in our Constitution: that our intelligence services 'must reflect the resolve of South Africans, as individuals and as a nation, to live as equals, to live in peace and harmony, to be free from fear and want and to seek a better life' (Chapter 11 Section 198a).

COMPLYING WITH THE CONSTITUTION: LESSONS FROM THE INCIDENCE OF XENOPHOBIC VIOLENCE

Bringing this Constitutional provision into play makes it especially clear why, with the recent outbreak of xenophobic violence in South Africa, the re-emergence of the debate on the role and function of the intelligence services gained considerable significance.

Let me explain by way of the following question: If we regard the intelligence services as structures that promote an environment in which every South African can be free from fear and want, is it correct to suggest that the National Intelligence Agency (NIA) and its associated structures should be expected to report only on manifest threats to security?

If we are striving for intelligence services that are truly in line with our Constitution, it would certainly be more appropriate to aim for structures that are able to anticipate and interpret intensifying problems, perhaps not directly related to security, but with the potential to become threats to the security of our communities and our country. The underlying causes of the recent xenophobic attacks are prime examples of such potential threats that manifested before they were detected.

The same applies to many other social problems in our poorer communities, which, through their susceptibility to downstream ills like substance and sexual abuse and petty crime, often offer fertile soil for security-threatening organised crime, such as gang-related activities and trafficking in illegal goods and people. However, I want to make the following clear: the impoverished nature of these communities cannot be used as a basis to claim that they can all of a sudden fall into committing crime en masse, for lack of any intelligence to the contrary.

We therefore cannot place ourselves in the position that the Minister is reported to have done subsequent to the outbreak of the xenophobic attacks, by stating that 'much of what subsequently happened has been extremely spontaneous and aimed particularly at looting people's shacks and shops'. Such a statement must be qualified by admitting to the apparent deficiencies in the gathering and reporting of the intelligence upon which it was based.

We cannot place ourselves in such a position, because it would clearly go against the Constitutional provisions underpinning the establishment and operation of our intelligence structures. It would also entrench an intelligence regime that acts far less in favour of the poor than it does for other sections of our society.

I would like to draw attention to a final question that arose from the recent incidents of xenophobic violence. It concerns the government's perceived failure to take sufficient precautionary action on earlier intelligence reports on the violence and its perceived lack of preparedness to respond to the situation with the necessary urgency (Johwa 2008).

Certainly some believe that we should attribute these perceived failures by government to the so-called 'eternal dilemma' that it is incumbent upon political leaders to act upon intelligence reports and that the gatherers of the intelligence 'have virtually no control over that process or its decisions' (Johwa 2008).[1] On the other hand, others ascribe the problem to a 'lack of understanding or prioritisation of the role of the intelligence services and the problems of integrating the state intelligence structures in the larger body politic' (Hutton 2007).

The question is whether or not we should accept that the government took too long to respond because our intelligence services lack the necessary credibility amongst the government departments and within cabinet to have their reports taken seriously. As pointed out by a resident ISS researcher (Hutton 2007), this problem was highlighted in July 2007 by the Special Browse Mole Report, which indicated that government departments were using private intelligence services instead of the state agencies.

If this is not the case and the intelligence services are accepted as the equal, legitimate and well-integrated part of the state that they should be, then I would like to level a challenge to the Minister to make better use of that influence in government and in cabinet.

I would first like to repeat to the Minister what we have said in Parliament: that he needs to take note that at this stage that the Minister of Home Affairs and her Department may very well be the biggest threat to our National Security. Even the scandalous and deplorable acts of xenophobia we have witnessed and are still witnessing are in certain respects related to the enormous inefficiency and corruption so rife in that Department. We will never win the fight against crime, solve the problems caused by our porous borders and deal with the illegal drain on our social and welfare capability if we do not sort out the Department of Home Affairs.

If we want to progress to a point where our intelligence services can live up to the Constitutional provisions that underpin them, we have to work towards a situation in which our intelligence services can act as an early warning system. In the same vein, but perhaps on a lighter note, may I also suggest to the Minister that he put tabs on Eskom to ensure that we are not left in the dark again!

AN INTELLIGENCE SERVICE FOR A DEMOCRATIC SOCIETY

While the DA clearly supports the appropriateness of the earlier-cited Constitutional provision as a basis upon which to establish and operate any intelligence structure in South Africa, we are of the opinion that provisions should exist to improve our understanding of what is required from our intelligence structures. Such an addition should increase our understanding to the extent that when we say our intelligence services must promote the ability of South Africans to live as equals, it should not merely mean equal before the law. It should mean comprehensive equality in terms of the legitimacy that we should enjoy as South Africans in our communities, our broader society and as far as our intelligence structures are concerned.

Let me elaborate on this statement, by way of the earlier example of the position of poor communities whose lives and security were recently threatened by xenophobic violence. For the people who live in these communities to be vindicated as equal members of our society, they need to benefit from intelligence services that are relevant to their particular needs. So, if the social problems they face because of their impoverishment and their frustrations caused by lack of proper service delivery and unemployment threaten to manifest as direct threats to the security of their communities, then these problems ought to be monitored at exactly the same level as any other direct security threat to our country.

The security of all our communities is equally important. For service delivery from our intelligence structure to be more equal, it needs to be relevant to all our communities, rich and poor, to ensure that opportunities are not denied to those who live in poor areas because their communities are troubled by instability and violence.

In addition, people should also be afforded:

- equality, within reason, in terms of the information they may access and in terms of the benefits they may enjoy from having a national intelligence system;
- equality in terms of what they may aspire to as citizens of South Africa; and, finally,
- equality in terms of gaining access to opportunities within the intelligence domain.

The greatest problem for the country is that the intelligence services have been deflected from their collective role as protector of the nation to being the handmaiden of the ruling party and its government. This is the last thing that should happen, but we have seen numerous examples. The case of Project Avani and the allegations of spying on businessman Saki Macozoma are perfect examples of the sacrifice of the open society to service of the party.

This also holds true of the allegations that National Intelligence Director General, Manala Manzini, was present when Glen Agliotti was pressured into signing a statement that refuted an earlier testimony made to the Scorpions implicating suspended Police Commissioner Jacki Selebi in illegal activities. Allegations of this nature also surfaced in the wake of the expulsion of National Director of Public Prosecutions, Vusi Pikoli. This could only bring the entire intelligence system into disrepute.

We cannot have an intelligence system that is vulnerable to the procurement of surveillance information, the manipulation of officials and the placement of partisan officials by any political leader or bureaucrat, for sectional political or commercial interests. The regrettable policy of the government to redeploy senior personnel who make a mess of their responsibilities, laterally or even to higher office, is unfortunately also evident in the security structures, most worryingly perpetuating the culture of unaccountability, even in this most secret branch of state activity.

This situation is not only undemocratic, but it is also unfair to the many of our intelligence officers, from the Directors-General down to the lower ranks, who work hard to advance their careers in loyal, non-partisan service to their country; to those who aspire to join their ranks and to the people of South Africa who depend on their services.

If this situation can be addressed comprehensively, it is certain that the high numbers of qualified staff that leave our intelligence services will drop, and that service delivery to the people through the intelligence structures will improve.

THE PROTECTION OF INFORMATION BILL

The DA does not believe that the pursuit of an open society in South Africa is incompatible with the establishment and operation of an intelligence regime able to provide the services necessary to ensure the security and stability of our democracy. It is within this context that I would like to address certain of our concerns about the Protection of Information Bill currently before Parliament.

The DA supports the overall objectives of the Bill, which seek to strike a balance between the need to protect state information and the rights of the public to access information in the interests of open and transparent governance. We also recognise that the bill seeks to make provisions for the public to access state information within certain parameters while requiring that government meet specific criteria when classifying state information. However, there are a number of aspects of the bill that give cause for concern in terms of how they may curtail the space for public inquiry and debate.

The most important concern, in the DA's view, is the absence of a public interest caveat that would protect people who disclose classified information in the public interest from punitive measures before they have had an opportunity to prove their argument. Without such a caveat, the general public is placed at a great disadvantage while a disproportionate amount of power is placed in the hands of government. Without suitable caveats, checks and balances, as well as an independent body of appeals and review, the bill will fail to uphold the constitutional principles of an open and democratic society, despite its being based on guiding principles that purport to do that very thing.

We are making a number of recommendations in this regard through our participation in the Joint Standing Committee on Intelligence, some of which are quite technical and which I do not want to repeat here. But it is important for some of them to be raised for discussion today, and I would like to mention the following five points:

- Firstly, there must be a clearly described objective standard in the Bill that is used to determine when references to the national interest of the Republic will be invoked to keep information secret, and it is important that this standard should err on the side of public access rather than on the side of state secrecy.
- Secondly, as it stands, the Bill does not distinguish clearly enough between commercial information that relates to organs of state, private-sector commercial interests in which members of the state have personal interests, or public utilities like Eskom, in which the public have a vested interest. Such a distinction must be clearly delineated to preclude ambiguity or confusion, in the interests of promoting clean government.
- Thirdly, the Bill grants heads of state the power to classify information as well as to delegate that power to any senior official within their organ

of state. However, the realities of the South African political context mean that we have to take special measures of scrutiny. The ANC's cadre deployment policy, which forms part of their strategy to bring about the National Democratic Revolution, would regard the delegation of such classification powers as highly desirable. This process must be subject to some form of independent scrutiny in order to ensure that individuals are not delegated the power to classify information in a way that serves to further special interests.

- Fourthly, I want to re-emphasise that the Bill must contain a public interest caveat enabling whistleblowers, whether from within the organ of state or from the public, to disclose classified information in the public interest. Such a caveat must be narrowly and clearly defined. This is crucial if they are not to be deterred from revealing information that has been wrongfully classified, or information on internal corruption, fraud and mismanagement.
- Finally, there must be an independent body to process appeals and to review the implementation of the Bill at all levels of government. This independent body must be empowered in terms of legislation to do more than just make recommendations It must also be able to enforce compliance with the constitutional requirement of public access to information in terms of Section 32 of the Constitution. It must further ensure that any limitation of Section 32 meets the full requirements of the Bill of Rights limitation clause in Section 36 of the Constitution.

The Bill will not be in the public interest if it is signed into law without due consideration to these points of concern.

I have set out to outline the DA's vision for issues to ponder in the pursuit of an intelligence service that will ensure the continued consolidation of our democracy into a free and open society that offers true equality, freedom and opportunity for all South Africans. I hope that I have succeeded in my quest and that my contribution here today has given you some food for thought for the debate that is to follow.

NOTES

1 The full quote is attributed to an unidentified intelligence official and reads, "The eternal dilemma for all democratic civilian institutions is that they can place the best intelligence on

the table, but what is done with it is not up to them, and they have virtually no control over that process or its decisions" (cited in Johwa 2008).

REFERENCES

Constitution of the Republic of South Africa Act 108 of 1996, Cape Town: Republic of South Africa

Johwa, W. 2008. Intelligence agencies reported on xenophobia long before attacks, *Business Day* 29 May 2008 Available online at: http://www.businessday.co.za/articles/article.aspx?ID=BD4A775165 last accessed 3 September 2008

Hutton, L 2007. *Looking beneath the cloak: An analysis of Intelligence Governance in South Africa*, ISS Occasional Paper 154, Pretoria: Institute for Security Studies.

4 Who shall guard the guards?

Civilian operational oversight and the Inspector General of Intelligence

Imtiaz Fazel

BACKGROUND TO INTELLIGENCE OVERSIGHT

Intelligence services are essential components of the security architecture in democratic societies, where they support the formulation of government policy; gather intelligence to identify and counter threats to national security; support the prevention, investigation and prosecution of crime and support the activities of the armed forces. However, the intelligence industry's effective functioning is dependent upon an imperative for secrecy and special intrusive powers for procuring information. If not subject to safeguards, especially in an environment characterized by secrecy, these powers may be abused, manipulated or misdirected, possibly subverting the very purpose for which intelligence services have been established.

Given that intelligence is an essential component of the security architecture of all states, the case for intelligence services and for spying, in answer to the question: 'To spy or not to spy?' has long been made. However, an important caveat is that intelligence personnel remain accountable for their actions and operate within a constitutional framework. Consequently, the question: 'Who shall guard the guards?' has taken over in the debate on the original question.

'Who shall guard the guards?' means supervising the work of spies through effective observation and the governance of intelligence and security services. Securing the legality and accountability of intelligence services is therefore a crucial element of democratic governance.[1]

While overseeing intelligence includes executive supervision and control alongside the policy-making responsibilities of the executive, it broadly denotes an activity looser than management and control and may assume many forms or instruments. These usually include executive, legislative, judicial and civilian oversight mechanisms, each approaching oversight with varying colours in different areas of interest and different strategies for scrutiny, both before and after the event.

This paper will explore some of the history and development of intelligence oversight mechanisms in South Africa in general and explores in more detail the concept and experience of civilian oversight of intelligence in South Africa.

SOUTH AFRICA: HISTORICAL PERSPECTIVE, OVERSIGHT AND CONTROL

Earlier in South African history, while the nature of intelligence priorities and targets was of keen interest to the executive (including the State Security Council), other areas of control and oversight were largely absent from the governance of intelligence[2] prior to the democratic dispensation. During this era, operational effectiveness was closely managed, even demanded from the services, and administrative controls were 'nominally' strong.

Governance as a whole, however, was characterized by an absence of clearly-defined mandates and laws governing the use of intrusive powers, selective executive control, lenient judicial control and a lack of proper coordination mechanisms, bedevilling the intelligence services with fierce competition for political influence and material resources. Control systems within the intelligence community evolved largely from practice and although many were documented, these were vague and instructive in nature, designed to secure performance effectiveness rather than the responsible use of the invasive or coercive powers of the security apparatus.

The intelligence services' use of secret funding to promote the activities of the former government and to fund operations against the opponents

of apartheid is well documented, although the extent of this may forever remain a mystery. The use of legislated secret funding instruments effectively circumvented organizational administrative control. Although Secret Service Evaluation Committees were deployed after 1991 to oversee the administration of covert operations, the opaque culture of the intelligence sector and the leniency of those charged with overseeing them rendered these mechanisms inadequate. The financial auditing by the Auditor-General of Secret Services, upon the insistence of parliament pursuant to the Information Scandal in 1979, was limited for long periods. It was also somewhat farcical in parts and made only a partial recovery after the adoption of the Auditor-General Act of 1989. The regulation of communications interceptions through the introduction of the Interception and Monitoring Prohibition Act, 1992 (Act 127 of 1992) was one of the few encouraging elements of the governance of the intelligence sector at the time.

Intelligence activities during this era were characterized by counter-intelligence actions against civil society, disinformation to promote party and sectarian political interests, suppression of the liberation movements and the liberal use of intrusive powers and the consequent gross human rights violations. It is of importance here that these unlawful activities and morally questionable practices occurred in an environment beset by a lack of proper control and oversight, where the end justified the means, leaving room for executive recourse to the principle of plausible denial.

THE NEW DISPENSATION FOR INTELLIGENCE AND OVERSIGHT

Intelligence reform in South Africa was a consequence of constitutional reform brought about by the new political dispensation. The transformation of the security architecture was informed by a different strategic security environment and the broader democratic transformation in society.

In recognizing its important role in South Africa's security architecture, the Constitution provides for the establishment of intelligence services. It does so within the context of a series of governing principles and other safeguards designed to ensure that the intelligence and security services and their members pursue national security in compliance with the law, act in accordance with the Constitution, disregard manifestly illegal orders and steer away from political

party prejudice and interests. The Constitution also provides that intelligence services may be established only in terms of national legislation,[3] must function under the control and direction of the President or designated Minister and parliamentary and civilian oversight (Chapter 11 Section 198a).

In formulating clear parameters and limits for intelligence operations, the constitution prescribes that national legislation must regulate the objects, powers and functions of the Services, including the intelligence arms of the police and defence. These Constitutional provisions are given expression by a series of legislative interventions that establishes the parameters for intelligence and law enforcement operations within the security sector.[4]

This legal framework provides for clearly defined mandates, powers and functions, mechanisms for coordination, oversight, control and accountability, which together with the White Paper on Intelligence provide the overall framework for an understanding of the philosophy and role of intelligence in a democratic South Africa. The conceptual framework for the oversight of intelligence is therefore anchored in the rule of law and the constitutional protection of human rights. In South Africa, this is the shared responsibility of the executive, the legislature, the judiciary and the civilian Inspector General. The challenges for intelligence oversight consequently lie in overseeing the efficacy, legality and probity of the intelligence services and remaining on the watchout for wrongdoing in the practice of intelligence and counter-intelligence within this framework.

CIVILIAN OVERSIGHT AND THE ROLE AND FUNCTION OF THE INSPECTOR-GENERAL

Turning to civilian oversight, Chapter 11, Section 210 (b) of the Constitution makes provision for intelligence oversight through the appointment of an Inspector-General[5] to carry out civilian oversight of the Intelligence Services in South Africa. The Inspector-General of Intelligence is appointed in terms of the Intelligence Services Oversight Act (Act 40 of 1994) (the Act) and is required to have knowledge of intelligence. The Inspector-General may be removed by the President alone, pursuant to investigation by Parliament and only on properly defined grounds.

The concept of civilian oversight implies that the Inspector-General is not a member of the intelligence services and is independent and reports on

his/her functions to Parliament through the Joint Standing Committee on Intelligence (JSCI). The Inspector-General is also responsible and accountable for his/her office administration and budget to the executive through the Minister for Intelligence Services. The accountability regime of the Inspector-General is therefore two-fold: line or functional accountability to parliament and an administrative accountability towards the Minister for Intelligence Services. Critical to effective oversight is the fact that the Inspector-General has access to all the information required for carrying out oversight work. South Africa, in adopting this form of oversight, became part of a select group of countries that have introduced similar provisions for operational intelligence oversight.

SCOPE AND SPAN OF OVERSIGHT

The Office of the Inspector-General (OIGI) is the capacity established to support the execution of the role and function of the Inspector-General and supports the latter's responsibility for overseeing the South African intelligence establishment. These designated Services include the domestic intelligence-gathering arm, the National Intelligence Agency (NIA), the foreign intelligence-gathering arm, the South African Secret Service (SASS), the Intelligence Division of the South African Defence Force (DI) and the Crime Intelligence Division of the South African Police Service (SAPS-CI).[6]

Within the parameters of the intelligence community, the Inspector-General is compelled to perform a broad range of oversight activities designed to provide assurance and comfort on the legality and efficacy of intelligence activities. The emphasis is on monitoring and reviewing the intelligence and counter-intelligence activities of the intelligence services.

Although other important incidental oversight functions, such as the evaluation of intelligence failures, are relevant, core oversight is generally distinguished by four broad themes, each containing its own elements. These include oversight directed at:

- the lawful conduct of the services;
- the effective performance of intelligence work;
- providing assurance on the operational conduct of the services to the executive and people of South Africa through a certificate; and

- performing the role of ombudsperson in investigating the complaints of members of the services and the public on the conduct of intelligence.

The core activities of the Inspector-General that give expression to core oversight are embodied in pro- and re-active monitoring and review activities.

SECURING COMPLIANCE WITH THE RULE OF LAW: THE INTELLIGENCE BUSINESS AS A REGULATED INDUSTRY

Essential to the understanding of the control and oversight of intelligence is an appreciation of the principle that the intelligence business is a 'Regulated Industry'. This implies that intelligence activities are conducted within a control or regulatory framework of checks and balances. These encompass, at one end of the continuum, the Constitution, primary legislation and ministerial directives, with standard operating procedures at the other end.

The philosophy underlying the conduct of intelligence is therefore one of laying down proper criteria for target identification and the utilisation of intrusive measures. The system of checks and balances requires procedures for authorization and administration; procedures for control and accountability; clear delegation of responsibility and associated accountability and the maintenance of proper records and audit trails. Careful operational planning, together with internal and external regulatory compliance are therefore essential prerequisites to operational activity.[7] The challenge is to ensure that the regulatory framework is carefully designed and developed so that intelligence objectives are realized in an effective manner and within the framework of the law and due process.

Within the intelligence business, oversight finds particular expression in monitoring the compliance of intelligence and counter-intelligence activities with this regulatory framework for intelligence operations. This framework is the basis for oversight and control and sets the parameters for professional, legitimate and lawful intelligence conduct, providing intelligence officers with certainty and confidence in their actions.

Evaluation of compliance with the regulatory framework is a labour-intensive process and is dependent on an understanding of intelligence practice in general, the law, and the principles of intelligence regulation. Our formative initiatives have been to secure from the services a more effective and comprehensive internal regulatory framework governing intelligence activities, primarily

at the operational and procedural levels of activity, thereby establishing the basis for lawful and efficient operational conduct.

REVIEWING THE EFFECTIVE AND EFFICIENT PERFORMANCE OF INTELLIGENCE AND COUNTER-INTELLIGENCE ACTIVITIES

Rules prevent abuse of intelligence resources but they also secure operational effectiveness on the tactical or business process levels. By far the most complex aspect of the performance review function of the Inspector-General is the evaluation of performance at the operational and strategic levels.

At the operational level, performance evaluation mirrors the intelligence process or cycle, and seeks to assess the quality of and strategies for intelligence collection, quality and sophistication of intelligence analysis, and, finally, the timeliness of dissemination of sound policy advice, warning or other intelligence process outcome. This is conducted largely by a sample approach. These initiatives are conducted at the macro-organizational level and in relation to specific operations or priorities within the intelligence services.

At the strategic level, the primary objective of the performance evaluation process includes an assessment of the manner in which the services interpret and operationalise their respective statutory mandates and consequently develop operational priorities and focus areas. Oversight assessments at this level are also directed at reporting systems/product flow, the coordination and sharing of intelligence within the intelligence community, highlighting performance weakness that may give rise to performance gaps or intelligence failures and the effectiveness of the intelligence landscape as a whole.

The statutory requirement for the heads of the Intelligence Services to report significant intelligence failures occurring under their watch to the Inspector-General, albeit after the event, provides a platform for the assessment of performance in critical areas of operation together with the development of corrective measures.

Performance evaluation of the activities of intelligence services is knowledge-intensive, and is an arduous challenge for intelligence oversight practitioners. It is heavily dependent on the appropriate expertise in intelligence practice generally and on an appreciation of domestic, foreign, military and crime intelligence disciplines in particular.

PROVIDING ASSURANCE TO THE GOVERNMENT AND THE PEOPLE OF SOUTH AFRICA

An innovative element of the South African intelligence oversight system is the annual certificate from the Inspector-General. The certification process is designed to provide assurance on intelligence conduct to the government and the people of South Africa, represented respectively by the Ministers responsible for intelligence and the Parliamentary JSCI.

The certificate conveys a dual assurance and serves a dual purpose. In the first instance, it serves as a medium for the Inspector-General to express satisfaction with the fair presentation of the annual reports of the intelligence services on their activities. In the second instance, it is a medium for the expression of an opinion as to whether anything done by a service is unlawful or involves an unreasonable or unnecessary exercise by that service of any of its powers during the course of its activities during that reporting period.

The certificate provides the Ministers responsible for the designated intelligence services and the JSCI with a level of assurance on the reasonableness of reports presented to them and of the lawfulness of intelligence activities, as part of executive control and Parliamentary oversight of the intelligence sector respectively.

The certificate of the Inspector-General is not a guarantee, but provides reasonable as opposed to absolute assurance that the intelligence services give reasoned accounts of the performance of their activities (through their reports) and operate within the framework of the law and due process. The certificate of the Inspector-General, with the reports of the auditor-general and the judge on lawful interceptions, together provide assurance on the operational and financial activities of the designated intelligence services in South Africa.

THE INSPECTOR-GENERAL AS THE OMBUDSMAN

An important element of the oversight process that may highlight abuse of the intelligence apparatus is the complaints responsibility of the Inspector-General, who is required to receive and investigate complaints from members of the public and of the intelligence community. Complaints range from corruption, through alleged maladministration, and abuse of power, to transgressions of the Constitution, laws and policies in relation to members of the Services. Moreover

should the JSCI receive complaints form the public, these may be referred to the Inspector-General for investigation.

The nature of complaints received and the complaints arena as a whole during the recent past has focused the Inspector-General's attention on the need for a deeper culture of due process in the management of human resource matters within some of the intelligence services. This is not to forget the promotion of the right of members to disobey manifestly illegal instructions should they be given. Poor management by secret agents, although isolated, has also given rise to recommendations to improve the process by which agents are contracted and managed.

Complaints containing allegations of all forms of misconduct within the services are given priority and treated very seriously in the office of the Inspector-General. Where appropriate, adverse findings are made and harsh remedies recommended. Allegations are often in the public domain, without the tabling of a formal complaint against the intelligence services, particularly the NIA, given its domestic mandate. Many of these allegations are subsequently found to be spurious, thereby undermining the credibility of the Services. Both formal complaints and allegations of misconduct on the part of the intelligence services made in the public domain are investigated without fear or favour.

APPROACH TO OVERSIGHT AND VALUE SYSTEM

Turning to more subtle challenges, intelligence oversight contributes to the democratic accountability of the intelligence community and the safeguarding of South Africans' fundamental rights and freedom. Its execution, however, can be realized only through unlimited access to information held within and outside of services. Although denial of access to information during an investigation by the office of the Inspector-General is a punishable offence, securing the cooperation of the services requires a finer approach than recourse to the courts.

In this regard confidence building and relationships of trust are critical ingredients in the relationship between oversight and intelligence services. The oversight approach is to constructively contribute and add value to the proper performance of the activities of the services. This is expressed mainly in the exchange of information, developing solutions and providing sound advice and reports on intelligence service activities. A faultfinding approach (other

than observance with the rule of law) to intelligence oversight has been widely viewed as ineffective.

'Plaudits' and commendations for good work used sparingly in conjunction with 'Audits' build confidence, as do initiatives (justifiably launched) that protect the integrity of the services, when it is unjustifiably questioned. These confidence-building measures create trust and facilitate candidness and openness in the oversight process. The principle of 'no surprise', secured through the advance notification of heads of services before conducting oversight activities is equally important in the intelligence environment and is now a statutory requirement in most intelligence oversight systems, including that in South Africa.

Pursuing the correct approach toward constructive engagement with the intelligence services requires a careful balance between independence and partnership, as well as securing the power to monitor free from any influence and restriction whatsoever, while remaining internal to government but external to and independent of the intelligence services.

Our expectations of intelligence practice are precise and whilst appreciating the important role of intelligence services within the security architecture, we are of the firm view that while they support the priorities of the government of the day, they serve the people of South Africa and do so within the broader framework of the principles of the Constitution. Our insistence on the principles of proportionality, reasonableness and necessity are equally clear and demand the use of the least restrictive alternative or the deployment of intrusive powers in proportion to the magnitude of a legitimate threat, weighed against the adverse impact on human rights.

The nature of our relationship with the intelligence services is characterized by an increasing willingness to cooperate with oversight requirements and dynamic exchanges of information. Although exceptions do exist, these relationships are in the developmental phases and much more needs to be done before they reach maturity or their full potential to secure a more robust oversight system.

CONCLUSION

As professional oversight practitioners, our value system is anchored in our Constitutional principles and the need to uphold those principles by means of

conducting activities with integrity, independence and impartiality and without fear, favour or bias.

Our role is to promote accountability and operational effectiveness within the intelligence services through constructive oversight and to provide assurance to the Government and people of South Africa that the intelligence services operate within the framework of the rule of law and due process, and act with probity and respect for human rights.

Recent investigations conducted by the office have highlighted a number of abuses and malpractices in sections of the intelligence community, which has severely tested our oversight capacity and ability to access information. While we believe that we have acquitted ourselves well under very difficult circumstances, the challenges inherent in pioneering intelligence oversight in South Africa were amplified and many valuable lessons were drawn. In the process, the cardinal requirement upon which the democratic functioning of intelligence hinges, 'the rule of law and due process', was re-established, and the notion of bending the rules was banished from the philosophy of intelligence conduct, while the intelligence mandate was re-examined and tightened up in certain areas. Operational procedures for the use of intrusive measures were refined, legislation and policies in general were strengthened and a multitude of initiatives were launched in the civilian intelligence community to enhance professionalism and awareness of the need for legality in the conduct of intelligence operations.

Our own inputs in developing the intelligence industry into a regulated business so as to secure lawful and effective intelligence conduct have been significant, and our efforts at uncovering wrongdoing has been significantly enhanced. The Intelligence Community is a vast one with many oversight challenges. Our growth continues, along with our increasing scope and span of oversight. The development of oversight approaches and techniques has likewise been dynamic and ongoing. After the previous lengthy failure to get off the ground, civilian oversight of intelligence in South Africa has developed substantially in four short years.

In answering the question: 'To spy or not to spy?' Caparini (2002) argues that security is one value that must compete with other values and that a balance should be struck between the security of the state and individual freedoms. She holds that the quest for intelligence control revolves around the objective of achieving effective security intelligence within a democratic

framework. Spying is therefore permissible only within strictly defined parameters, with intelligence oversight acting as the bridging activity connecting the seemingly divergent worlds of secrecy and transparency within such a democratic framework.

NOTES

1 Although Intelligence Oversight systems are known to have functioned earlier in Germany and the USA and in the Netherlands since the 1950's, the exposure of abuses in the intelligence community of the USA during the 1970s focused attention on the democratic governance of intelligence and served as a catalyst for intelligence reform across the globe. Intelligence reform was further spurred on in a number of countries during the 1980s and 1990's by a combination of constitutional reform (South Africa and Canada), transition from military to civilian rule (Argentina) and legal challenges to intelligence systems (United Kingdom) (Leigh I, More Closely Watching the Spies: Three Decades of Experiences in Who's Watching the Spies, Born, Johnson & Leigh, pp3-4)). Intelligence Reform and Oversight continue to occupy the agenda in Europe and more recently in Africa as part of broader democratic reforms on the continent.

2 The Intelligence Community prior to the new dispensation included the intelligence division of the South African Police Services, the Security Branch (SB); the Intelligence Division of the South African Defence Force, Military Intelligence (MI) and the civilian Intelligence arm, the National Intelligence Service (NIS) which replaced the Bureau of State Security (BOSS) in 1979. Other line departments at a national level are also known to have engaged in secret operations/intelligence gathering in support of their line functions or for providing intelligence to the State Security Council.

3 This requirement excludes the intelligence divisions of the South African Police Services and the South African National Defence Force.

4 These constitutional provisions are given expression by primary legislation that include the Defence Act, the South African Police Service Act, the National Strategic Intelligence Act and Intelligence Services Act which regulate the objects, powers and functions of the Security Services together with interceptions and other legislation that specifically regulate and establish the parameters for intelligence and law enforcement operations within the security sector.

5 The President appoints the Inspector-General after a process of nomination by the Joint Standing Committee on Intelligence (JSCI) and approval thereof by at least two-thirds of the members of Parliament.

6 The NIA and the SASS are referred to as civilian intelligence Services and are accountable to the Minister for Intelligence Services. The DI and SAPS-CI fall under the executive control of the Minister of Defence and the Minister for Safety and Security respectively.

7 Whilst the development of formal checks and balances is essential in ensuring intelligence conduct within the rule of law, these are dependent on sound personal, ethical and professional conduct and value systems within the intelligence services.

REFERENCES

Constitution of the Republic of South Africa Act 108 of 1996, Cape Town: Republic of South Africa.

Caparini, M. *Challenges for control and oversight of intelligence services in a liberal democracy.* Paper presented at a workshop held in Geneva 3 – 5 October 2002, Geneva Centre for the Democratic Control of the Armed Forces (DCAF).

5 Are our intelligence services really that bad?

Barry Gilder[1]

There is something amiss with the public discourse on intelligence and democracy in the new South Africa. For one thing, there is very little intelligent discourse on this topic. Our thanks must go to ISS for organising this series of seminars.

For another thing, such discourse as there is, is listing to starboard. In other words, the discourse is leaning to the right in three main respects. Firstly, there is the assumption that the intelligence services of the democratic South Africa are no less repressive and invasive than those of the apartheid era. Everyone seems to think our intelligence services are tapping their phones, bugging their bedrooms, following them around and opening their mail. Our services are subjected, directly or in the media, to a steady stream of complaints from individuals and organisations who are convinced they are under surveillance. This is simply not true. It is not true because it's not practical. And it's not true because it's not allowed.

There is one essential difference between the apartheid intelligence services and those of the new South Africa. The apartheid services protected a minority against the majority. Our democratic services are designed to protect the majority against a minority, a minority engaged in crime, who subvert our democracy

and, inter alia, undermine our international political and economic relations. I will come back to this.

Secondly, there is the assumption that all governments are bad; therefore our government must be bad. If you believe the public discourse, our democratic government is corrupt and self-seeking, cares nothing for the plight of its people, goes to extreme lengths to hide its activities from the public and sees the people as its enemy, all of which makes it not that different from its apartheid predecessor.

This is also simply not true. This is the government that designed one of the best constitutions in the world, that repealed reams of apartheid legislation, that has grown our economy exponentially, that made equity in the workplace obligatory, that has begun to break the minority hold on our economy, that has put billions of rands into providing a cushion for the worst-off of our people, that has dramatically increased access to clean water, to electricity, to education and to health care, that has made the proactive resolution of conflict on our continent and globally one of the key planks of its foreign policy.

I was a member of our democratic government for 12 years. I sat in many forums of government through those years, including cabinet meetings and makgotla. I can attest that the collective mind of the leadership of our government is constantly focused on creating a better life for all South Africa's people and on overcoming the incessant obstacles to its endeavours.

And there's the thing – the incessant obstacles. It constantly perturbs me that many public commentators do not seem to realise or understand exactly how difficult it has been to govern this country and to turn apartheid around. There seems to be a subconscious belief that the ANC's election to govern this country in 1994 was no different from Labour taking over from the Tories in the UK, or the Democrats taking over from the Republicans in the USA.

The reality has been that we have had to govern this country and simultaneously turn it around with a public service that, in the main, has not only been uncommitted to the new government and its programmes, but in many cases has obstructed it. We have had to contend with resistance from the private sector, from foreign interests who do not quite like our progressive foreign and economic policies, from apartheid die-hards who seek constantly to turn back the hands of time, and – most frustratingly – from a range of crooks and criminals who found the lifting of the cloak of repression in 1994 most suitable to their constant and ever more clever schemes to rip off our young democracy,

even, some would argue, turning to crime, particularly organised crime, as a form of resistance to ANC rule. Indeed, there are those in government who are corrupt, who are self-seeking, who care nothing for the plight of the people, who see the people as the enemy. But all these vices are an obstacle to democratic governance, not the nature of governance.

The third assumption in the starboard-listing discourse about intelligence in our South African democracy is particularly irksome – that the leadership of our intelligence services are somehow not aware of the constitutional and legislative imperatives that govern them. Many of the current leaders of our intelligence services were involved, even prior to 1994, in designing our democratic intelligence dispensation, drafting the relevant sections of the Constitution, composing the White Paper on Intelligence, and framing the founding legislation, including intelligence oversight mechanisms that surpass those of many much older and supposedly wiser democracies.

More importantly, it fell to them to put flesh onto the constitutional and legislative framework that they helped shape. This, to put it mildly, was not easy. We did not win our freedom by rolling into Pretoria on the top of Soviet tanks with pretty women throwing flowers at us. We did not line up all the apartheid securocrats against a wall and shoot them. We had to build our new intelligence dispensation by amalgamating all the pre-1994 intelligence services, including the apartheid service, the Bantustan services and those of the liberation movements. The intelligence officers of the liberation movements were in the minority, with no experience of government.

Thus, we had to fight for every inch of constitutionality, legality, openness and transparency. We had to fight to change a culture of extreme authoritarianism, of excessive secrecy, racism, and sexism. We had to fight to reach agreement with our old enemies as to who were the new enemies of a democratic South Africa and what methods we could legitimately use against them. We had to do this in the face of all the general obstacles that the new government had to face in imposing its transformatory programme on the new South Africa. And we had to do this in the face of specific obstacles that were incessantly thrown in our path: disgruntled apartheid-era intelligence officers who made it as difficult as possible for us to work; a burgeoning private security and intelligence industry that did its best to usurp us and spy on us; information-peddlers who planted juicy but false information on us to divert us from the real issues; renegade officers who leaked (often false) information to the media;

foreign intelligence services that sought energetically to infiltrate us and influence us to see the world as they saw it; and a public (and some in other arms of government) who saw intelligence in a post-apartheid and cold-war world either as an anachronism, or as an old-style repressive organ of state, the enemy of the people and of democracy. Against these, and many other obstacles, the Constitution and the law were our weapons, our solace, our lodestar.

What can we do, then, to set this starboard-listing discourse on intelligence and democracy in South Africa back on an even keel? The first thing, I imagine, is to understand what intelligence really is. First and foremost, intelligence is spying. It is finding out the secrets that others don't want you to know. But, importantly, and most arduously, it is about making intelligent sense of those secrets. That's why it's called 'intelligence'. It's about contextualising those secrets into the body of things that are already known, that are not necessarily secret, in order to develop as profound an understanding of an issue as possible. And, most profoundly, it is about knowing what it is that you don't know – in other words, knowing when to collect secrets in order to complement the information that is readily available from other sources.

Intelligence does this to give government an edge in dealing with the obstacles to good governance and in ensuring that South Africa can hold its own in relating to an increasingly complex world in pursuit of its legitimate programmes. To achieve this with any value, intelligence needs to give government time to prepare any actions to counter obstacles or to give it an advantage in its dealings with the outside world. Intelligence therefore needs to be predictive not 'post-dictive'. It provides little of value if it says: 'The Zimbabwean army sent troops across our border last night'. It should be able to say: 'The Zimbabwean army is planning to send troops across our border tomorrow night'.

This predictive nature of intelligence is its greatest challenge. If you want to predict, you must have a profound understanding of political, economic, social, criminal and international dynamics in order to anticipate from where a threat may emerge and you must know where you need to deploy your resources to better understand and pre-empt that threat.

I said, 'Intelligence is spying'. I said that to be provocative. The reality is that spying is only a small part of the intelligence effort. The far greater effort lies in developing the contextual understanding of the dynamics from which threats emerge and, as I've said, determining with precision exactly where you deploy your spying tool when necessary. This is done by keeping ears to the ground,

through interacting with communities and their organisations, partnering with other government departments, with research institutions and academia, through reading and researching.

Out of this reality emerges a major theme in the current debate about intelligence and democracy in South Africa. Many seem to think that 'ears to the ground' means 'bugging devices in the bedroom'. For instance, many argue that monitoring any possible threat to stability emerging from the leadership race in the ruling party constitutes spying on a political party or, to bandy an over-bandied term, 'political intelligence'. Monitoring is not spying. Understanding the possible impact of contestation within and between political parties is not spying. The laws and internal regulations governing the intelligence services in fact disallow spying, except in clearly defined circumstances, notwithstanding relatively recent breaches of those prescripts (breaches that were, in fact, discovered and dealt with by the oversight mechanisms of the intelligence dispensation).

Use of the spying tool in the intelligence toolbox becomes legitimate if the adversary against whom it is used is a legitimately determined adversary. This, as far as I am concerned, is the crux of the matter. I have purposefully used the term 'adversary' as a less value-laden term than 'enemy', although the same broad conceptual strokes apply to 'adversary' as they do to 'enemy' in times of war. If, as a nation, we could agree on who South Africa's adversaries are, then there would be little need for acrimony in the debate about intelligence and democracy. But South Africa is a politically and socially diverse country. One person's adversary may be another's friend. That, I surmise, is true in all democracies. It is certainly not practical to hold a national referendum to get consensus on an official list of South Africa's adversaries. The way of democracy is that the government of the day gets to decide who our adversaries are.

Part of the problem is that anyone who thinks they are of interest to the intelligence services (or that they ought to be of interest) believes that they are an adversary. But the distinction I have drawn is important. Being of interest to the intelligence services and being a target for spying is not the same thing. The possible impact of intra- or inter-party contestation may be of interest to the intelligence services as the possible source of violence, but that does not make the parties concerned adversaries and therefore the targets of spying.

Let me outline the process by which the South African government and its intelligence services determine their adversaries. Every year, the intelligence

community prepares a national intelligence estimate. This is a comprehensive document that draws on the intelligence from the services themselves, as well as from other government departments, open sources and research, in which the intelligence community outlines the key issues it believes are security concerns on the domestic and international terrains for the year under review. This is presented to and discussed by Cabinet. The estimate concludes by recommending intelligence priorities for the coming year. These, too, are discussed and finally approved by Cabinet. Once so approved, these priorities become the official guide for the intelligence services as to what they should and should not focus on. Flowing from these priorities, the intelligence services draw up their operational plans for the year, which go into more detail about how they are going to attend to these priorities, who their targets (or adversaries) are going to be and what intelligence methods should be employed on them. These plans also have to be approved, and all operations carried out by the services have to flow from them.

I can assure you that if I were allowed to suspend briefly my oath of secrecy and present to you today an example of such priorities and plans, there would be little if any disagreement on them. What I can broadly outline is that our adversaries are mainly obvious ones – criminal syndicates, organisations seeking the unconstitutional overthrow of democracy, foreign intelligence services, organisations that perpetrate violence, and so on. On the international front they would include parties to conflict in conflict zones on the continent, foreign governments who are in competition with us on international terrain, or transnational crime syndicates.

The simple truth is that we use the techniques of spying against adversaries who, by their very nature, operate in secret. If they did not think they ought to operate in secret, we would not feel we should spy on them.

Which brings me to another important fulcrum on which the debate about intelligence and democracy sways – the balance between secrecy and transparency. In some senses I think this is a false debate. Intelligence services, to be effective, have to operate in secrecy. There are many, especially in the media, who seem convinced that the reason for secrecy on the part of the intelligence services is to hide their nefarious deeds from the public. The real purpose of secrecy in the intelligence services is to hide their activities from their adversaries. If their adversaries knew, inter alia, how the intelligence services worked, who their operatives were, their methods and what they know about their

adversaries, it would undermine the ability of the services to deal effectively with their adversaries. If the services were to be open about these things with the public they serve, they would, in fact, be open to their adversaries. The public is an innocent bystander, not the target of the need for secrecy.

The current media debate surrounding the draft Protection of Information Bill seems to me to miss this point. This legislation is not aimed at the public. It is aimed at protecting the integrity of certain state information from our adversaries, not from our people. Are we not yet enough of a nation to understand and accept this? Do we need a vicious and all-threatening enemy (such as so-called international terrorism for the big western powers) before we can agree what our national secrets should be? Do we think, in our new *laissez faire* world, that espionage against us is acceptable?

Do we have the balance between secrecy and transparency right? I believe that is a complex judgement call. The reality is that we have a remarkably transparent government and intelligence services. The existence, roles, functions, responsibilities, leadership, make-up, controls on and limitations of our intelligence services are public knowledge (although those noble educators of the public, the media, often fail to do the most basic homework before they write about our services). Our intelligence community has as open and proactive a communication strategy as is humanly possible. The services are subject to thorough oversight, from the Inspector General for Intelligence, Parliament, the Auditor General, the Public Protector, the Human Rights Commission and the courts.

Surely, we must allow our services the right and ability to protect knowledge about their methods, structures, capacities, personnel, or knowledge from their adversaries? For surely their adversaries are our adversaries, the nation's adversaries? At least, I believe, that is how it should be.

Surely (I can sense the question linger in the air) the power of secrecy is open to abuse? Indeed it is. But so is the right to privacy, which is indeed abused by the criminals, right-wing extremists, anti-democracy subversives and the espionage agents. But there is an important difference. The criminals, extremists, subversives and espionage agents are not subject to an Inspector General, a Parliamentary Committee, an Auditor General, a Public Protector and the Human Rights Commission. Ultimately they are accountable only to the country's security and judicial services. And to hold them accountable, our intelligence services must surely be allowed to operate against them in secret.

But I will come back briefly to the issue of abuse before I close. There is one concept about intelligence in a democracy that I have to debunk: the notion that intelligence is somehow neutral, removed from politics and policy. That simply is not and cannot be true.

To explain myself, let me give my very simple views on what democracy is. Political parties represent the collective views on governance of certain sections of the population. Before elections they seek to persuade the electorate that their views are best for them. The electorate decides through the ballot box which political party they want to govern them. The party that wins the elections earns the right to use the implements of governance to pursue the policies and promises they put before the electorate. The governing party wins the right to elect the President, select cabinet ministers, directors-general of government departments and the heads of the intelligence services. Surely, in doing so, they appoint people they believe are capable of understanding and driving the implementation of the policies and programmes for which they were elected.

So am I saying that the governing party gets to appoint party hacks to run the intelligence services and the services become weapons against the ruling party's adversaries? No. I am simply saying that the democratic process gives the ruling party the right to rule and to utilise the instruments of governance, including the intelligence services. Once elected, it does so as government, not as party. The party's adversaries do not automatically become the government's adversaries, but the ruling party does earn the right to determine, in the context of its policies and programmes, who the nation's adversaries are. But it does this in the context of the Constitution and the law, and in the name and under the watchful eye of Parliament, of the courts, of the Chapter 9 institutions and of the public as a whole. Again, it does so as government, not as party.

It has always intrigued me, when talking to intelligence counterparts from countries that experience a fairly regular change in ruling party, such as the UK, how their intelligence services prepare themselves for a possible change in governing party. They study the election manifestoes of the two main parties before the election and prepare two sets of strategic plans, one for each of the possible winning parties. After the election they simply present the relevant strategic plan to the winning party. As a young democracy, we have not yet reached that stage, but the principles are the same. The intelligence services, like other government departments, serve the government of the day and are obliged to carry out its policies and programmes.

If the renaissance of Africa, the building of democracy and the ending of conflict on the continent are the policies of the ruling party, then the intelligence services are obliged to conduct intelligence against warring factions on the continent and against regional and international players who influence the conflicts in which they are engaged. If a new ruling party were to be elected, whose policy was to focus attention, not on international and continental matters, but on domestic issues, then the intelligence services would be obliged to change their focus appropriately. It's as simple as that. This is how democracy works.

Intelligence services are thus not neutral and above politics and policy. What they are, and must be, though, is professional. Professionalism means being able to tell the difference between party and government, between party adversaries and national adversaries. It means being able to give the government of the day objective, reliable, timely information based on government's policy and programmatic information needs – being able, in the famous phrase, to tell truth to power.

Which brings me back to the issue of abuse. It is true that the power given to the intelligence services is open to abuse. But it is also true of the private sector, which more often than not abuses the freedom that free enterprise gives them. It is true of the media who abuse the power given them by freedom of the press. It is sometimes true of other arms of the state. It is certainly true, as I have said, of many private citizens who abuse the right to privacy to do bad things in the privacy of their homes, offices and the streets.

Only two things mitigate the abuse of power – integrity and accountability. Integrity is the more powerful. If the individuals charged with the exercise of power have the strength of character to understand and comply with the legality and professionalism required of them, then there is little cause for concern. If not, then the systems and processes of accountability must catch up with them. This is precisely what happened in the infamous e-mail saga that afflicted the National Intelligence Agency a few years ago. My 12 years' experience in South Africa's intelligence community tells me that, in the main, our intelligence services are not short of integrity. What they are certainly not short of is a system of accountability. I think, contrary to popular belief, we are safe.

To sum up and conclude I would like to highlight some key points. This series of seminars is entitled 'Intelligence and Democracy in South Africa'. It is not about intelligence and democracy in general. What is special about South Africa in this debate?

The historically unavoidable project of a post-apartheid South African government must be to redress the imbalances of our past. It does this on behalf of the vast majority of our people, who were victims of these imbalances and who elected the government to do precisely this. This involves a massive transformatory programme that must touch on every aspect of South African life and on South Africa's place on the global stage. But it must carry out this transformatory programme in the face of a wide range of obstacles – resistance to change, opposition to and sabotage of change, competing selfish interests in society, a reluctant and unsuited public service, competing and inimical foreign interest, and so on. Out of these obstacles arises a range of adversaries to the transformatory project.

The intelligence services are a tool of the government for tackling these adversaries and overcoming these obstacles. They are not the only tool, but they are a highly specialised one that has been assigned the very special power of secrecy. This power is and must be used against those adversaries who operate in secret and whose activities are illegal. This power is used on behalf of and in the name of the vast majority of South Africa's people.

Intelligence in a democratic South Africa must therefore be allowed to cast off the shackles of perception that it is a repressive organ of state used against the people, that it spies indiscriminately on anybody who steps out of the 'party line', that it is an anachronism in a democracy, and that it operates in secret only to cover up its misdemeanours. There is nothing to support these perceptions but the misdemeanours of some, the mischief of others, and the misconceptions of many.

I would go so far as to argue – at the risk of being accused of facile sloganeering – that our intelligence services must be allowed to become 'the people's intelligence services', serving and defending our democratic transformatory programme on behalf of the people. Just as we call upon our communities to support our police services in the fight against crime, we should be able to call on our communities to be our eyes and ears in the fight for a better life for all and against those who would stand in the way of this noble project.

NOTES

1 Barry Gilder retired from the South African intelligence community in 2007. At the time he was the coordinator for intelligence at the National Intelligence Coordinating Committee.

6 To spy or not to spy?

Intelligence in a democratic South Africa

Sam Sole[1]

I want to put forward a proposition: being a spy means never having to say you're sorry. There is a great deal of comment that says, 'You never hear when we get it right - you only hear when we get it wrong'. This obscures the basic point I want to make. Secrecy generally reduces accountability, promotes abuse and hides incompetence. Secrecy distracts us from answering the question: What are intelligence agencies for? How well do they carry out what they do? And what degree of secrecy do they actually need if they are to function properly?

Let's take one view from the inside, to quote former Central Intelligence Agency counter-intelligence officer Aldrich Ames, who is serving a life sentence for passing on secrets to the Soviet Union. He said espionage was: 'A self-serving sham carried out by careerist bureaucrats who managed to deceive policy-makers and the public about the necessity and value of their work' (in Earley 1997)

I believe that spying, like policing, prosecuting, and even journalism, can be a noble and honourable profession. But to what extent does this apply in reality? To what extent are good intentions matched by positive outcomes?

Let's take another view, this time from *New York Times* Pulitzer Prize winner Tim Weiner's book *Legacy of ashes: The history of the CIA*. Here's an extract from the review of the book in *The Economist* (2007):

> The CIA failed to warn the White House of the first Soviet atom bomb (1949), the Chinese invasion of South Korea (1950), anti-Soviet risings in East Germany (1953) and Hungary (1956), the dispatch of Soviet missiles to Cuba (1962), the Arab-Israeli war of 1967 and Saddam Hussein's invasion of Kuwait in 1990. It overplayed Soviet military capacities in the 1950s, then underplayed them before overplaying them again in the 1970s.
>
> The record of covert action is little better. In Japan, France and Italy the CIA sought to protect democracy by buying elections. It sponsored coups in Guatemala, Iran, Syria and Iraq, where a Ba'ath Party leader boasted in 1963, "We came to power on an American train". When an invasion of Cuba masterminded by the agency failed, it plotted to kill Fidel Castro. In ascending order of bloodshed, it took a hand in military coups in South Vietnam, Chile and Indonesia.
>
> Was such skulduggery worth it? Did the extra security for the United States outweigh the immediate human cost, the frequently perverse geopolitical consequences and the moral damage to American ideals? Doubters repeatedly warned presidents that on balance the CIA's foreign buccaneering did more harm than good. Mr Weiner has dug out devastating official assessments of covert operations from the 60 years he covers suggesting that many were not worth it. The sceptics were not peaceniks or bleeding hearts but hard-headed advisers at high levels of government.'

In her analysis of intelligence governance in South Africa, Lauren Hutton (2007) makes the point:

> The intelligence sector is possibly the most difficult one for civil society to engage in, and yet it holds the greatest potential to impinge upon civil liberties and the rights and freedoms of citizens. The challenge for intelligence services is to overcome the tendency to formalise the bureaucracy of secrecy, which has resulted in an obsession with secrecy.

The essence of democracy is the potential for self-correction. That can happen only if errors are exposed. Secrecy inhibits that process. The more secrecy, the more likely it is to affect the system in ways that reduce security in the long run. This is especially important when it comes to intelligence, because it is information of a particularly powerful nature.

Because it is secret, because it is supplied by spies from sources with supposedly privileged access, it carries with it a weight, an aura and an incontestability that places it above other, perhaps countervailing information. And because it is often supplied in secret, it is not open to credibility checks, or to peer review in the market place of ideas. Furthermore, the special nature of intelligence information makes it open to abuse, with the potential to influence policy outcomes that might possibly have been rejected.

Within the last few years, there have been two graphic international examples of the potential dangers of an over-reliance on secrecy: the UK and US cases for going to war with Iraq. The British government dossier of September 2002 has, in the face of two inquiries, been exposed as having been 'sexed up', despite the formal denials. Moreover, the United States evidence for links between Al Qaeda and Iraq and the presence of weapons of mass destruction as justification for the invasion of Iraq, as presented to the world by Colin Powell, has been exposed as having been based on very poor intelligence. In this case, there have been accusations of the use of torture, such as water boarding, to extract information, and an over-prioritisation of intelligence gained from pseudo-sources.

More recently, the veil of secrecy surrounding the events that led to the ending of the UK Serious Fraud Office (SFO) investigation of bribery allegations concerning the sale of weapons by BAE-Systems to Saudi Arabia was lifted, exposing the very duplicitous nature of the appeal to national security that forced the director of the SFO to end the probe. Even here in South Africa, we should remember President Thabo Mbeki's private briefing to Parliament regarding the HIV/AIDS issue, in which he implied that he was in possession of intelligence that foreign pharmaceutical companies were funding the Treatment Action Campaign.

The special credibility given to intelligence information ignores the historical fact that it is often behind the events curve, not in front. Consider, for example, the fall of the Soviet Union, when the very thing on which Western agencies were training their sights most closely had not been predicted or considered a likely outcome. In this instance, Western intelligence failed to interpret or communicate properly.

It should be remembered that intelligence agencies, like other large bureaucracies, are also interested in their own survival, and tend to ignore or downplay information suggesting that their *raison d'être* is slipping away.

Although one argument says that the greater uncertainty of the post-cold war period requires more spending on intelligence, not less, it is notable that, in the interregnum between the demise of the Soviet threat and the emergence of the 'War on Terror', a number of intelligence agencies were casting around for new reasons to justify their budgets, such as punting the possibility of getting more involved in the provision of economic intelligence. The point is that they lobby for and highlight factors that tend to confirm the reasons for their own existence.

Even internal secrecy - the hallowed need to know principle - inhibits internal accountability and an accurate perception of the 'big picture'. In the recent film documentary *Secrecy* (Peter Galison & Robb Moss, 2008) there was a revealing interview with the former CIA station chief in Jerusalem, Melissa Mahle. Mahle comes across as almost a caricature, displaying strictly practical rather than ethical reservations about the use of torture, for instance, and seemed to support the use of torture for intelligence purposes. But her insight into the organisation is valuable: she points out that the agent on the ground in Somalia was not permitted even to talk to the analysts at the Mid-East desk to check if there was a link between what was going on in the two places. She also noted that, while the intelligence focus was getting narrower and more specialised over the 1990s, the CIA missed the fact that the threats to national security were moving out of the nation state, becoming more diffuse, and were riding the wave of new technology. This was happening while agencies like the FBI were still stuck in the paper world of the 1960s.

There has been an aggressive campaign to catch up. We have seen, over the past 50 years, but especially since 2001, the enormous expansion of the secret world, of the capacity for surveillance, and therefore the capacity for abuse. Until now I have focused on international examples. Our intelligence services are different (I can hear Barry Gilder say).

That may be true, to a degree and we will come back to some specific concerns about this claim. But I want to argue that the problems of intelligence are endemic. They flow from the combination of secrecy and power that is fundamental to the way intelligence services operate. Let me first emphasize that I am not arguing for no secrecy at all. There are obviously areas that the state needs to keep secret, relating to the core areas of national security, inter alia, secure communications, operational methods, sources, the identities of covert agents, legal surveillance, information relating to the security of strategic installations

and the physical safety of individuals, and information relating to weapons of mass destruction.

But, as we have seen from the recent Protection of Information Bill, the inclination in this country, as in many others, is for the state to cast the net of secrecy much wider if it can, to the extent that you have to question whether the underlying motivation is really about national security.

Secondly, I am not totally against things like spying and covert surveillance. There are obviously cases where individuals and organisations abuse their rights to privacy and commit serious crimes, like plotting violence or sedition, or otherwise engaging in activities threatening national security or public safety. Obviously a case can be made for legal surveillance in such situations. The real questions are: Where should we draw the line between secrecy and openness? How can we prevent abuses, while allowing justified spying to take place effectively?

Let's look at the situation in South Africa in more detail and ask the question: How much of what is currently secret is justifiably so?

At the moment there are a great many things that are not publicly disclosed that could be, although, perhaps, in slightly more edited form. For instance:

- The Auditor General's reports on the spending probity within the intelligence services are only released to the intelligence oversight committee (Joint Standing Committee on Intelligence) behind closed doors.
- The numbers of requests for legal interception, and from which agencies they are received. Gilder has suggested this would disclose to our enemies how little we actually do, and would render us vulnerable. I argue that if the agencies are not carrying out their mandate properly we ought to know.
- We might legitimately demand public annual reports on what the Intelligence Services believe the major security threats and priorities are. A public annual National Intelligence Estimate would set out the major threat assessments and intelligence priorities. The US produces a public National Intelligence Estimate (NIE) without noticeably compromising their national security. Our current domestic NIEs may contain more operational detail, but there is no reason why a more restricted version should not be made public.

Gilder[2] makes a general point that disclosure of information to the public discloses information to our adversaries that they would not otherwise know. My experience is that those who are the object of intelligence scrutiny generally

make it their business to know about it, and not from accessing public sources. I can say, for instance, that when we, the media, made contact with the alleged French agent who was the subject of the surveillance operation in the Saki Macozoma saga, our impression was that his discovery from us that he had been under surveillance was far from sudden.

It is not clear to me why this most important policy area should not be subject to greater public scrutiny and discussion. Threats to national security are, after all, among the most drastic threats that a nation can face, and we all deserve the right to debate the best response to them. The publication of such independent NIEs can also help insulate intelligence professionals from the manipulation of intelligence for political ends, as described above.

The recent case in the US, when the NIE stated publicly, with a high degree of certainty, that the threat of Iran becoming a nuclear power had receded, arguably played a role in preventing the Bush administration from pushing the button for some kind of military action against Iran, which would have immeasurably worsened the poor security legacy to be inherited by the next administration.

In our own case, if, for instance, the National Intelligence Agency (NIA) reports on the development of xenophobic tensions had been made public, we could arguably have developed a national consensus to deal with the problem before it exploded in our faces. To offer another domestic example: the Human Sciences Research Council (2008) has recently published a detailed and apparently well-sourced review of our policy on Zimbabwe. The review makes it clear that policy has been ideologically heavily skewed towards ushering in a 'reformed-Zanu-PF' regime and avoiding the so-called Chiluba option, in which a former trade-union leader ousted an erstwhile liberation movement.

This skewed perspective led to a situation whereby Pretoria was repeatedly surprised by the outcome of events, such as the poor election showing of their preferred compromise candidate, Simba Makoni. A more open dissemination of strategic intelligence would either have exposed how our government was ignoring the advice their own intelligence agencies were providing, or shown how ideologically polluted our intelligence provision had become. In either case, lifting a corner of the veil of secrecy would have been in the national interest.

As far as the claim that sufficient safeguards have been built into our own systems goes, let me argue that this is not the case. Firstly, our domestic agency, the NIA, has an extremely broad mandate that makes it very easy to blur the distinction between national security and much narrower party, personal or

factional interests. The National Strategic Intelligence Act defines domestic intelligence as:

> [i]ntelligence on any internal activity, factor or development which is detrimental to the national stability of the republic, as well as threats or potential threats to the constitutional order and the safety and well-being of its people.

As Hutton (2007) points out, stability is a far more reflexive and subjective term than stability. Arguably, what we do, or try to do in the *Mail & Guardian* every week - quite legally - can sometimes be made out to be posing a threat to stability. As Gilder points out, that could make me, Sam Sole, of interest to the intelligence services, but does not necessarily make me an enemy, or an adversary as he prefers, and therefore a target.

The problem is, and this is the international experience, that the capability for covert collection is usually an irresistible temptation, as is also the tendency for covert collection to be turned into covert action. If the intelligence agencies pick up evidence that something would potentially cause instability, what are they supposed to DO? They inevitably come under pressure to do something, even if it is on the softer side of covert action, like leaking damaging information.

It is not necessary for agencies to carry out intrusive surveillance to gather potentially sensitive or damaging information: we at the M&G do not have any surveillance rights or capacity, but we are able to garner sensitive information without resorting to those methods.

The collection of sensitive domestic political intelligence is part of the NIA's mandate. The NIA's 2002/2003 annual report contained this assessment:

> Typical issues that might attract intelligence include political intolerance, inter and intra party conflict of a violent or disruptive nature or, opposition to democratisation. Any instability resulting from transformation in government structures and parastatals or from social transformation in general, would also attract NIA's attention.

As Hutton (2007) points out, it becomes difficult to separate political intelligence from partisanship and meddling in domestic political processes. That is exactly what we saw in the hoax e-mail saga, which led to the ousting of the top

leadership of the NIA. The situation concerning Masetlha's successor, Manala Manzini, is no less fraught. We have the example of Manzini's extraordinary intervention in the case against police commissioner Jackie Selebi, when he obtained an exculpatory affidavit from key witness Glenn Agliotti (later retracted) without informing the National Prosecuting Authority, Agliotti's lawyer or his own minister about his involvement in this exercise. Instead of handing this highly contentious issue with the utmost good faith, he involved a police crime intelligence official with a strong conflict of interest regarding Agliotti and the Scorpions investigation. On top of that, Agliotti's affidavit was immediately handed to Selebi for use in his bid to stop charges being laid against him.

In South Africa, there are democratic oversight structures: an Inspector-General of Intelligence and a multi-party intelligence oversight structure at the parliamentary level. But such bodies are prone to institutional capture by the big, sexy departments they are supposed to oversee. This is especially so, given that most of the work of both bodies is never open to broader public scrutiny.

In any case, the deference often displayed by such bodies and the frequently artificial blanket drawn over 'operational issues' allows them to be quite easily fed a sanitised selection of information. The oversight bodies did not pick up any of the alleged abuses that took place under Masetlha and the eventual report of the Inspector-General into that affair was never released in full. As it was, the report drew some criticism from the committee.

But all of this architecture really obscures the question: What are intelligence agencies for? And how well do they do what they are supposed to do?

It is worth recalling that the kinds of organisations that are now regarded as so vital to national security were established largely in the first half of the 20th century – MI5 in 1909, and the CIA only in the post-World War II period. Somehow nation states survived up until then without the enormous bureaucracy of secret information that we have now. The distinctive characteristic of the birth of many of the current agencies was the highly politicised, highly ideological milieu of the Cold War.

Have intelligence agencies, which, after all, are theoretically supposed to provide objective and well-sourced information, thrown off these ideological shackles, which are an obvious barrier to making the kind of accurate, predictive evaluations that should be their forte? I think not.

Let's take one example of the innate political bias of our own services. The Minimum Information Security Standards, which are the South African

regulations on information security, contain this gem: "Political appointees will not be vetted unless the president so requests." And then it goes on to say: "From the lowest level up to the deputy director general all staff members and any other individual who should have access to classified information must be subjected to security vetting."

In other words, your suitability to have access to the nation's most secret information should be rigorously tested – unless, of course, you are a political appointee. What a giveaway attitude to security!

Gilder acknowledges the political nature of intelligence. He notes: 'There is one concept about intelligence in a democracy that I have to debunk – that is the notion that intelligence is somehow neutral, removed from politics and policy. That simply is not and cannot be true.' He then goes on to argue that this is all right as long as the governments that set the political agenda for intelligence are democratically elected.

But that is simply not enough. Intelligence agencies are too powerful to serve simply as a "tool" of government. Like the rest of the security and justice system, they should be there to uphold the constitution, to serve the nation.

To quote Australian academic Paul Monk (2007):

> What political decision-makers generally do is trust their own estimates and seek from intelligence agencies data to support them. This is the case not only with dictators (Stalin was notorious in this regard), but the leaders of democratic states. There is, also, an increasing demand for current intelligence, which detracts from whatever capacity the agencies might otherwise have for taking a longer or deeper view of things. As CIA veteran Carl Ford has observed, this results in them churning out piles of insubstantial fluff, too often trying to feed the perceived preferences of their political masters.

This applies particularly to the process that Gilder calls identifying our adversaries. On the one hand, he says, if he could tell us, we would probably all agree on those identified by government as our legitimate adversaries: those who abuse their privacy to plot crime and violence and sedition.

But, in contradictory fashion, he concedes,

> If, as a nation, we could agree on who South Africa's adversaries are, then there would be little need for acrimony in the debate about intelligence

> and democracy. But South Africa is a politically and socially diverse country. One person's adversary may be another's friend. That, I guess, is true in all democracies. It is certainly not practical to hold a national referendum to get consensus on an official list of South Africa's adversaries. The way of democracy is that the government of the day gets to decide who our adversaries are.

Frankly, if the identification of an adversary is so debatable, then it should be debated, especially given the powerful spying tools government can bring to bear against its 'adversaries'.

Obviously, in the realms of both crime and defence, there are areas of what one might call 'tactical intelligence', which must enjoy the highest protection. But I suspect that much of what intelligence agencies actually do relates to far broader strategic analysis. I cannot do better here than to offer a final quote from Monk 2007:

> The challenge is not to collect secrets; it is to reason well with the abundance of information at our disposal; to subject our reasoning to the most exacting tests at the bar of open and public debate; and to invent ways to get political leaders and other decision-makers to embrace the best practices in this regard – a liberal and democratic approach to policy making and strategic thinking.

NOTES

1 Sam Sole is a journalist with the Mail & Guardian, a weekly newspaper published in South Africa.

2 References to Barry Gilder are in reference to the paper by Gilder in this publication.

REFERENCES

Earley, P. 1997. *Confessions of a spy: The real story of Aldrich Ames*, New York: G. P. Putnam's Sons.

Human Sciences Research Council (HSRC) and African Policy Institute. 2008. *Saving Zimbabwe – An agenda for democratic peace.* Pretoria: HSRC Available at http://www.hsrc.ac.za/Media_Release-353.phtml Last accessed 10 September 2008

Hutton, L. 2007. *Looking beneath the cloak: An analysis of intelligence governance in South Africa*. ISS Occasional Paper 154. Pretoria: Institute for Security Studies.

Minimum Information Security Standards. 1996. Cape Town: Republic of South Africa.

Monk, P. 2007. *Another view on the role of intelligence agencies* in The Interpreter – Weblog of the Lowy Institute for International Policy. Available at http://www.lowyinterpreter.org/post/2007/12/Another-view-on-the-role-of-intelligence-agencies.aspx Last accessed 10 September 2008

National Intelligence Agency, *Annual Report 2002/ 2003.* Available at http://www.nia.gov.za Last accessed on 8 September 2008.

National Strategic Intelligence Act 39 of 1994. Cape Town: Republic of South Africa.

Review *of Legacy of ashes: The history of the CIA*, by Tim Weiner, published in *The Economist* print edition on 16 August 2007: *The CIA – A second rate espionage agency*. Available online (by subscription) at: http://www.economist.com/books/displaystory.cfm?story_id=9644588 Last accessed on 8 September 2008.

7 PAIA and Public Participation

Chantal Kisoon

The South African Human Rights Commission has a broad constitutional mandate to promote, protect and monitor human rights in the country. Coalescing with this mandate is the mandate conferred by the Promotion of Access to Information Act 2 of 2000 (PAIA). It is largely the research garnered through monitoring and its work with the public sector that informs the substance of this paper.

In essence, the information shared in the paper makes no serious comment on the need for national security per se. What it does seek to establish is that the constitutional right to access information and legislation grounding public participation is currently obstructed, both procedurally and through the lack of internal readiness within the public sector, from delivering on the right.

If legislation governing access to information is thwarted by impediments or laws that have the potential to further restrict the fundamental right, this is cause for concern. This paper goes further to consider other challenges relating to PAIA and, in doing so raises concerns over the proposed Protection of Information Bill as a regulatory mechanism.

This look at the South African information regime through PAIA has significant implications for public scrutiny and participation. Central to the global right to information is the presumption that government-held information

should be publicly available. The Johannesburg principles create a normative framework for freedom of and access to information that seeks to balance legitimate restrictions on fundamental rights in democratic dispensations. In practice, this means that, unless government officials can give good reasons for saying that the release of information would harm legitimate government interests, the information should be given.

Some of the discussion in this paper will consider the implications of the proposed Protection of Information Bill, as a further restriction to disclosure rights entrenched in PAIA. Although, the proposed Bill accords with laudable principles in its formulation, the breadth of some of its provisions, ambiguity in processes and lack of independent review mechanisms could potentially create restrictions to openness and access to information. This could further frustrate delivery in terms of PAIA. A rational and relevant regulation framework for information management in the public sector is therefore critical.

In the South African context, through the 1994 government, we saw masses of information on the covert activities of the intelligence and security branches of the previous government become public. It is important to note, too, that masses of information from this era was destroyed. However, what has come to light has confirmed some of the gross human rights violations that occurred under the guise of national security in apartheid South Africa.

The process of opening up information previously regarded as classified has resulted in a necessary redress of past abuses. In this sense, disclosure also facilitates a sense of closure and justice for victims of authoritarian rule. Jamaica, India, Mexico, Panama and Peru have all enacted new comprehensive laws to allow for citizens to access state-held information. Even countries in Eastern Europe are now embracing openness by opening up the archives of the Soviet-era secret police. While this is a step in the right direction, it is easier to disclose information about the conduct of others than to allow scrutiny and perhaps censure of oneself.

A pattern is emerging in other jurisdictions. Comparatively, we have seen a number of jurisdictions embrace access to information legislation, but they have equally quickly weighted their legislation with a proliferation of sophisticated related legislation. Our own current security matrix, while seeking to reform legislation like the Official Secrets Act and the Protection of Information Act of 1982, is still too protective of its activities in the name of national stability and security. The proposed Protection of Information Bill is heavily weighted in executive discretion and exhibits just such a characteristic.

Globally, national security remains a common exemption found in most freedom of information legislation. Progressive democracies are, however, increasingly advancing the idea that the privileges conferred by national security demands as a justification for secrecy can only be exceptional.

The tension between executive action and the need to increase transparency cannot be easily diffused. In fact, it would be naïve to expect complete openness and transparency. The trend gaining momentum in many democracies is informed by the primacy of the need for commitment to transparency, accountability and democratic governance by state actors. This is a reaction to the recorded and potential danger of using national security as a trump on the operation of fundamental rights.

In South Africa as with many commonwealth jurisdictions, the public interest clause in PAIA trumps all of these exemptions. So even where exemptions apply in terms of national interest, if the public benefit of knowing the information is proven to be greater than the harm in making the disclosure, then information should be released on the basis of that interest. But in practice and in the context of the South African dynamic, this will be difficult to achieve, particularly because of the vast socio-economic disparities in our demographic.

Tom Blanton argues that it is

> inappropriate to balance open government which is both a condition and a value of democratic society against national security which is not a value itself but rather a condition that allows a nation to maintain and protect its values…in balancing a right one starts with two things that are prima facie equal and have to be given equal weight at the onset. With national security one is not talking about a right but a restriction, which has to be interpreted in a limited way…national security has become an obese beast, which urgently needs to be put on diet if one is to protect fundamental rights from its crushing bulk. The proposal was not to shoot this beast but rather to slim it down!' (in Darbishire 2003).

CHALLENGES WITH OVERSIGHT

Secrecy forces the public to accept being uninformed and subject to the judgement of the executive as opposed to being able to exercise the right to informed

participation and self determination. In moments of greatest insecurity, the public is most likely to accept the need for information to be kept secret in the public interest. This is also the most likely time when decisions impacting on national interests and individual rights will go unchallenged. It is, however, undoubtedly the time when there is the most significant need for accurate information to be shared.

Lauren Hutton's commentary aptly advocates the need for a commitment to national values, human rights and personal freedoms, when she states:

> Ensuring sufficient mechanisms of control over the use of force should, in democratic theory, guard against the misuse of the state security arsenal for personal or group interest at the expense of individual security…the state security arsenal should be bound by the same principles of good governance as the other tools of statecraft, and constant vigilance is required to ensure that the covert use of power does not infringe on national values, human rights and personal freedoms (Hutton 2007).

But the national security trump is one of those areas in which it is difficult for civil society actors and activists to promote reform. This is primarily because of the secrecy surrounding executive decisions impacting on national security, and because of the nature and manner of decision-making. Non-experts are often forced to assess subjective and technical information, usually involving political sensitivities, while hampered by insufficient information. It becomes difficult for those outside of the decision-making process to assess rationality and the degree of seriousness. In the face of these factors it often becomes easier to defer to the executive.

Most courts in comparative jurisdictions also appear to indicate a preference for handing over their role in intervening in and assessing national security matters to the executive. It is precisely this demarcated jurisdictional boundary, marked by such ambiguity that ultimately jeopardises the enforcement and realisation of fundamental rights.

In terms of PAIA, enforcement presents difficulties, but this will be explored later in the paper. This obstacle to enforcement is heightened in the proposed Protection of Information Bill by the absence of an adjudicatory body, independent of government, to review refusals. Ultimately such decisions will be subject to the scrutiny of the courts.

Using the judicial system as an adjudicatory body when it comes to access to information matters is, in fact, extremely problematic for a number of reasons. These include, inter alia, the inherent imbalance of power between those who request and those who hold information, and a demonstrated reluctance to engage on these matters in comparative jurisdictions.

The overly broad and vague definitions of national interest and security in the proposed Protection of Information Bill create significant opportunity for government to legitimately block access. This will be almost impossible for the majority of South Africans to challenge before the court. We need to assess how our courts will review and assess decisions to classify, define and refuse disclosure.

The Johannesburg principles established a sound threshold that restrictions on a fundamental right in terms of national security must of necessity be informed by clear and restrictively-drawn categories of information. This must be driven by serious threat. The limitation posed should be least restrictive in ambit and be compatible with democratic principles. The grounds listed in the proposed Protection of Information Bill, however, are vast and span just about any describable activity as worthy of being in the national interest. It will be extremely difficult in practice to challenge non-disclosure on these grounds, particularly where the already restrictive public interest clause in PAIA is pitted against the broad national interest provisions of the Bill.

EFFECT

It is now accepted that openness and transparency are necessary for protection against human rights abuses by intelligence and security services. Shielding even previous operations from scrutiny means that the public can never know or assess the conduct or legitimacy of their elected representatives. And perhaps more significantly, it means that this conduct is usually not corrected or prevented from future recurrence. Resource allocations and government spending on secret operations and processes are also usually not made public. In this sense the public can never quite influence the actual division and allocation of their money. The result is that gaps cannot be identified, there is less public confidence, and the public is unable to effectively mobilise, pressurise or influence priority agendas or spending.

Sometimes information withheld in the name of security translates into an unwillingness to disclose vulnerability or capacity. The rationale is that this in

effect weakens security rather than promoting it. It should be borne in mind that accountability is the end result of disclosure. This does not concern information alone. The vulnerability described in the information must also be eliminated. It also means that institutional inertia for inaction or omission cannot readily be kept in check.

Secrecy safeguards like non-disclosure result in public ignorance of the type and magnitude of past and current activities. In this sense a number of violations can potentially be protected and kept secret. It leaves very little leeway for a people to influence this critical area of governance within the security sector. The National Intelligence Agency (NIA) is one of the state organs claiming a complete exemption from PAIA to avoid compliance with Section 14. This provision in PAIA requires public entities to list which categories of information in their possession can be accessed automatically and which can be obtained on request. The exemption granted to NIA demonstrates how national security and the inherent need for secrecy associated with the intelligence sector can be raised as shields to information-sharing legislation.

PAIA AND THE PROTECTION OF INFORMATION BILL

A number of challenges already exist for PAIA without the compounding effect of the proposed Protection of Information Bill. Enforcement and resource constraints underpin the key challenges to successful realisation of the implementation of access to information processes in the public sector.

It has been noted through monitoring-based research that the internal readiness of the public sector to fully implement PAIA is extremely weak. Apart from the lack of adequate systems and processes to operationally implement PAIA, issues relating to lack of capacity constrain implementation. Some of the issues noted are that public sector personnel struggle with the procedural nature of PAIA, its interpretation and application, and that these competency-based challenges are exacerbated by the culture of secrecy prevalent in the sector.

Similar criticisms will find force in the implementation of the Protection of Information Bill. In particular, it is alarming that neither implementation nor operational costs have been factored as needs for the realisation of the proposed legislation. While the broad scope of terms like national security will result in a heightened commitment to non-disclosure, the lack of any financial budgeting

for realistic implementation will render arbitrary the implementation of its processes. This will in effect give rise to inconsistent application and implementation, to the detriment of requesters.

The actual process of requesting has also posed substantial challenges. In the physical sense, many requesters are unable to lodge requests, on account of geography or economy. The Development Policy Research Unit in Cape Town cites statistics averaging the number of people having access to IT communication at only 15 people per 1000 in the SADC region. This is a bleak figure, which improves somewhat for South Africa where the average is 47 computers per 1000 people. This means that large numbers of people do not have access to modern modes of communication. It is of even more concern when one considers the impact of this on vulnerable groups. These types of statistics demonstrate a need for government to drive information sharing through commitment of resources, especially to utilise mass media.

Procedurally, the time frames imposed by PAIA, although not unique comparatively, are already proving burdensome, with allocations for extensions and appeals significantly slowing down public-sector responses. The 90-day period prescribed in the Protection of Information Bill will significantly hamper an already slow process.

The appeal process in terms of PAIA is also negatively impacted by a number of factors. These include the fact that appeals are internal and outcomes rarely endorse the reversal of a refusal, which in effect means further delays. Requesters usually drop out because the next step in securing or enforcing the right to access information is going to court. Our research reveals a disturbing trend showing that most implementers, when they are unsure about granting access, prefer to refuse, allowing the matter to go on an internal appeal. This guarantees some immunity from accountability for the possibly incorrect release of information.

PAIA enforcement is another area that warrants scrutiny: at present, final enforcement rests with the courts. Increasingly critics of this enforcement process will necessitate the creation of an office of an information commissioner. It is envisaged that this body will have a broad mandate to assume the role of monitor, counsel, and advocate and intermediary enforcement authority to pronounce on access to information matters cheaply and expeditiously. The Protection of Information Bill allocates many of these functions to the NIA. Recommendations from South African civil society organisations, however,

cogently address the need for an independent expert to address protection of information matters. The South African Human Rights Commission (SAHRC) has endorsed such a submission to the Ad Hoc Committee on Intelligence Legislation currently reviewing the Bill.

However, the SAHRC has noted that, regarding the role with which independent bodies are tasked, special precautions have to be taken to ensure that adequate resources are deployed for the execution of the mandate. According to Dave Banisar, a world-renowned freedom of information advocate, the United States Security Oversight Office estimated in 2000 that the annual cost of creating and maintaining secrets was 4.3 billion US dollars. These costs excluded those of the Central Intelligence Agency (CIA).

It is problematic that, as far as both PAIA and the proposed Protection of Information Bill are concerned, there are no budgetary allocations for implementation. Should the office of an information commissioner materialise, government will have to commit resources to ensure that the body is fully able to exercise its powers and mandate independently and effectively.

RECOMMENDATIONS

The challenge, appropriately stated at the beginning of this presentation, is that it is not a balance between a condition and a fundamental right that is sought in harmonising information management policies, but rather the need to advance openness, transparency and public participation in a vulnerable area of governance.

Certainly a need to harmonise legislation at the local level has to be demonstrated if any commitment to this ideal is to be realised. But the increased cross-border flows of people and information mean that a primacy will have to be accorded and committed to regionally as well as internationally.

This can only happen if regional bodies like Southern African Development Community and the African Union ensure that the frameworks placed in response to anticipated threats and the work of the intelligence community all take fundamental rights as their starting point. Harmony must be sought in the codes and practices binding states with common interests, purposes and objectives. Regional bodies must therefore integrate and prioritise a full commitment to access to information and accountability principles. Formal compliance is no longer adequate.

It is also necessary for those existing oversight committees that are dedicated to reviewing and maintaining democratic standards on human rights in operations of the intelligence services to share information more accurately and frequently. Operations per se must be subjected to sound human rights-based impact assessments to test potential for harm to fundamental rights prior to and during the conduct of secret operations.

The commitments called for must be closely monitored in terms of implementation and adherence through processes like the African Peer Review Mechanism and through networks of independent review bodies, continentally and globally. When South Africa underwent peer review, the implementation of the access to information regime was rated as extremely poor, and yet no substantive response to implementation challenges has been forthcoming.

Executive action conducted in secrecy creates fertile ground for unchecked human rights abuses at every level. A demonstrated commitment to democratic principles of openness, transparency and accountability must be secured. In conclusion, I would like to stress the need for a commitment not only in political will but also in resources to drive implementation and the attitudinal changes necessary for informed scrutiny. To address these issues, the executive should discard paternalistic approaches to vulnerable operations in favour of developing a partnership with its constituents, premised on respect for human rights and public participation in its processes.

REFERENCES

Darbishire, H. 2003. *National security and open government – striking the right balance*. New York: Campbell Public Affairs Institute, The Maxwell School of Syracuse University.

Hutton, L. 2007. *Looking beneath the cloak: An analysis of intelligence governance in South Africa*, ISS Occasional Paper 154 Pretoria: Institute for Security Studies

8 Critique of the Protection of Information Bill

Melissa Moore

The Freedom of Expression Institute (FXI) was established in 1994 to protect and foster the rights to freedom of expression and access to information, and to oppose censorship. The primary objectives of the FXI are to fight for and defend freedom of expression, to oppose censorship, to fight for the right of equal access to information and knowledge, and to promote access to media and a free press.

It is with these objectives in mind and our pursuit of the maximum degree of individual liberty that we have studied and submitted comment on the new Protection of Information Bill.

At the outset, I would like to emphasize the undoubted necessity for a new law to be promulgated that would alleviate and cure the current climate of uncertainty and inconsistency surrounding the classification, environment, the powers of the National Intelligence Agency (NIA). It should also provide for the adequate protection of information that genuinely requires protection.

The Protection of information Act of 1982 currently on the statute books was promulgated at the height of the apartheid era. It is characterized by sweeping powers and a general disregard for human rights, particularly the rights to freedom of expression and access to information. This has resulted in the public

being denied access to information. There is also a lack of openness, transparency and accountability on the part of the government of the day. It is with this in view that we should be extremely circumspect in the appraisal of the law which is to replace it.

It is true that we need to move away from a presumption of secrecy to a presumption of openness, but the question that we must all ask ourselves is whether the Bill will attain this objective.

The Bill defines sensitive information as 'information, which must be protected from disclosure in order to protect the national interest of the Republic from being harmed' (Chapter 15 Section 14). For the sake of brevity, I am not going to repeat the full definition of national interest as contained in the Bill, but will quote subsection 15(1)(a), which states that the National Interest of the Republic includes *'all matters relating to the advancement of the public good'*. This definition forms the core of FXI's many reservations in respect of the constitutionality of the Bill.

In terms of the principle of legality, laws must be clear and accessible. They must be drafted with such precision that they allow those who are tasked with their implementation to have reasonable certainty about the conduct required of them.

Section 36 of the Constitution states the terms in which a right in the Bill of Rights may be limited, in this instance the right to freedom of expression and access to information. Such information may be limited in terms of law of general application to the extent that the limitation is reasonable and justifiable in an open and democratic society based on human dignity equality and freedom. What qualifies, as a law of general application is a law which is stated in a clear and accessible manner. The definition of national interest is vague and overbroad, and is an unjustifiable limitation on freedom of expression, which could promote arbitrary and discriminatory decision-making. It would encapsulate virtually everything in contemporary society from a method by which Bafana Bafana could win the World Cup to information on Zimbabwean atrocities.

In my view, the correct approach would be to limit the operation of the Bill to matters that are necessary to protect the national security of the Republic of South Africa and matters directly related thereto. It is also my view that what is then required is for the threshold to be raised one step higher to require that the disclosure of information sought to be classified must inevitably, directly and

immediately cause the occurrence of an event which would harm the national security of the Republic, which harm the classifying authority would have to identify and describe.

It has been argued that, by virtue of the intrinsic value approach (IV), sufficient checks and balances have been incorporated in the Bill to safeguard against abuse, which is the public's primary concern. According to the Bill, the intrinsic value approach should be used to determine what State information should be protected from unauthorized disclosure, destruction and loss (Chapter 2 Section 8). The IV approach demands a reasoned and rational approach on the part of the classifier. It should promote the effective administration of government and balance the rights of individuals with legitimate governmental requirements and objectives. It 'involves a consideration of the content of information and the consequences of disclosure' (Chapter 2 Section 8.2c).

The IV approach then goes on to state that the determination should also include the following considerations (Chapter 8 Section 3):

- whether the organ of state has a legitimate interest in protecting the information from disclosure;
- an understanding of the types and categories of information within an organ of state;
- an appreciation of the inherent and essential utility and significance of the information;
- an assessment of the reasonably foreseeable consequences if specific information is disclosed, altered or destroyed; and
- an assessment of the protection and administrative costs associated with each type or category of information compared with the ultimate benefits of protection against disclosure, alteration or destruction.

Regardless of the existence of standards and methods and criteria for classification, unless there are appropriate external checks and balances, such methods, approaches and criteria are meaningless and remain a fundamental flaw in the Bill.

Coupled with the overbroad definition of national interest are the extremely broad parameters of the application of the Bill. The Bill applies to all organs of state, natural and juristic persons, and goes so far as to include a facility of installation that has been declared a national key point. The problem with

this is that, although it is necessary to protect certain places or areas from loss, damage, disruption or immobilization which would prejudice the security of the republic, as the National Key Points Act currently stands, the declaration of a specific area as a national key point is left to the sole discretion of the Minister of Defence.

If we look at the internal review and appeals procedures in the Bill, it is essentially the same persons tasked with classifying information who are going to attend to the reviews of the status of such information and the appeals. While there is the possibility of recourse to the courts, practical difficulties exist in this regard, such as costs and the information available to prepare papers. The fact is, this route is time-consuming, making it impossible to report timeously.

I have already alluded to the fact that it is extremely difficult for practitioners to draw accurate documents as required by the Bill when applying for a status review, when they have no access to the register or documents denied them under what I term the "double blind rule". Section 30(6) of the Bill allows the head of an organ of state in response to a request for a review of the classified status of information to refuse to confirm or deny whether information exists whenever the fact of its existence is itself classified as top secret. We regard this provision as fundamentally unconstitutional, inviting as it does an element of untruthfulness, equivocation and obstruction of fair and reasonable enquiry. It is virtually impossible to make any reasonable headway in discovering the true state of affairs when such provisions are in operation.

The construction of this section is such that it effectively allows public servants rights that are in direct contradiction to the obligations that the Bill imposes on all citizens not to provide false information to intelligence services (Chapter 11 Section 47). This is not a fair and even-handed approach and, as such, is an unequal handling of the relationship between the state and the individual. We do not believe that this limitation on the right to receive information would stand the test of a balancing of interests analysis according to section 36 of the Constitution.

The Bill also has a severe impact on investigative journalism, as it sets penalties of up to five years for disclosure of classified information and up to five years imprisonment for failing to report the possession of such information (Chapter 11 Section 39 & 40). It is interesting to note that the penalties set for improper classification have been limited to a maximum period of three years

(Chapter 11 Section 49). This, in my view, creates the perception that there is a clear bias in favour of the state or classifier.

These penalties and the threat of prosecution will be a powerful disincentive to investigative journalism. It is cold comfort to contend that prosecutions would not be lightly undertaken, as the mere threat of prosecution is a sword of Damocles hanging over the head of any journalist who, quite rightly, pursues the truth. The rights of freedom of expression are directly affected by the absence of such an exemption, as the media find it extremely difficult to operate in an environment fundamentally hostile to the gathering of essential information, which is, after all, required to expose wrongdoing and corruption in government circles.

Absence of an exemption means that those working on stories dealing with classified information are always at risk of prosecution. While it has been intimated that no such prosecution would be instituted if the aim of the investigation were clearly to expose criminal behaviour on the part of those protected by the classification, the Ministry has not seen fit to formally acknowledge this essential function of the media. As the situation stands, journalists face the prospect of a complex legal battle with attendant costs, personal discomfort and intimidation. This cocktail is a powerful disincentive for any diligent journalist seeking to provide the public with a truthful comment.

We are likewise disturbed that, despite discussions held with the drafters of the Bill, there is no section dealing with the so-called 'public interest exemption'. The crucial role of the media in promoting Constitution building and maintaining a watchful eye on the activities of government will be adversely affected by this omission. In addition, the Ministry has seen fit to include severe penalties, as evidenced by section 23 read with section 46. While we note that those who drafted the Bills have already engaged in discussion on this issue, we believe that the proposed remedy (acquittal) does not fully address the problem. The individual is still exposed to the danger and inconvenience of prosecution, which in turn will provide a powerful disincentive to pursuing this essential function. We believe that, in accordance with the general principles of the administration of justice, it would be inappropriate to place the onus of proof on the journalist. This is inconsistent with our approach that things done in the public interest should not attract censure.

What is required is an exemption requiring of the journalist only to allege a bona fide interest. In the event that such bond fide interest was contended by

the state, the onus would be on the State to prove the absence thereof in line with the normal criminal law onus of proof.

The concept of access to information, which was espoused by the Promotion of Access to Information Act, is sound, and it appears that an attempt has been made to recognize the importance of access as visualized in that PAIA in section 34(1). It is, however, unfortunate that there appears to be an overlapping of the area in which PAIA and the Bill operate. We believe that a large number of requests for information and the declassification thereof could have been avoided by a narrowing of the scope and application of this Bill. This would have resulted in considerable savings for the state and advanced the general openness and transparency of the information regime.

Owing to the overlapping referred to above, there is a considerable danger that regulations published under this Bill could well cloud the legal landscape even further. Extreme care will have to be taken to harmonise such regulations with those extant in PAIA. We also believe that, had the Bill contained a provision for an ombudsperson's office, this would have been a suitable way to handle requests for information.

Under PAIA, internal appeals are possible in respect of information held by a public body in terms of section 74 of PAIA, after which the matter may be appealed to the court. However, where a requester is denied access in respect of private bodies, no internal appeal exists. The procedure is at odds with the Bill, which provides for internal appeals on classified records in respect of both private and public bodies. However, had there been an ombudsperson's office, the discrepancy could have been eliminated by allowing the ombudsperson to fulfil an appeal role. This is particularly important in order to avoid the significant costs of an appeal to court. These costs represent an effective barrier to access to information and work against the spirit of freedom to receive information.

The Bill does not make provision for the creation of the Office of the Ombudsperson whose function it would be to assist the public at large in its quest for access to classified documents and to assist all as an overseer of the classification process. The arguments advanced against the creation of such an ombudsperson have been concerned with cost implications and the fact that other avenues are available under other legislation. The arguments also point to the process declared in the Bill relating to declassification, whether by the head of the relevant organ of state or the courts. We believe that the creation of such an office would have gone a long way to allaying public disquiet about

intelligence affairs. In addition, an ombudsperson would have been a useful, easily accessible and cost effective means of addressing inquiries and complaints in respect of the status of classified information.

The fact is that, if the Bill genuinely intends to create a culture of openness and transparency (as opposed to the secrecy of the past), the public should embrace any steps that would inculcate an acknowledgement of the need to debunk the myth of the supremacy of secrecy and advance constitutional legitimacy. It is ludicrous that the state should plead insufficient expertise among the public to permit of the appointment of an ombudsperson, and equally unbelievable that the Ministries represented by one of the drafters of the Bill (in an interview on Radio 702) have claimed that there are financial constraints. The proper utilization of an ombudsperson would result in the avoidance of costly processes to determine whether classification is justified or not, and would certainly serve to avoid the lengthy delays that are intent in the proposed appeal procedure and the conduct of court proceedings, which are prohibitively expensive for the members of the wider public. Nor should it be argued, as has been suggested by the Ministry's representatives, that the pre-eminent matter is one of protection. The pre-eminent matter should always be the preservation of the maximum amount of individual liberty and the limitation of the state's attempt to withhold information from its citizens.

The departure point should be one of maximum disclosure on a timely basis, which would itself present substantial cost savings. Classification should always be a last resort. The ombudsperson's role should be twofold, involving both the prevention of unnecessary classification and the facilitation of access to information already classified. This would be an easy and relatively inexpensive operation. If concerns exist as to the suitability and stature of candidates for an ombudsperson/external oversight body, then one need only look to the processes employed on bodies like the Broadcasting Complaints Commission of South Africa (BCCSA), where the public plays a direct role in the nominations and the candidates are suitably screened.

Only by creating this public-friendly approach will it be possible to avoid the perpetuation of a legacy of public distrust of those charged with administering the protection of information. To expect the public to blindly invest their trust in officials appointed by the Ministry or the head or organ of state is unrealistic. The Ministry's integrity has been tarnished in recent times and the vast majority of South Africans are still extremely sceptical of an organization whose

predecessor was a key cog in the apartheid wheel. It will take more than just the inclusion of constitutionally friendly-sounding phrases to create a climate in which the media and the public could begin to establish faith in the integrity of those tasked with the classification of information.

The unwillingness of the Ministry to embrace the concept of the ombudsperson or some other external monitoring body will undoubtedly reinforce the view that this Bill is nothing more than another attempt to create an additional hurdle for those seeking to hold the state and the ruling party accountable for their deeds.

REFERENCES

Constitution of the Republic of South Africa Act 108 of 1996, Cape Town: Republic of South Africa.

Promotion of Access to Information Act 2 of 2000, Cape Town: Republic of South Africa.

Protection of Information Bill (B28-2008), Cape Town: Republic of South Africa.

9 Concluding remarks

Lauren Hutton

Since this series of seminars was conducted and the compendium of papers compiled, much has changed in the South African intelligence environment. Following the resignation of former president Thabo Mbeki, Ronnie Kasrils resigned as Minister for Intelligence Services on 25 September 2008. Before leaving office, former minister Kasrils convinced Mbeki's Cabinet to release the report of the Ministerial Review Commission on Intelligence.[1]

Kasrils established the Commission in August 2006 with the purpose of reviewing mechanisms of control of the civilian intelligence structures to ensure compliance with legal and constitutional imperatives and to minimise the potential for the misuse of position and the abuse of power. This came after the scandals involving the ousted Director General of NIA, Billy Masetlha, and the infamous hoax e-mail saga. The report, totalling more than 300 pages, is particularly critical of the manner in which secrecy is used and information kept confidential contrary to constitutional provisions guaranteeing transparency and access to information. Specific aspects recommended for publication included ministerial regulations, audit reports and annual budgets, annual reports and periodic security assessments.

Also key were the Commission's recommendations on the mandate of the domestic intelligence service. It was recognised that the broad mandate

assigned to the NIA by the White Paper and the National Strategic Intelligence Act has detracted from the ability of the agency to focus on serious criminal threats and the potential for violence. Further, as pointed out by various commentators in this collection, the broad mandate of the NIA is a possible cause of the politicisation of the agency and 'has given rise to an inappropriate focus on political activities'.

The report focuses intensively on mechanisms of control, including ministerial control and the role of the Inspector General, as well as controls on the use of intrusive methods of investigation. The Commission also called for a new White Paper on Intelligence based on the recognition that the current document does not translate democratic philosophy and principles on security and intelligence into meaningful policies.

Sam Sole and Nic Dawes of the *Mail & Guardian* published the report on the *M&G* website (http://www.mg.co.za), and reported that the current head of the NIA, Manala Manzini, had tried to block the public release of the report. At the time of writing, the report was still not publicly available on any government websites.

In the light of the resignation of Kasrils, Dr Siyabonga Cwele was appointed Minister for Intelligence Services. Until his executive appointment, Dr Cwele had been serving as chairperson of the Joint Standing Committee on Intelligence. He will serve in this ministerial portfolio until the elections in April 2009.

Meanwhile, in the weeks following the premature departure of Kasrils, the report of the Commission was shelved somewhere in the offices of the spooks. Hopefully Kasrils' initiatives will not be lost and the reform processes outlined in the recommendations of the report will one day become a reality. The almost inaudible voice of civil society in issues relating to the intelligence sector guarantees a lack of advocacy for the implementation of the Commission's recommendations. The handful of people interested in and devoted to the development of a model of democracy in terms of intelligence governance, such as those who contributed to this publication, are a very small minority with a marginal voice. With the scale of troubles facing our nation, perhaps it is not too surprising that advocacy on the democratic control of the intelligence sector is not at the top of the list.

There were real gains to be made with the work of the Commission and it was hoped that Kasrils would implement some of the recommendations,

particularly those relating to the White Paper, mechanisms of control and the mandate of the NIA. Many see the departure of Kasrils as the end of the potential for significant reform, especially in the remarkably changed political environment in which South Africa finds itself in the post-Mbeki era.

After a meeting of the Ad Hoc Committee of Intelligence Legislation on 15 October 2008, the Protection of Information Bill was withdrawn. The final stumbling block, after many revisions to remedy issues such as the public interest clause and the definition of national interest, was the manner in which the bill addressed private intelligence companies. The parliamentary committee decided that insufficient time remained for the Committee to deal with further revisions and the bill should be reintroduced in 2009.

With all the issues on the table concerning classification and declassification and the pressing need to create more openness and transparency, it was an interesting decision not to create a new information security regime, because of the private intelligence issue. The issue of private intelligence has only been dealt with peripherally in this text, as the primary focus has been on the state actors. Private intelligence in South Africa is a particularly complex and emotive topic, not because of the outsourcing phenomenon experienced in western states, but because of the historical legacy. With security sector transformation and the preceding political transformation of the mid-1990s, many security service personnel resigned or were demobilised. These experienced apartheid-era intelligence, police and military personnel have formed the core of the private security and intelligence industry in South Africa.

From the earliest days of the democratic era, the intelligence services were concerned about private intelligence actors and the so-called information peddlers who knowingly supplied false information to the state and others. The Protection of Information Bill was to provide regulations, and outlined criminal offences for knowingly providing false information to the state intelligence services. It was expressed, however, by the parliamentary committee that this was not sufficient and that more regulations for the private intelligence industry should be applied, specifically that they should be registered and be under the control of the state.

This is a very complex area, thanks not only to the difficulties that arise when one tries to define private intelligence and to differentiate private intelligence from think-tanks and research institutions. The inclusion of the issue of private intelligence in the debate on the protection of information seemed a

strange marriage. The lack of clarity on private intelligence, an area in which the creation of clarity is going to be difficult, has derailed potential steps towards declassifying pre-1994 information and establishing more openness and better access to information.

The end of 2008 brought with it a certain *déjà vu*. At this time last year, we were talking about the impending Protection of Information Bill, in the hope of seeing a revision of the apartheid-era information control regime and the possibility of reforms driven by the report of the review Commission. We await 2009 with similar hopes.

NOTES

1 The Report of the Ministerial Review Commission on Intelligence, *Intelligence in a Constitutional Democracy,* is available at: http://www.issafrica.org/index.php?link_id=31&slink_id=5985&link_type=12&slink_type=12&tmpl_id=3.

Appendix

Intelligence in a Constitutional Democracy

EXECUTIVE SUMMARY

Final Report to the Minister for Intelligence Services, the Honourable Mr Ronnie Kasrils, MP, Ministerial Review Commission on Intelligence.
23 September 2008.

CHAPTER 1: INTRODUCTION

The Minister for Intelligence Services, Mr. Ronnie Kasrils MP, established the Ministerial Review Commission on Intelligence in August 2006. The Commission comprises Mr. Joe Matthews (Chairperson), Dr Frene Ginwala and Mr. Laurie Nathan.

In this Report to the Minister we present our findings and recommendations.

The aim of the review was to strengthen mechanisms of control of the civilian intelligence structures in order to ensure full compliance and alignment with the Constitution, constitutional principles and the rule of law, and particularly to minimise the potential for illegal conduct and abuse of power.

The review was expected to cover the following intelligence structures: the National Intelligence Agency (NIA); the South African Secret Service (SASS); the National Intelligence Coordinating Committee (NICOC); the National Communications Centre (NCC); the Office for Interception Centres (OIC); and Electronic Communications Security (Pty) Ltd (COMSEC).

The terms of reference identified the following topics to be addressed in the review: executive control of the intelligence services; control mechanisms relating to intelligence operations; control over intrusive methods of investigation; political and economic intelligence; political non-partisanship of the services; the balance between secrecy and transparency; and controls over the funding of covert operations.

The first phase of our work entailed reading the relevant legislation, meeting the heads of the intelligence organisations and reviewing their submissions and operational policies. In the second phase we had follow-up sessions with some of these organisations, met with other government bodies and did research on intelligence controls internationally. In the third phase we wrote the Report and provided the Minister with comment on draft legislation.

Many of our recommendations are based on proposals made to us by the intelligence services, other government bodies and non-governmental organisations, and we acknowledge this throughout the Report.

Our terms of reference required us to produce a public report with an emphasis on practical recommendations. We have endeavoured to make realistic proposals and have written the Report in a style that we hope will be accessible and informative to an audience beyond the intelligence community.

CHAPTER 2: KEY PRINCIPLES AND PERSPECTIVES ON SECURITY AND INTELLIGENCE

The main functions of intelligence services are to predict, detect and analyse internal and external threats to security and to inform and advise the Executive about the nature and causes of these threats. The services are thereby expected to contribute to preventing, containing and overcoming serious threats to the country and its people.

In order to fulfill their vital functions, intelligence services throughout the world are able to operate secretly and have special powers to acquire

confidential information through surveillance, infiltration of organisations, interception of communication and other methods that infringe the rights to privacy and dignity.

Politicians and intelligence officers can abuse these powers to infringe rights without good cause, interfere in lawful politics and favour or prejudice a political party or leader, thereby subverting democracy. They can intimidate the government's opponents, create a climate of fear and manipulate intelligence in order to influence state decision-making and public opinion.

Given these dangers, democratic societies are confronted by the challenge of constructing rules, controls and other safeguards that prevent misconduct by the intelligence services without restricting the services to such an extent that they are unable to fulfill their duties. In short, the challenge is to ensure that the intelligence agencies pursue a legitimate mandate in a legitimate manner.

This challenge lies at the heart of our terms of reference. We have addressed the challenge and conducted the review through the lens of the Constitution. The Constitution is our legal and ethical framework because it is the supreme law and lays "the foundation for a democratic and open society in which government is based on the will of the people and every citizen is equally protected by law".

Notwithstanding their grave responsibilities and the perils they might have to face, the intelligence agencies and other security services are at all times and in all respects bound by the Constitution. The Constitution states that the security services must act, and must teach and require their members to act, in accordance with the Constitution and the law; that national security must be pursued in compliance with the law, including international law; and that no member of any security service may obey a manifestly illegal order.

The Bill of Rights enshrines the rights of all people in our country and affirms the democratic values of human dignity, equality and freedom. It binds the legislature, the Executive, the judiciary and organs of state. The intelligence services are obliged to respect constitutional rights and may not infringe these rights other than as permitted by the Constitution and legislation.

The Constitution insists that the security services may not prejudice a political party interest that is legitimate in terms of the Constitution or further, in a partisan manner, any interest of a political party. We are concerned that NIA's mandate may have politicised the Agency, drawn it into the realm of party politics, required it to monitor and investigate legal political activity and, as a result, undermined political rights that are entrenched in the Constitution. As

NIA has noted, the politicisation of the intelligence process and product has a high risk of impairing the Agency's command and control, oversight, accountability and ability to serve the national interest.

The Constitution proclaims, "national security must reflect the resolve of South Africans, as individuals and as a nation, to live as equals, to live in peace and harmony, to be free from fear and want and to seek a better life". National security should thus not be conceived as separate from, and potentially in conflict with, human security and human rights. It encompasses the security of the country, its people, the state and the constitutional order.

The Constitution states that "national security is subject to the authority of Parliament and the national executive". The accountability of the intelligence services to the Executive and Parliament is strong. But the accountability of the services and the intelligence oversight and control bodies to the public is less strong. This is a consequence of excessive secrecy, which is inconsistent with the constitutional tenet that all spheres of government must be transparent and accountable.

CHAPTER 3: THE WHITE PAPER ON INTELLIGENCE

The aim of the White Paper on Intelligence of 1994 was to provide a framework for understanding the philosophy, mission and role of intelligence in the post-apartheid era. The White Paper has two core themes – democracy and the rule of law, and a holistic approach to security - which were intended to guide intelligence transformation in the new democracy.

The main strength of the White Paper is that it lays out a democratic philosophy and set of principles on security and intelligence. The main weakness of the document is that it does not translate the philosophy and principles into meaningful policies. The emphasis is almost exclusively on values and norms. Policies on intelligence functions and operations that ought to be covered in the White Paper have instead been addressed only in departmental policies that are secret.

A further weakness of the White Paper is that it defines NIA's mandate too broadly. The broad mandate has led to a lack of clear and consistent focus, created pressure for analytical breadth rather than depth and left the Agency over-extended. It also creates the risk that NIA neglects its most important and difficult function, which is to identify, analyse and forewarn government about violence and other extreme threats that entail criminality.

A new White Paper on Intelligence is needed. It should cover the mandates, functions and powers of the intelligence organisations; controls and oversight in relation to their powers to infringe constitutional rights; executive responsibility and accountability; civilian oversight; the co-ordination of intelligence; intelligence relations with other countries; secrecy and transparency; and ensuring respect for the Constitution and the rule of law.

The process of preparing the White Paper should include consultation by the Minister and parliamentary hearings and debate following a call for public submissions.

CHAPTER 4: MINISTERIAL CONTROL AND RESPONSIBILITY

The Constitution states that the President must either assume political responsibility for the control and direction of the civilian intelligence services or designate a member of Cabinet to assume that responsibility. The President has appointed a Minister for Intelligence Services (hereafter "the Minister"), who is accountable to the President, Cabinet and Parliament for the exercise of his or her powers and functions.

The Minister's powers and functions as specified in the intelligence legislation are clear, precise, appropriate and necessary to enable him or her to exercise political responsibility.

However, a number of critical issues are not covered adequately in the legislation: the provisions on the supply of intelligence to the Minister, the President and government departments are unsatisfactory; the legislation does not deal with authority to task the intelligence services; it does not cover the dismissal or suspension of the Director-General of an intelligence service; and it does not provide for ministerial approval of intrusive operations.

The National Strategic Intelligence Act of 1994 should be amended to provide that the Minister must receive national strategic intelligence as well as intelligence relating to threats to the security of the Republic and its people. The Minister's powers in relation to intelligence reports should be covered in a ministerial directive approved by the Joint Standing Committee on Intelligence (JSCI).

The Act should provide that the intelligence structures may only supply intelligence to government departments with the Minister's approval. The

Act should provide that NIA, SASS and NICOC may only be tasked to gather and supply intelligence by the President, Cabinet, the Minister and the Coordinator of NICOC. The supply of intelligence to the President by NIA, SASS and NICOC, and access to the President by the heads of these bodies, should be regulated by legislation, regulations or a presidential directive. The rules should state that intelligence given to the President must also be given to the Minister.

The intelligence legislation should provide for disciplinary measures against, and the dismissal and suspension of, the heads of the intelligence structures.

There is an acute absence of ministerial regulations and directives. This is most problematic with respect to politically sensitive activities like intrusive operations, countermeasures and the identification of targets for investigation. Policies and rules on these matters that ought to have been determined by the Executive have instead been determined by the heads of the services.

The Minister should issue regulations on the conduct of intelligence and counter-intelligence operations; the supply of intelligence to the Minister, the Executive and government departments; authority for tasking the intelligence structures to gather intelligence; and disciplinary measures against, and the dismissal and suspension of, the heads of the intelligence structures.

The existing regulations and those issued by the Minister in the future should be published in the *Government Gazette*. Rules that must be kept confidential for operational reasons should be issued as directives and not regulations.

CHAPTER 5: THE INSPECTOR-GENERAL OF INTELLIGENCE

The Constitution states that legislation must provide for civilian monitoring of the activities of the intelligence services by an inspector who is appointed by the President and approved by a resolution of the National Assembly. The Intelligence Services Oversight Act of 1994 provides for the appointment and functions of the Inspector-General of Intelligence.

The Act should be amended so that the Inspector-General's mandate is confined to the ombuds role. This role entails monitoring compliance by the intelligence structures with the Constitution, legislation and policies; investigating complaints of abuse of power, misconduct and illegality by these structures; and certifying the reports submitted by the heads of the structures. The Inspector-General's mandate should not cover significant intelligence failures,

the efficiency and effectiveness of intelligence operations, and human resource complaints. The Inspector-General lacks the capacity to deal with all these functions and this may detract from adequate performance of the ombuds role.

The President, the Minister, the JSCI and/or Parliament should determine the most appropriate means of investigating significant intelligence failures on a case-by-case basis.

The ombuds role should be extended to cover the South African National Academy of Intelligence (SANAI). The Inspector-General should be empowered to assess whether the training conducted by SANAI is consistent with and helps to promote respect for constitutional rights and the rule of law. The Office of the Inspector-General of Intelligence (OIGI) does not have the resources to implement its mandate. It therefore undertakes its ombuds function at a minimum level of performance and with reduced scope. The budget of the OIGI should be increased substantially.

The OIGI should have an independent organisational status, allowing it to receive and manage its budget independently of NIA. The Inspector-General would remain functionally accountable to the JSCI but would be financially and administratively accountable to the Minister for the purposes of the Public Finance Management Act of 1999.

There is an urgent need for the Minister to issue regulations governing the Inspector-General's investigations, inspections and certification of the reports submitted by the heads of the services.

When undertaking investigations, the Inspector-General should not have the power to subpoena witnesses; he or she should be obliged to report criminal conduct by a member of an intelligence service to the police; the right to legal representation should apply where criminal charges might be laid against a member; and the Inspector-General should not be authorised to indemnify witnesses against prosecution.

Consultation with the Inspector-General should be mandatory when intelligence legislation, legislative amendments, ministerial regulations and operational policies are being drafted.

Once the relevant court proceedings have been concluded, the Minister should initiate an evaluation of the investigation undertaken by the Inspector-General during the intelligence crisis of 2005/6.

The OIGI should have a higher public profile. It should have a website that provides contact details and describes its functions, activities and findings.

CHAPTER 6: THE MANDATE OF NIA

Intelligence mandate

There are three major problems with NIA's intelligence mandate. First, the mandate is too broad and open to interpretation. The National Strategic Intelligence Act (hereafter "the Act") requires NIA to focus on threats and potential threats to the security of the Republic and its people; internal activities, factors and developments that are detrimental to national stability; and threats and potential threats to the constitutional order and the safety and well-being of the people of South Africa.

NIA has interpreted this mandate in so expansive a fashion as to encompass the thematic focus of virtually every state department. This is impractical and unnecessary, and it detracts from NIA's focus on serious criminal threats and the potential for violence.

Second, the terms 'security of the Republic and its people', 'national stability' and 'threats to the constitutional order' are imprecise and open to interpretation. NIA's mandate has in fact been reinterpreted three times since 1994 but the results of this process have not been subject to an open and vigorous parliamentary and public debate.

Third, the broad mandate and NIA's political intelligence function may have politicised the Agency and given rise to an inappropriate focus on political activities. The political intelligence function has entailed monitoring and reporting on transformation within government departments, on competition within and between political parties and on the impact of political policy decisions. This is very troubling given NIA's powers to operate secretly and infringe constitutional rights. Intelligence agencies in a democracy should not violate the rights of people who are behaving lawfully.

In light of the above, we support NIA's proposals that the concept of 'security threat' should be defined more clearly; that the Agency should have a narrower mandate; that the mandate should concentrate on serious crimes; and that the political intelligence function as currently conceived should be abandoned.

NIA should also abandon its focus on economic intelligence in support of national economic policy. There is no need for it to cover macro-economic and social issues, duplicating the work of experts within and outside of government.

NIA should rather be concerned with crimes that have an economic or financial character or a severe impact on the economy.

The Act should be amended so that NIA's intelligence mandate is not based on imprecise terms like threats to 'national stability' and the 'constitutional order'. Instead, the mandate should be defined with reference to large-scale violence, terrorism, sabotage, subversion, espionage, proliferation of weapons of mass destruction, drug trafficking, organised crime, corruption and specified financial crimes (hereafter "the designated threats"). The legislation should also state explicitly that security threats exclude lawful activities.

In relation to the designated threats, NIA should have the following functions: to predict, detect and analyse the threats; to gather intelligence on the plans, methods and motivation of persons and groups responsible for the threats; to discern patterns, trends and causes in relation to the threats; to forewarn and advise the Executive on the threats; to provide strategic intelligence to NICOC; and to contribute to law enforcement and preventive action by providing intelligence to the police and other government departments.

In order to fulfill these functions, NIA should continue to undertake non-intrusive monitoring of the political and socio-economic environment. Despite focusing on serious crimes, NIA's mandate would be completely different from that of the police. Whereas the police are responsible for law enforcement and criminal investigation leading to prosecution, the emphasis of the domestic intelligence agency should be on detection, analysis, prediction, prevention, forewarning and advice to the Executive.

Counter-intelligence mandate

In terms of the Act, NIA's counter-intelligence mandate entails four functions, two of which are clear and regulated: to protect intelligence and classified information, and to conduct security-screening operations. The other two functions – to impede and neutralise the effectiveness of foreign or hostile intelligence operations, and to counter subversion, treason, sabotage and terrorism – are not described precisely and are not regulated.

The absence of legal rules and executive policy on these countermeasures is extremely dangerous as it might lead to interference in politics and infringing rights without sufficient cause. The Act should define counter-measures more precisely and should regulate the use of these measures.

The Act should prohibit the intelligence services from disseminating false or misleading information and from interfering with lawful political and social activities in South Africa and other countries.

Departmental intelligence

The definition of departmental intelligence in the Act should be narrowed in line with the preceding proposals on narrowing NIA's intelligence mandate. The Minister should issue guidelines that regulate and expedite the provision of departmental intelligence.

A request for NIA to provide departmental intelligence must be made by the responsible minister in the case of a national department and by the provincial Premier in the case of a provincial department, and the request must be made to the Minister for Intelligence Services.

CHAPTER 7: INTRUSIVE OPERATIONS

Intrusive methods of investigation by the intelligence services, such as spying on people and tapping their phones, are a matter of great constitutional and political importance since they infringe the rights to privacy and dignity. They might also breach the political rights that are enshrined in the Constitution.

Because intrusive methods infringe rights, they are unconstitutional unless they are employed in terms of law of general application. Legislation currently permits the intelligence services to intercept communication and enter and search premises. Other intrusive methods – such as infiltration of an organisation, physical and electronic surveillance, and recruitment of an informant – are not regulated by legislation and are thus unconstitutional.

The Minister should introduce legislation that governs the use of all intrusive measures by the intelligence services. The legislation should be consistent with Constitutional Court decisions regarding infringements of the right to privacy and should therefore contain the following safeguards:

The use of intrusive measures should be limited to situations where there are reasonable grounds to believe that a) a serious criminal offence has been, is being or is likely to be committed; b) other investigative methods will not enable the intelligence services to obtain the necessary intelligence; and c) the

gathering of the intelligence is essential for the services to fulfill their functions as defined in law.

The intelligence services should be prohibited from using intrusive measures in relation to lawful activities unless these activities are reasonably believed to be linked to the commission of a serious offence. The use of intrusive measures should require the approval of the Minister.

The use of intrusive measures should require the authorisation of a judge. The legislation should prescribe the information that the applicant must present in writing and on oath or affirmation to the judge. The application must provide sufficient detail to enable the judge to determine whether the circumstances warrant resort to intrusive measures. Intrusive methods should only be permitted as a matter of last resort.

The intelligence services must delete within specified periods a) private information about a person who is not the subject of investigation where the information is acquired incidentally through the use of intrusive methods; b) private information about a targeted person that is unrelated to the commission or planning of a serious criminal offence; and c) all information about a targeted person or organisation if the investigation yields no evidence of the commission or planning of a serious offence.

Pending promulgation of the new legislation, the heads of the intelligence organisations should take immediate steps to ensure that their policies and procedures on the use of intrusive measures provide for ministerial approval and are aligned with the Constitution and relevant legislation. The Minister should request the Inspector-General to certify the revised policies and procedures in terms of their alignment with the Constitution and the law.

CHAPTER 8: INTERCEPTION OF COMMUNICATION AND THE NCC

NIA's policy on interception of communication is inconsistent with the Constitution and legislation. The policy states that the right to privacy is limited to citizens when in fact this right applies to everyone in South Africa.

The NCC appears to be engaged in signals monitoring that is unlawful and unconstitutional. This is because it fails to comply with the requirements of the Regulation of Interception of Communications and Provision of

Communication-Related Information Act of 2002 (hereafter "RICA"), which prohibits the interception of communication without judicial authorisation.

In June 2008 the Minister tabled legislation providing for the establishment and functions of the NCC; the legislation is intended to ensure the legality and constitutionality of the NCC's operations. The key function of the NCC is the collection and analysis of foreign signals, which include communication that emanates from outside the borders of South Africa or passes through or ends in South Africa.

The NCC Bill does not contain adequate safeguards to protect the right to privacy. It is therefore unlikely to satisfy the Constitutional Court, which has stressed the need for such safeguards to be included in legislation that allows for infringements of the right to privacy.

The Bill should state that the NCC is bound by RICA and may not intercept the communication of a targeted person without judicial authorisation.

The Bill should indicate which intelligence and law enforcement bodies are entitled to apply to the NCC for assistance with the interception of communication and should describe the information that must be contained in an application for signals monitoring.

The Bill should state that interception of communication is a method of last resort and may only occur where there are reasonable grounds to believe that a serious criminal offence has been, is being or is likely to be committed.

The Bill should provide for the discarding of personal information that is acquired in the course of intercepting communication where the information is unrelated to the commission of a serious criminal offence.

The legislation should cover the NCC's 'environmental scanning', which entails random monitoring of signals.

The intelligence services should take immediate steps to ensure that their policies on interception of communication provide for ministerial approval and are aligned with the Constitution and legislation. The Minister should request the Inspector-General to certify the revised policies.

CHAPTER 9: INTERNAL CONTROLS

The intelligence services have numerous internal controls that are intended to ensure adherence to the Constitution, legislation and policies. The controls reflect the professionalism of the services, which appreciate that misconduct

by their members is detrimental to the security of the country. Over the past decade the intelligence organisations have engaged in a continuous process of improving their control systems. This has intensified since the intelligence crisis of 2005/6, which exposed many gaps and weaknesses in the systems.

We support the proposals of the Legislative Review Task Team, established by the Minister in 2005, regarding the need for regulations and operational directives to further strengthen controls over intelligence operations.

The directives should specify the process for targeting in light of Cabinet's intelligence priorities; the criteria and procedures for authorising intrusive operations; the level of authority required to approve these operations; the level and system of supervision of operations; the procedures for dealing with incidental information; the details required for record-keeping; and the mechanisms for monitoring compliance and dealing with non-compliance.

We support the Task Team's proposal that the Minister should initiate an engagement with the Inspector-General and the JSCI to ensure more effective routine and ad hoc monitoring of compliance with ministerial and departmental prescripts on the conduct of operations.

Steps should be taken to ensure that the operational policies of the intelligence services interpret correctly and are properly aligned with the relevant constitutional and legislative provisions. This is currently a lack of alignment in a number of policies.

As an additional control measure, the intelligence services should establish internal clearance panels comprising senior officials who would assess applications to initiate intrusive operations.

We do not believe that the intelligence services are over-regulated or subject to too much oversight. However, efforts should be made to achieve greater rationalisation and co-ordination of oversight and review activities, provided that the solutions do not compromise the quality of control and oversight.

CHAPTER 10: FINANCIAL CONTROLS AND OVERSIGHT

The financial controls and oversight of the intelligence services are important for two reasons: the risk of abuse of funds for personal gain is high wherever money can be used for secret projects; and major acts of political misconduct by intelligence services usually require the use of organisational funds and other

resources. Effective control and oversight of these funds and assets might therefore help to prevent or detect misconduct.

The legislative framework governing the funds and financial controls and oversight of the intelligence services is generally sound. The Public Finance Management Act of 1999 and the Public Audit Act of 2004 reflect state-of-the- art principles of financial governance. They ensure that the heads of the intelligence services have a high level of accountability and a set of rigorous regulatory obligations regarding financial matters.

The Security Services Special Account Act of 1969 and the Secret Services Act of 1978, on the other hand, are relics of covert security funding in the apartheid era and should be repealed.

The budgets and financial reports of the intelligence services are reviewed by the JSCI, which reports to Parliament, but these documents are confidential and are not presented to Parliament. As a result, according to the National Treasury, the services are not directly accountable to Parliament for their budgets and spending. This is inconsistent with the Constitution, which states that national budgets must promote transparency and accountability.

We endorse the National Treasury's proposal that the intelligence services should have their own vote in respect of monies approved annually by Parliament and should present their annual budgets and financial reports to Parliament. They would not be expected to disclose information that would prejudice security or compromise intelligence operations.

The Auditor-General does not conduct an adequate audit of the intelligence services' expenditure and assets relating to covert operations. There is resistance to such scrutiny from sectors of the intelligence community and there is also a measure of self-restraint on the part of the Auditor-General's staff. This is a matter of great concern. We support the solution of using the Inspector-General to assist with the audit. The Minister should facilitate the finalisation of arrangements in this regard.

The Constitution states that the Auditor-General must submit audit reports to any legislature that has a direct interest in the audit and that all reports must be made public. However, the audit reports on the intelligence services are presented only to the JSCI and are classified documents. We support the Auditor-General's view that the reports should be presented to Parliament. In addition, the audit reports on the intelligence services for the past five years should be disclosed to Parliament. As permitted by law,

sensitive information can be withheld if deemed necessary by the Auditor-General or the Minister.

CHAPTER 11: INSTITUTIONAL CULTURE

The institutional culture of the intelligence services is as important as their internal rules because it is one of the key factors that determine whether intelligence officers abide by the rules or break them. By institutional culture we mean the widely shared or dominant values, attitudes and practices of the members of an organisation.

At the very least, intelligence officers must abide by the rules as a matter of obedient habit. Ideally, they should adhere to the rules because they consider ethical and lawful conduct to be an intrinsic component of professionalism and regard the constitutional and legislative constraints on organs of state not as burdensome impediments but as essential safeguards of democracy.

The institutional culture of the civilian intelligence community has a number of positive features:

Executive policy on the political norms governing the intelligence services is perfectly aligned with the Constitution and democratic principles. The Constitution, executive policies and operational directives insist that the intelligence services must be politically non-partisan. The operational directives of the intelligence services emphasise compliance with the Constitution and the law.

The Minister has introduced a civic education programme aimed at promoting respect for the law, democratic values and ethical conduct in the intelligence community.

We discern five negative features of the institutional culture of the civilian intelligence community. First, the ban on political interference and partisanship has been compromised by NIA's political intelligence focus, which has drawn the Agency into the arena of party politics.

The intelligence legislation should make it a criminal offence for intelligence officers to act in a politically partisan manner or interfere in lawful political activities and for other persons to request or instruct intelligence officers to act in this manner.

Second, there are management and labour relations problems that impinge on the rights of staff, undermine morale and might consequently impair the efficacy of control systems. According to the Inspector-General, the problems

include abuse of authority; unfair labour practice; the limitation of labour rights; the absence of an independent dispute resolution mechanism; and manifestly illegal instructions that might be obeyed because of fear or threats.

In consultation with the members of the intelligence organisations, the Minister should find an arrangement that is consistent with the Constitution and covers labour rights to the satisfaction of all the parties. The Minister should also ask the Intelligence Services Council on Conditions of Service to make proposals on improving the mechanisms for addressing grievances and disputes, and should ensure that the independent appeals board provided for in the 2003 ministerial regulations is set up promptly.

Third, some senior officials believe that it is legitimate to break the rules when dealing with serious security threats. This position is unconstitutional, flouts the rule of law and negates efforts to develop an institutional culture of respect for the law. It is subversive of democracy and executive policy.

It is essential that there be unanimous support for the position of senior officials who advocate a policy of zero-tolerance of misconduct and for the Minister's insistence on adherence to the principle of legality. The heads of the intelligence organisations must pursue a zero-tolerance approach to misconduct and illegality, and the Minister, the Inspector-General and the JSCI should ensure adherence to this policy.

Fourth, there is a lack of adequate legal expertise in the intelligence community. As a result, internal policies and memoranda mistakenly ignore or misinterpret the Constitution and legislation. Full compliance with the law is obviously unlikely in these circumstances. The Minister and the heads of the services should take steps to enhance the quality of legal advice.

Fifth, there is an absence of familiarity with those aspects of international law that have a bearing on intelligence operations. The Minister should request the Inspector-General or SANAI to do a survey of international law and propose any amendments to domestic laws and policies that are necessary. The relevant aspects of international law should be included in the civic education curricula.

CHAPTER 12: TRANSPARENCY, SECRECY AND PROVISION OF INFORMATION

The Constitution provides for the right of access to information and emphasises the principles of transparency and openness as fundamental tenets of

governance. The right of access to information lies at the heart of democratic accountability and an open and free society. Secrecy should therefore be regarded as an exception, which in every case demands a convincing justification. The justification should not rest on the broad notion of 'national security' but should instead specify the significant harm that disclosure might cause to the lives of individuals, the intelligence organisations, the state or the country as a whole.

The intelligence organisations have not shed sufficiently the apartheid-era security obsession with secrecy. Their emphasis is on secrecy with some exceptions when it should be on openness with some exceptions.

The following steps would enhance openness in the interests of democracy without undermining security or compromising intelligence operations:

The National Intelligence Priorities approved annually by Cabinet should be subject to parliamentary consultation and debate. Information that is extremely sensitive could be withheld.

All ministerial regulations on intelligence should be promulgated in the *Government Gazette*, and the existing regulations that are secret should be published in this manner.

Once finalised, the draft regulations on the conduct of intelligence operations should be tabled for public comment. Executive policy on intelligence operations should be in the public domain.

The intelligence services should put their annual reports on their websites and the Minister should table these reports in Parliament. The services should also publish periodic security assessments on their websites.

As proposed above, the annual budgets and financial reports of the intelligence services and the audit reports on the services should be tabled in Parliament. Information that would endanger security or compromise intelligence operations could be withheld.

NICOC and the OIGI should establish websites that include detailed information about their respective functions and activities. All the intelligence bodies should have on their websites a section that assists members of the public who want to request information in terms of the Promotion of Access to Information Act of 2000. The intelligence services should produce the information manuals required by this Act.

The intelligence services would benefit from greater provision of information. Excessive secrecy gives rise to suspicion and fear and this reduces public

support for the services. In a democracy, unlike a police state, the services must rely on public co-operation rather than coercion to be successful. The publication of greater information would raise their profile in a positive way, improve public co-operation and thereby enhance their effectiveness.