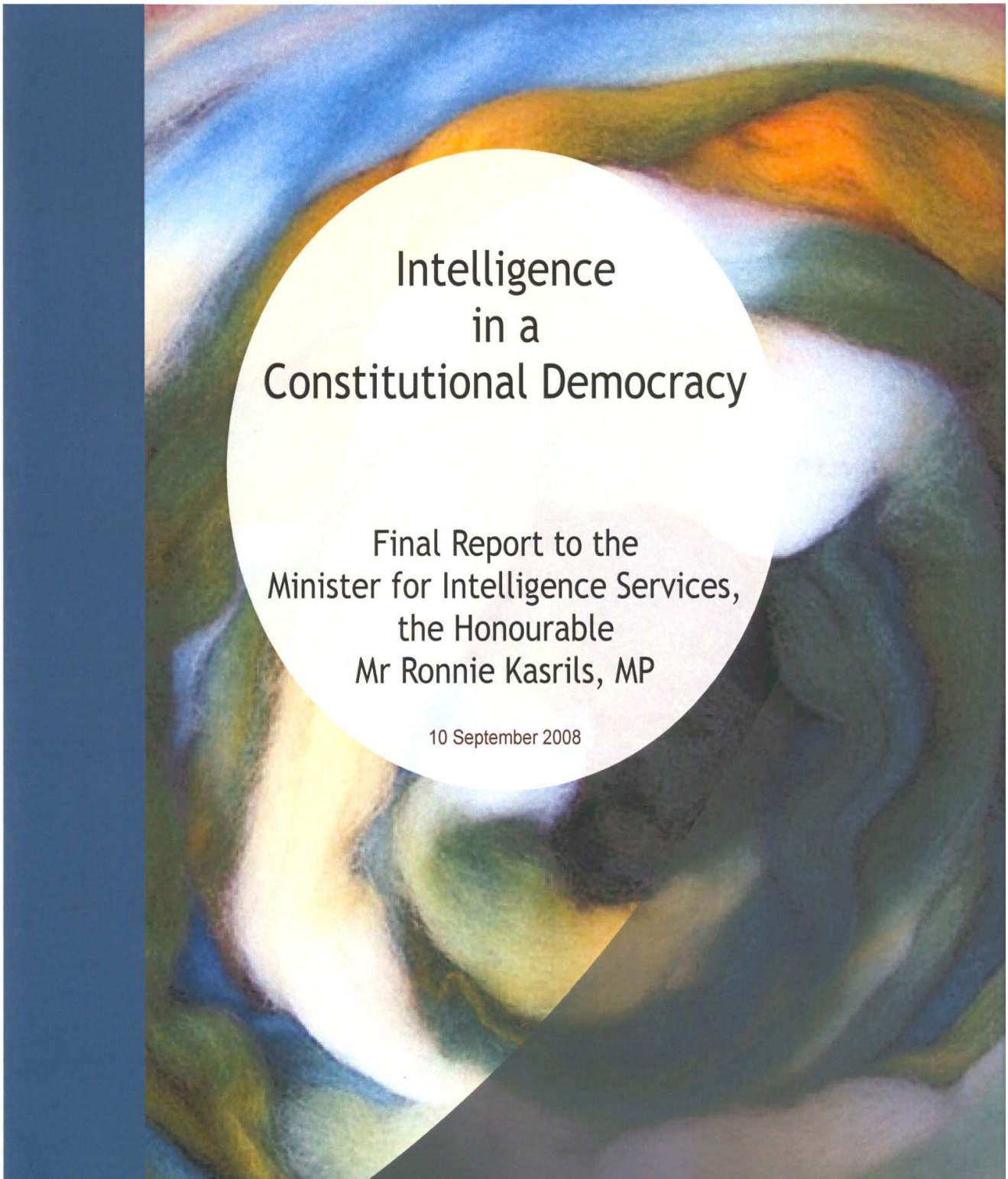
MINISTERIAL REVIEW COMMISSION ON INTELLIGENCE
REPUBLIC OF SOUTH AFRICA



# Intelligence in a Constitutional Democracy

## Final Report to the Minister for Intelligence Services, the Honourable Mr Ronnie Kasrils, MP

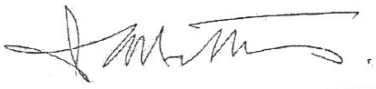
10 September 2008

# INTELLIGENCE IN A CONSTITUTIONAL DEMOCRACY

## FINAL REPORT
## TO THE MINISTER FOR INTELLIGENCE SERVICES, THE HONOURABLE MR RONNIE KASRILS, MP

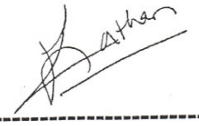
## MINISTERIAL REVIEW COMMISSION ON INTELLIGENCE

## 10 SEPTEMBER 2008



Mr Joe Matthews (Chairperson)

Dr Frene Ginwala



Mr Laurie Nathan

**TABLE OF CONTENTS**

## FOREWORD BY JOE MATTHEWS, CHAIRPERSON OF THE MINISTERIAL REVIEW COMMISSION ON INTELLIGENCE

From time immemorial, nations, governments and communities have relied on intelligence as an essential guide to statecraft. It is on record, for example, that the Persian Empire, the Moguls of India and the City State of Venice utilised intelligence in a systematic manner as an essential feature of government. They recorded their concepts of intelligence in texts that are available for study today.

It is evident from this history that intelligence techniques have been used in pursuit of different objectives and that statecraft and its instruments are always a reflection of the culture and value system of a given society.

Some nations believed in conquest and the creation of empires that exploited the resources of their subjects. Others used intelligence as an instrument in pursuit of wars and military supremacy. Still others sought dominance in trade and wealth creation for themselves and their peoples.

With the emergence of modern democratic states, a fundamental change has occurred in the nature of intelligence as an instrument of government. Whereas previously the emphasis was on the security of the state and the survival of the regime, now there is a strong emphasis on human security and human rights and freedoms.

In our country the Constitution is the supreme law and it enshrines the principles, culture and values of our democratic state and people. Our constitutional arrangements are not confined to setting out the distribution of power and the means for the peaceful settlement of disputes. The Constitution also reflects the basic values of our democracy and the economic and social principles for ensuring a cultured existence for all our people.

Unlike many other jurisdictions, our Constitution provides expressly for the setting up of intelligence services as part of the security system in the country. There are also statutes that describe in detail the role and functions of the intelligence services. Whilst operational techniques of covert collection of information are secret, the rest of our intelligence activities should be open and above board. This reflects confidence that our objectives and policies are ethical, honourable and in accordance with fundamental human rights and freedoms.

Our intelligence and other security services are not oppressors of the people but are protectors of their security and well-being. Hence our services can count on the full support of the people. That is not the case in many other countries, where the security services are feared and even hated.

What, then, are the ideal intelligence services we are striving for? We envisage intelligence services that are fully conscious and proud of our democratic and constitutional foundations. We expect our intelligence operatives, researchers and analysts to be highly trained and sophisticated. The main function of our services should be the collection of true and relevant information that can serve as a basis for first class decision-making on security.

Our intelligence services must be seen to be collectors of information both inside the country and abroad, using human resources and the latest modern technology. They must rely on brains rather than brawn. They must be effective and efficient and deliver quality products superior to those ordinarily available.

Our intelligence services are not and must never be another police service with powers of arrest. It is true that the modern trend is to use the special methods of intelligence to assist the police in the realm of combating serious international crime syndicates, but essentially the services must aim at providing information for decision-makers rather than prosecution of criminals.

The intelligence services have been given special powers but these powers must be exercised in accordance with legislation, regulations, guidelines and rules. In any democracy it is essential that intelligence services behave in an ethical and lawful manner. In South Africa these matters are considered so important that they governed by the Constitution itself.

Intelligence services have the particular misfortune of going unnoticed and unappreciated when they are successful. We wish to record our thanks to and respect for the South African intelligence services and all their members, who make a significant contribution to the security of our country and people.

## EXECUTIVE SUMMARY

### 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 Co-ordinating 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 fulfil 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 fulfil 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 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". 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 Co-ordinator 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 fulfil 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 fulfil 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.

**LIST OF ACRONYMS**

| | |
|---|---|
| CEP | Civic Education Programme for the intelligence services |
| COMSEC | Electronic Communications Security (Pty) Ltd |
| JSCI | Joint Standing Committee on Intelligence |
| NCC | National Communications Centre |
| NIA | National Intelligence Agency |
| NICOC | National Intelligence Co-ordinating Committee |
| OIC | The Office for Interception Centres |
| OIGI | Office of the Inspector-General of Intelligence |
| PAIA | Promotion of Access to Information Act No. 2 of 2000 |
| RICA | Regulation of Interception of Communications and Provision of Communication-Related Information Act No. 70 of 2002 |
| SAHRC | South African Human Rights Commission |
| SANAI | South African National Academy of Intelligence |
| SANDF | South African National Defence Force |
| SAPS | South African Police Service |
| SASS | South African Secret Service |

## CHAPTER 1: INTRODUCTION

### 1.1 Introduction

The Minister for Intelligence Services, Mr Ronnie Kasrils MP, established the Ministerial Review Commission on Intelligence in August 2006 and finalised its terms of reference on 1 November 2006 (Appendix A). On that date the Minister announced the launch of the Commission at a press conference in Cape Town.

The Commission comprises Mr Joe Matthews (Chairperson), Dr Frene Ginwala and Mr Laurie Nathan.[1]

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

This Chapter covers the following topics:

- The context of the establishment of the Commission (Section 1.2).
- The Commission's terms of reference (Section 1.3).
- The content and style of the Report (Section 1.4).
- The activities and methods of the Commission (Section 1.5).
- An overview of the civilian intelligence community (Section 1.6).
- Acknowledgements (Section 1.7).

[1] The bios of the Commissioners can be found on the Commission's website at www.intelligence.gov.za/commission.

## 1.2 Context of the Commission's Establishment

In 2005 and 2006 South Africa was rocked by a political crisis involving the National Intelligence Agency (NIA). Indications of possible misconduct emerged when a prominent businessman and political figure complained to Minister Kasrils that he was under surveillance by NIA. The Minister requested the Inspector-General of Intelligence to investigate the matter. The Inspector-General found, among other things, that NIA had conducted illegal surveillance for political reasons and that the Director-General of NIA had unlawfully ordered the interception of the communication of ruling party and opposition politicians, some of whom were members of Parliament.[2] The Director-General and two other officials were suspended and thereafter dismissed. These dramatic events provoked considerable consternation among political parties and members of the public.

The crisis led to the Minister's decision to set up the Commission. Speaking at the launch of the Commission, Minister Kasrils made the following remarks:

> I indicated in my Budget Vote speech that it was necessary to use this lamentable episode at NIA to undertake fundamental reforms aimed at preventing such abuses in the future. To do so, we need to review legislation and strengthen regulations, operational procedures and control measures where necessary. I also pointed out the need to attend to the perfidious mentality that enabled these dirty tricks to take place and most importantly, that such reforms be placed in the public domain so as to rebuild public confidence and trust.[3]

---

[2] Office of the Inspector-General of Intelligence, 'Executive Summary of the Final Report on the Findings of an Investigation into the Legality of the Surveillance Operations Carried out by the NIA on Mr S Macozoma. Extended Terms of Reference Report on the Authenticity of the Allegedly Intercepted E-Mails', media briefing, 23 March 2006, available at www.intelligence.gov.za/OversightControl/IG%20Exec%20Summary%2023%20Mar%2006.doc.

[3] Minister Ronnie Kasrils, 'Launch of Ministerial Review Commission on Intelligence by the Minister for Intelligence Services', Cape Town, 1 November 2006.

The intelligence crisis of 2005/6 was thus the catalyst for the formation of the Commission but it was not the focus of our review. As discussed in the following section, we were mandated to identify ways of tightening controls over the civilian intelligence organisations in order to prevent future incidents of misconduct and illegality.

### 1.3 Terms of Reference

Our terms of reference state that "the aim of the Review is 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".[4]

The review was expected to cover the following structures:

- NIA
- The South African Secret Service (SASS)
- The National Intelligence Co-ordinating Committee (NICOC)
- The National Communications Centre (NCC)
- The Office for Interception Centres (OIC)
- Electronic Communications Security (Pty) Ltd (COMSEC).

We were also directed to address the following topics:

- Executive control of the intelligence services
- Control mechanisms relating to the intelligence services' operations
- Control over intrusive methods of investigation
- Political and economic intelligence
- Political non-partisanship of the intelligence services
- The balance between secrecy and transparency
- Controls over the funding of covert operations.

[4] The Commission's terms of reference are attached as Appendix A.

In order to achieve its aim, the Commission was empowered to undertake the following methods of inquiry:

- Review the legislation, regulations and policies governing the intelligence services.

- Review the reports of the Legislative Review Task Team.[5]

- Review the directives on intrusive methods of collection and the conduct of surveillance.

- Consider any other reports submitted to the Commission by the Minister.

- Invite written or oral submissions from interested parties.

- Invite submissions from the intelligence services.

- Hold public consultations at which members of the public and interested parties can make submissions to the Commission.

- Undertake comparative study of good practice in the governance of intelligence services in other countries.

- Any other methods that the Commission deems appropriate.

The Commission was expected to submit a public report to the Minister by the end of 2007. Following the illness of our Chairperson for several months, the Minister agreed to extend this deadline to the end of July 2008.

Our terms of reference state that the Commission shall be independent and that no person or body may do anything to undermine its independence or

[5] We explain the Legislative Review Task Team in Section 1.6.3.

seek to influence the Commissioners in an improper manner. We did not experience any interference with our work.

### 1.4 Content and Style of Report

Our terms of reference have shaped the content and style of the Report in three ways. First, the terms of reference identified the organisations that fell within our focus and, by implication, the organisations that lay outside our scope. The latter included the intelligence division of the South African Police Service (SAPS), the intelligence division of the South African National Defence Force (SANDF) and the National Security Council, which advises the President. We do not discuss these organisations in the Report.

Also excluded from our ambit was an evaluation of the activities of the Joint Standing Committee on Intelligence (JSCI), the parliamentary committee responsible for oversight of the intelligence organisations. At the time at which our terms of reference were being finalised, the Minister and the JSCI agreed that it would not be appropriate for a member of the Executive to commission a review of the work of a parliamentary committee.

Second, our terms of reference have shaped the themes and priorities of the Report. As required by our mandate, we have concentrated on ensuring that the civilian intelligence structures and their activities, controls, policies and governing legislation and regulations are properly aligned to constitutional principles and provisions. Consequently, we have paid more attention to certain types of intelligence activity and to certain of the civilian intelligence bodies than to others.

There are a number of important topics regarding the intelligence community that lie outside our core focus and are not examined in the Report. These topics include the quality and methodology of the analysis and forewarning undertaken by the civilian intelligence structures; the technical training and

skills of these officials; and the co-ordination and sharing of intelligence among the various intelligence bodies. We have not examined the issue of rendition because the Minister for Intelligence Services and the civilian intelligence organisations do not have jurisdiction over this issue.[6] We also reiterate that our job was not to uncover or investigate misconduct but rather to buttress controls in order to minimise the potential for misconduct.

Third, our terms of reference require us to produce a public report with an emphasis on practical recommendations. We have therefore avoided lengthy historical, comparative and philosophical discussions on intelligence and have endeavoured to make realistic proposals backed up by convincing motivations. Since the Report will become a public document, we have written it in a style that we hope will be accessible and informative to an audience beyond the intelligence community.

In the course of the Report we discuss and quote from classified intelligence policies and reports. We could not otherwise have described the policies under review and provided clear findings and recommendations. Public disclosure of the classified information required the authorisation of the Minister for Intelligence Services, who decided that one set of quotes relating to intelligence methods should be withheld from the public version of the Report for security reasons. Subject to the removal of these quotes, the Minister authorised disclosure of the excerpts from the classified material.

## 1.5 Activities and Methods of the Commission

### *1.5.1 Overview*

Our work proceeded in three phases. The first phase entailed reading the intelligence legislation, meeting the heads of the intelligence organisations and reviewing their submissions and operational policies. In the second

[6] Letter to the Commission from Minister Kasrils, 31 August 2007.

phase we had follow-up sessions with some of these organisations and met with other government bodies. We also did research on intelligence controls internationally and prepared informal discussion papers with provisional observations and conclusions. In the third phase we wrote the chapters for the Report and, as explained below, provided the Minister with comment on draft legislation.

On 7 August 2008 we presented an earlier version of the Report to the Minister. After reviewing it, he commented positively on the document but also indicated his disagreement with certain points of fact and interpretation. He asked us to consider amending these points. In some cases we found the Minister's comments persuasive and we amended the Report accordingly. In other instances we felt that our observations and conclusions were justified. As noted in Section 1.4, on security grounds the Minister asked the Commission to exclude from the public version of the Report a set of quotes from a classified intelligence document.

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

### *1.5.2 Meetings with the Joint Standing Committee on Intelligence*

We requested a meeting with the JSCI and met with the Committee on 19 September 2007 and 29 February 2008. The aims were to brief the Committee on our activities, draw on its knowledge and experience and provide its members with an opportunity to put their views to us. The meetings were extremely beneficial to the Commission.

Members of the JSCI supported the need for greater public debate on intelligence and said that the Report could be used to stimulate such debate. They also encouraged us to consult the President and the Auditor-General.

### *1.5.3 Meeting with the President*

We requested a meeting with President Mbeki in order to hear his comments and recommendations on the topics covered by our terms of reference and on the following issues in particular:

- The notion that the President is the 'primary client' of the intelligence services.

- The relationship between the President, the Minister for Intelligence Services and the heads of the intelligence services, and procedures for supplying intelligence to the Executive.

- Means of enhancing control over the intelligence services so as to prevent abuse of power.

The meeting with President Mbeki and Dr Frank Chikane, Director-General in the Presidency, took place on 10 May 2008. The discussion was of great value to the Commission in drafting Chapter 4 on ministerial control and responsibility.

### *1.5.4 Interaction with the Minister*

We had several meetings with Minister Kasrils at which we informed him of our progress and sought information on certain issues. We gave him draft chapters as we prepared them and submitted two activity reports to him.[7]

In March 2008 the Minister asked us to comment on the Protection of Information Bill. We drafted a detailed memorandum, which was published on

[7] Ministerial Review Commission on Intelligence, 'Report to the Minister for Intelligence Services', I July 2007; and Ministerial Review Commission on Intelligence, 'Report to the Minister for Intelligence Services', 31 January 2008.

the website of the Ministry for Intelligence Services.[8] When the Protection of Information Bill (B28-2008) was presented to Parliament, the Ad Hoc Committee on Intelligence in the National Assembly issued a call for public submissions. After consulting the Minister we made a submission to the Committee.[9] We discuss the Bill in Chapter 12 of the Report.

We also prepared for the Minister a memorandum on the draft bills that provide for the establishment and functions of the National Communications Centre (NCC).[10] Since the NCC intercepts private communication and thereby infringes the constitutional right to privacy, we solicited a legal opinion from an advocate in private practice.[11] Following the tabling of the draft legislation in June 2008,[12] we made a submission to the Ad Hoc Committee on Intelligence in the National Assembly.[13] The NCC and the draft legislation are discussed in Chapter 8.

### *1.5.5 Interaction with the intelligence organisations*

The Commission met with the heads of the following bodies: NIA; SASS; NICOC; the NCC; the OIC; COMSEC; the Office of the Inspector-General of Intelligence; the South African National Academy of Intelligence (SANAI); and the Task Team on the Review of Intelligence-Related Legislation, Regulation and Policies. In most instances the heads of the organisations were accompanied by senior officials. The proceedings were recorded.

---

[8] Ministerial Review Commission on Intelligence, 'Memorandum on the Protection of Information Bill', submitted to the Minister for Intelligence Services, 31 March 2008.
[9] Ministerial Review Commission on Intelligence, 'Revised Submission on the Protection of Information Bill', submitted to the Ad Hoc Committee on Intelligence in the National Assembly, 20 July 2008, available at www.intelligence.gov.za/commission.
[10] Ministerial Review Commission on Intelligence, 'Memorandum on the NCC and Draft NCC Legislation', submitted to the Minister for Intelligence Services, February 2008.
[11] L. Nkosi-Thomas, 'Legal Opinion', commissioned by the Ministerial Review Commission on Intelligence, 4 October 2007.
[12] National Strategic Intelligence Amendment Bill [B 38-2008] and Intelligence Services Amendment Bill [B 37-2008].
[13] Ministerial Review Commission on Intelligence, 'Submission on the National Strategic Intelligence Amendment Bill [B 38-2008]', submitted to the Ad Hoc Committee on Intelligence in the National Assembly, 10 July 2008, available at www.intelligence.gov.za/commission.

The intelligence organisations made written submissions on their functions and on the topics covered by our terms of reference. We also received the operational policies of NIA, SASS and the NCC.

After the initial meetings the Commission wrote to several of the organisations asking for further information and documentation. We had follow-up meetings with NIA and the Inspector-General of Intelligence.

The Secretariat of the Commission, comprising staff from the Ministry for Intelligence Services, wrote a memorandum on the role of the Ministry and prepared a paper on international experience regarding intelligence reforms. They gave us local and foreign court judgements, academic articles on intelligence and numerous background documents.

*1.5.6 Submissions from other bodies*

In April 2007 the Commission placed adverts in the print media and on radio, calling for submissions from the public. The Chairperson also wrote letters inviting submissions from government departments, Chapter 9 institutions, universities and non-governmental organisations.

We received twenty submissions from non-governmental organisations and members of the public (Appendix B). Two of the submissions were from former members of the intelligence services. A former head of one of the services made an oral presentation to the Commission. In our assessment there was not a sufficient number of high quality inputs from non-governmental organisations to warrant the public hearings we had planned to convene and the hearings were cancelled.

Submissions were made by the Ministry of Public Service and Administration, the National Treasury and the Office of the Auditor-General. We had meetings with senior members of the National Treasury, an official in the

Presidency and the Auditor-General's staff who are responsible for the audits of NIA and SASS.

With the consent of Minister Kasrils, the Chairperson wrote a letter to members of the intelligence community inviting them to make submissions. The letter was placed on the intelligence intranet in May 2007. We did not receive any inputs from individuals but the Staff Council in the Intelligence Services made a submission.

### *1.5.7 Website*

The Commission created a website to stimulate debate on intelligence and publicise its terms of reference (www.intelligence.gov.za/commission). We added to the website our submissions to the Ad Hoc Committee on Intelligence in the National Assembly, as well as the submissions received from the South African Human Rights Commission, the South African National Editors' Forum, the Institute for Security Studies, the South African History Archives and the Open Democracy Advice Centre. The submission from the Institute for Security Studies provided a comprehensive perspective on many of the topics covered by our terms of reference.

## 1.6 Overview of the Civilian Intelligence Community

### *1.6.1 Constitutional provisions*

The Constitution of the Republic of South Africa of 1996 contains the following provisions on the establishment and control of intelligence services:

- Any intelligence service other than an intelligence division of the defence force or police service may be established only by the President, as head of the national executive, and only in terms of national legislation.[14]

- The President as head of the national executive must appoint a woman or a man as head of each intelligence service established in terms of sub-section 209(1) of the Constitution, and must either assume political responsibility for the control and direction of any of those services, or designate a member of the Cabinet to assume that responsibility.[15]

- National legislation must regulate the objects, powers and functions of the intelligence services, including any intelligence division of the defence force or police service, and must provide for a) the co-ordination of all the intelligence services; and b) civilian monitoring of the activities of those services by an inspector appointed by the President, as head of the national executive, and approved by a resolution adopted by the National Assembly with a supporting vote of at least two thirds of its members.[16]

In Chapter 2 and elsewhere in this Report we discuss other provisions of the Constitution that impact on the intelligence services and their activities.

### *1.6.2 Intelligence legislation*

The main intelligence legislation is as follows:

- The National Strategic Intelligence Act No. 39 of 1994, which defines the functions of NIA and SASS and the intelligence functions of the SAPS and the SANDF; provides for the functions of other state departments with reference to national security intelligence; establishes and defines the functions of NICOC; provides for the appointment and functions of a Co-

[14] Section 209(1) of the Constitution.
[15] Section 209(2) of the Constitution.
[16] Section 210 of the Constitution.

ordinator for Intelligence as the chairperson of NICOC; and defines the functions of the Minister for Intelligence Services.

- The Intelligence Services Act No. 65 of 2002, which regulates the establishment, composition, administration, organisation and control of NIA, SASS and SANAI; provides for the powers and responsibilities of the heads of these organisations; specifies the powers and duties of the members of the organisations; establishes and regulates the Intelligence Services Council on Conditions of Service; and provides for the general powers of the Minister for Intelligence Services.

- The Intelligence Services Oversight Act No. 40 of 1994, which provides for the establishment of the JSCI and defines its functions; and provides for the appointment of an Inspector-General of Intelligence and defines the functions of this official.

*1.6.3 Civilian intelligence organisations*

The negotiations that gave birth to democracy in South Africa in 1994 led to the amalgamation of a range of disparate intelligence organisations, including the National Intelligence Service of the minority government; the Department of Intelligence and Security of the African National Congress; the Pan Africanist Security Service of the Pan Africanist Congress; and the intelligence structures of the homeland governments of Bophuthatswana, Ciskei, Venda and the Transkei.

We describe below the main office-bearers, officials and bodies that comprise the civilian intelligence community.

- The Minister for Intelligence Services is appointed by the President in terms of section 209(2) of the Constitution and must exercise political responsibility for the control and direction of the civilian intelligence

services (www.intelligence.gov.za).[17] The Minister is supported by ministerial staff.

- The Joint Standing Committee on Intelligence (JSCI) is responsible for oversight of the intelligence and counter-intelligence functions of NIA and SASS and the administration, financial management and expenditure of NIA, SASS, the OIC, COMSEC and SANAI.[18] The JSCI's functions include consideration of the financial statements of the intelligence organisations, ministerial reports on their budgets and reports from the Inspector-General of Intelligence, the Auditor-General and the judge responsible for approving the interception of communication by the intelligence services.[19] The Committee also considers and makes recommendations on intelligence legislation and regulations.[20] The JSCI must report to Parliament on the performance of its functions.[21] The legislation specifies the basis on which political parties are represented on the Committee.[22]

- The Inspector-General of Intelligence is appointed by the President subject to the approval of the National Assembly.[23] He or she is accountable to the JSCI for the overall functioning of his or her office.[24] The Inspector-General must monitor compliance by the intelligence organisations with the Constitution, legislation and policies; investigate complaints against these organisations by members of the organisations, members of the public and the JSCI; and certify annual reports prepared by the heads of the intelligence services.[25]

---

[17] The powers and functions of the Minister are discussed in Chapter 4.
[18] Section 2(1) of the Intelligence Services Oversight Act.
[19] Section 3 of the Intelligence Services Oversight Act.
[20] Section 3 of the Intelligence Services Oversight Act.
[21] Section 2(1) of the Intelligence Services Oversight Act.
[22] Sections 2(2) - 2(5) of the Intelligence Services Oversight Act. In Section 4.8.1 of the Report we describe the relationship between the JSCI and the Minister for Intelligence Services.
[23] Section 210 of the Constitution and section 7(1) of the Intelligence Services Oversight Act.
[24] Section 7(6) of the Intelligence Services Act.
[25] Sections 3(f) and 7(7) of the Intelligence Services Act. The mandate and functions of the Inspector-General are discussed in Chapter 5.

- The National Intelligence Agency (NIA) is responsible for domestic intelligence (www.nia.gov.za). NIA's functions include gathering, correlating, evaluating and analysing domestic intelligence in order to identify any threat or potential threat to the security of the Republic or its people and supplying intelligence regarding any such threat to NICOC.[26] Domestic intelligence means "intelligence on any internal activity, factor or development which is detrimental to the national stability of the Republic, as well as threats or potential threats to the constitutional order of the Republic and the safety and well-being of its people".[27] NIA also has a counter-intelligence mandate.[28]

- The South African Secret Service (SASS) is responsible for foreign intelligence (www.sass.gov.za). SASS's functions include gathering, correlating, evaluating and analysing foreign intelligence, excluding foreign military intelligence, in order to identify any threat or potential threat to the security of the Republic or its people, and supplying intelligence relating to such threats to NICOC.[29] Foreign intelligence means "intelligence on any external threat or potential threat to the national interests of the Republic and its people, and intelligence regarding opportunities relevant to the protection and promotion of such national interests…".[30]

- The National Communications Centre (NCC) is government's national facility for intercepting and collecting electronic signals. Its clients are NIA, SASS, the SAPS and the Financial Intelligence Centre. The NCC is part of NIA but in June 2008 legislation was tabled providing for its separate establishment as an intelligence service under the Intelligence Services Act.[31]

---

[26] Section 2(1)(a) of the National Strategic Intelligence Act of 1994.
[27] Section 1 of the National Strategic Intelligence Act.
[28] NIA's mandate is discussed in Chapter 6.
[29] Section 2(2)(a) of the National Strategic Intelligence Act.
[30] Section 1 of the National Strategic Intelligence Act.
[31] National Strategic Intelligence Amendment Bill [B38-2008] and Intelligence Services Amendment Bill [B37-2008]. We discuss the NCC in Chapter 8.

- The National Intelligence Co-ordinating Committee (NICOC) comprises the Co-ordinator for Intelligence, who is appointed by the President, and the heads of the other national intelligence structures.[32] The 'national intelligence structures' are NICOC, NIA, SASS and the intelligence divisions of the SAPS and the SANDF.[33] NICOC's functions include the following: co-ordinate the intelligence supplied to it by the national intelligence structures; interpret such intelligence for use by the state and the Cabinet in order to detect and identify any threat or potential threat to the national security of the Republic and protect and promote the national interests of the Republic; co-ordinate and prioritise intelligence activities within the national intelligence structures; prepare and interpret intelligence estimates; and make recommendations to Cabinet on intelligence priorities.[34] NICOC does not have an operational intelligence mandate.

- The Office for Interception Centres (OIC) was established in terms of the Regulation of Interception of Communications and Provision of Communication-Related Information Act No. 70 of 2002. The OIC reports to the Minister for Intelligence Services. It provides a centralised interception service for law enforcement agencies and intelligence organisations that have received judicial authorisation to intercept private communication (www.oic.gov.za).[35]

- Electronic Communications Security Pty Ltd (COMSEC) ensures that the electronic communication infrastructure and systems of organs of state are protected and secure (http://e-comsec-com.win7.wadns.net/). The state is the sole shareholder of COMSEC and the responsible minister is the Minister for Intelligence Services.

[32] Section 4(1) of the National Strategic Intelligence Act.
[33] Section 1 of the National Strategic Intelligence Act.
[34] Section 4(2) of the National Strategic Intelligence Act.
[35] Interception of communication by the intelligence organisations is discussed in Chapter 8.

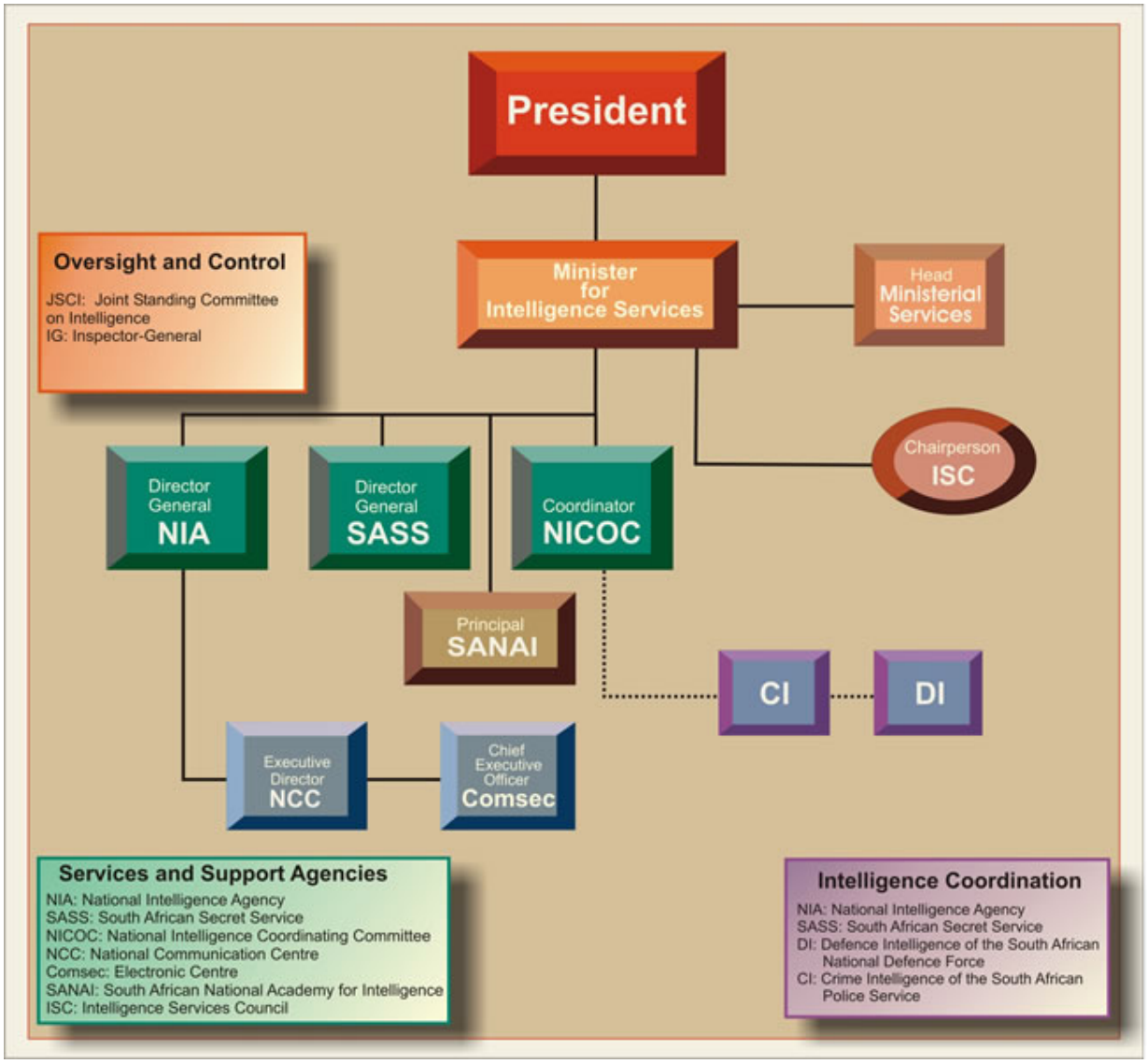
- The South African National Academy of Intelligence provides training to members of the intelligence community. The management and administration of the Academy fall under the control of the Minister for Intelligence Services.[36]

- The Intelligence Services Council on Conditions of Service was established under the Intelligence Services Act to make recommendations to the Minister on policies regarding conditions of service, salaries and benefits and other human resource matters and to promote the effective and efficient implementation of human resource policies.[37]

In 2005 Minister Kasrils established the Task Team on the Review of Intelligence-Related Legislation, Regulation and Policies. Headed by the NICOC Co-ordinator, it included officials from the civilian intelligence bodies. The Task Team's mandate was to provide the Minister with an integrated assessment and set of recommendations on a range of legislative and policy issues that had arisen from various commissions, task teams and ministerial decisions and directives over the preceding two years. After the onset of the intelligence crisis of 2005/6, the Minister instructed the Task Team to pay special attention to the operational policies of NIA, SASS and the NCC.[38]

On the following page we reproduce from the website of the Ministry for Intelligence Services an organogram of the civilian intelligence community in South Africa.

[36] Section 5(1) of the Intelligence Services Act.
[37] Section 22(3) of the Intelligence Services Act.
[38] We discuss the Task Team's findings and recommendations in Chapter 9 and elsewhere in the Report.




Organogram of the Civilian Intelligence Community in South Africa

## 1.7 Acknowledgements

The Commission was ably assisted by a Secretariat comprising staff from the Ministry for Intelligence Services. The Secretariat was headed initially by Dr Sandy Africa and subsequently by Adv Lucia Mtshali. The other members of the Secretariat were Ms Kerenza Millard and Ms Thembani Phiri. Dr Africa also provided research support to the Commission. We received administrative support from Mr Mxolisi Dlamini, Head of Ministerial Services.

We are very grateful to the above-mentioned people for their assistance. We also express our appreciation to Minister Kasrils for his support and enthusiasm and to all those who made submissions to the Commission and addressed our requests for information.

## CHAPTER 2: KEY PRINCIPLES AND PERSPECTIVES ON SECURITY AND INTELLIGENCE

### 2.1 Introduction

In this Chapter we present our perspective on intelligence and national security. This perspective has informed all aspects of our review and constitutes the normative basis for the commentary and recommendations in the Report. The perspective is drawn principally from South Africa's Constitution, which includes provisions on security and intelligence and contains a Bill of Rights that is binding on all organs of state.

The Constitution asserts that the values on which our democratic state is founded include human dignity, the achievement of equality, the advancement of human rights and freedoms, and the supremacy of the Constitution and the rule of law.[1] In the course of this Chapter we discuss the implications of these values for the intelligence services.

The Chapter covers the following topics:

- The challenge of intelligence services in a democracy (Section 2.2).
- The primacy of the Constitution (Section 2.3).
- The rule of law (Section 2.4).
- Non-partisanship and promotion and respect for rights (Section 2.5).
- National security (Section 2.6).
- External control and oversight (Section 2.7).

[1] Section 1 of the Constitution.

- Internal controls and institutional culture (Section 2.8).

- Transparency and public discussion on intelligence (Section 2.9).

## 2.2 The Challenge of Intelligence Services in a Democracy

The existence of security services in democratic countries gives rise to a political paradox.[2] On the one hand, the security services are established in order to protect the state, its citizens and the democratic order and they are given special powers and capabilities for this purpose. On the other hand, by virtue of their special powers and capabilities they have the potential to undermine the security of citizens, threaten the state and subvert the democratic process. In order to avert these dangers, the security services are subject to a range of controls and forms of oversight.

The intelligence services present a particular challenge because of the nature of their role, their intrusive powers and their distinctive characteristic of secrecy. Their main functions typically include identifying and analysing internal and external threats to national security; informing and advising the Executive about the nature and causes of these threats; providing government with forewarning of future threats; and protecting state information that is deemed secret. The intelligence services are thereby expected to contribute to preventing, containing and overcoming serious threats to the country and its people.

In order to fulfil their vital functions, intelligence services throughout the world are given special powers. They have the power to acquire confidential information through surveillance, infiltration of organisations, interception of communication and other methods that infringe the right to privacy; to

[2] Section 199(1) of the Constitution states that the security services of the Republic consist of the defence force, the police service and any intelligence services established in terms of the Constitution.

undertake covert operations aimed at countering threats to national security; and to operate with a high level of secrecy.

Politicians and intelligence officers are able to abuse these powers to infringe civil liberties, interfere in lawful political activities and favour or prejudice a political party or leader, thereby compromising the integrity of the democratic process. They can intimidate the opponents of government, create a climate of fear and fabricate or manipulate intelligence in order to influence government decision-making and public opinion. They are also able to abuse intelligence funds and methods for personal gain and to promote private commercial interests.

Given these dangers, democracies are confronted by the challenge of constructing rules, controls and other safeguards that protect rights and freedoms and prevent misconduct by the intelligence services but do not restrict the services to such an extent that they are unable to fulfil their responsibilities. In short, the challenge is to ensure that the intelligence agencies pursue a legitimate mandate in a legitimate manner and in the national interest.

This challenge lies at the heart of our review, the aim of which is to strengthen mechanisms of control of the civilian intelligence structures in South Africa 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.

### 2.3 The Primacy of the Constitution

The role, character and activities of intelligence organisations throw up a number of difficult questions in democratic countries. What should be the primary focus of these organisations? What powers should they have and what limits should be placed on those powers? How can abuse of power be

prevented in conditions of secrecy? Is there too much secrecy? In what circumstances and subject to what safeguards can intelligence services infringe human rights in the interests of national security? What is meant by 'national security'? Who should be involved in determining national security and intelligence priorities?

As required by our terms of reference, we have considered these questions and the other topics under review through the lens of the Constitution. The Constitution is our legal and ethical framework because it is the supreme law[3] 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".[4]

Notwithstanding their grave responsibilities and the threats and dangers they might have to face, the security services are at all times and in all respects bound by the Constitution. The Constitution states explicitly that the security services must act, and must teach and require their members to act, in accordance with the Constitution and the law.[5]

In a recent judgement relating to the intelligence services, the Constitutional Court made the following observation about this provision of the Constitution:

> Besides the rule of law imperative, this constitutional injunction is also inspired by and deeply rooted in a repudiation of our past in which the security forces were, for the most part, law unto themselves; they terrorised the opponents of the government of the day with impunity and often in flagrant disregard of the law.[6]

[3] Section 2 of the Constitution states that "this Constitution is the supreme law of the Republic; law or conduct inconsistent with it is invalid, and the obligations imposed on it must be fulfilled".
[4] Preamble to the Constitution.
[5] Section 199(5) of the Constitution.
[6] *Masetlha v President of the Republic of South Africa and Another*, 2008 (1) SA 566 (CC), para 33.

The Bill of Rights is a cornerstone of democracy in South Africa. It enshrines the rights of all people in our country and affirms the democratic values of human dignity, equality and freedom.[7] It applies to all law and binds the legislature, the Executive, the judiciary and all organs of state.[8] The state must respect, protect, promote and fulfil the rights in the Bill of Rights.[9] The intelligence organisations are thus obliged to respect constitutional rights and may not infringe these rights other than as permitted by the Constitution and legislation.

Section 36(1) of the Constitution stipulates the basis on which rights can be limited. It provides as follows:

> The rights in the Bill of Rights may be limited only 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, taking into account all relevant factors, including a) the nature of the right; b) the importance of the purpose of the limitation; c) the nature and extent of the limitation; d) the relation between the limitation and its purpose; and e) less restrictive means to achieve the purpose.

In the course of this Report we refer on several occasions to section 36(1) of the Constitution. We stress the necessity for any potential infringement of constitutional rights by the intelligence services to be governed by legislation. The requirement of 'law of general application' has the profound benefit of enabling Parliament and citizens to consider draft legislation, debate issues that are vital to democracy and ensure that any limitation of rights is subject to adequate safeguards.

We are extremely concerned that some of the intrusive methods employed by the intelligence services, which infringe the constitutional right to privacy, are

[7] Section 7(1) of the Constitution.
[8] Section 8(1) of the Constitution.
[9] Section 7(2) of the Constitution.

not governed by legislation (Chapters 7 and 8). These methods are regulated by departmental policies but this is not sufficient in terms of the Constitution.

## 2.4 The Rule of Law

The Constitution declares that the values on which our democratic state is founded include the rule of law.[10] The rule of law is one of the cardinal features of governance that distinguish a democratic state from an undemocratic state. It establishes the primacy of law in order to create a legitimate and stable political dispensation based on rules approved by elected representatives. A product of protracted struggles against tyranny throughout the ages, it constrains rulers and organs of state so that they do not pose a threat to citizens.

Accordingly, the Constitution contains the following provisions:

- The security services must be structured and regulated by national legislation.[11]

- National security must be pursued in compliance with the law, including international law.[12]

- No member of any security service may obey a manifestly illegal order.[13]

- The security services must act, and must teach and require their members to act, in accordance with the Constitution and the law.[14]

[10] Section 1(c) of the Constitution.
[11] Section 199(4) of the Constitution.
[12] Section 198(c) of the Constitution.
[13] Section 199(6) of the Constitution.
[14] Section 199(5) of the Constitution.

- Any intelligence service other than an intelligence division of the defence force or police service may be established only by the President, as head of the national executive, and only in terms of national legislation.[15]

- National legislation must regulate the objects, powers and functions of the intelligence services.[16]

In light of these provisions, we reject the view that it is legitimate for intelligence officers to bend or break the rules when dealing with serious threats to security (Section 11.6).

## 2.5 Non-Partisanship and Promotion and Respect for Rights

In the nature of their business, which includes intrusive operations and collecting secret information, there is a risk that intelligence services might interfere in lawful political activity, favouring some political parties, organisations or leaders and prejudicing others. In many countries they have done this by infiltrating organisations, spying on politicians and activists, leaking confidential information about political leaders and spreading malicious rumours in political and media circles.

Malpractices of this kind might be initiated by intelligence officers or by politicians who have control or influence over the intelligence services. Whichever is the case, such malpractices would constitute a serious breach of trust and undermine the democratic system so severely that they can be considered a form of subversion. If exposed publicly, they can create a long-lasting crisis of confidence in the intelligence services and the government.

The Constitution therefore insists that members of the security services must be strictly non-partisan:

[15] Section 209(1) of the Constitution.
[16] Section 210 of the Constitution.

> Neither the security services nor any of their members may, in the performance of their functions, a) prejudice a political party interest that is legitimate in terms of the Constitution; or b) further, in a partisan manner, any interest of a political party.[17]

The intelligence services must exercise restraint not only in relation to political parties but also, more generally, in relation to legal political activities undertaken by civil society groups and citizens. The services are obliged to respect the political rights enshrined in the Constitution. These rights encompass the right to freedom of expression, including freedom of the press and other media;[18] the right, peacefully and unarmed, to assemble, demonstrate, picket and present petitions;[19] the right to freedom of association;[20] and the right to campaign for a political party or cause.[21]

Opposition to the ruling party, the government and members of the Executive is natural and legitimate in a democratic society. It is a dire misconception for the government or anyone else to regard lawful opposition as 'subversive', a 'national security threat' or 'contrary to the national interest', thereby necessitating and justifying investigation by the intelligence organisations.

We are concerned that NIA's mandate, and its political intelligence function in particular, may have politicised the Agency, drawn it directly into the arena 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. The intelligence transgressions of 2005 highlighted these dangers, leading the Minister for Intelligence Services to instruct NIA to abandon its political intelligence gathering (Chapter 6).

[17] Section 199(7) of the Constitution.
[18] Section 16(1) of the Constitution.
[19] Section 17 of the Constitution.
[20] Section 18 of the Constitution.
[21] Section 19(1)(c) of the Constitution.

In addition to guaranteeing political rights, the Constitution protects freedom of religion, thought, belief and opinion.[22] It also prohibits the state from unfairly discriminating against anyone on the grounds of race, gender, ethnic or social origin, sexual orientation, religion, belief, culture or language.[23] Against the backdrop of South Africa's history of racial oppression, and in a contemporary world wracked by all kinds of prejudice, the intelligence services must be at pains to be objective and non-discriminatory.

Finally, it should be noted that many of the rights in the Bill of Rights apply to "everyone", as the Constitution puts it, and are therefore held by foreign nationals in South Africa as well as by citizens.[24]

## 2.6 National Security

### *2.6.1 The concept of national security*

The Constitution states that national security must be governed by the following principle:

> 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.[25]

It is evident that the Constitution views national security in a comprehensive and holistic fashion that is much broader than a narrow conception of state security, territorial integrity and law and order. It follows that national security should not be conceived as separate from, and potentially in conflict with, human rights, fundamental freedoms and human security.

---

[22] Section 15(1) of the Constitution.
[23] Section 9(3) of the Constitution.
[24] See *Lawyers for Human Rights v Minister of Home Affairs* 2004 (4) SA 125 (CC); and *Mohamed v President of the Republic of South Africa* 2001 (3) SA 893 (CC).
[25] Section 198(a) of the Constitution.

One of the major implications of this constitutional perspective is that violations of constitutional rights by the intelligence services cannot be justified simply on the grounds of national security. National security requires the protection of human rights. Infringements of rights must instead be justified on more concrete grounds relating to the prevention of severe and demonstrable harm to the country and its people.

An emphasis on human security does not mean that the security of the state is unimportant. Since South Africa is a democracy and the state is legitimate, we are concerned equally with the security of the state and the security of its people. Indeed, there is a symbiotic relationship between the two. This is because the state has a primary responsibility to protect its citizens and provide for their security and also because serious threats to the state can imperil the security of citizens.

In short, national security encompasses the security of the country, its people, the state and the constitutional order. These elements are interlinked and none of them is more important than the others.

National security, defined broadly in this fashion, is not the preserve of the security services. It is the responsibility, first and foremost, of higher level entities, namely the Executive and Parliament. The Executive formulates and implements national security policy and exercises political control over the security services. Parliament is the legislative authority and exercises oversight of the Executive and the security services. According to the Constitution, all spheres of government and all organs of state have a responsibility to "secure the well-being of the people of the Republic".[26]

Nor does a broad approach to national security imply that the security services should have expansive mandates. This would make the services too influential, powerful and intrusive. It would create the danger of the security services encroaching inappropriately into politics, governance and social life.

[26] Section 41(1)(b) of the Constitution.

It would also lead to 'securitising' political and social problems in a way that results in ever greater restrictions on human rights and freedoms.[27]

Finally, a broad notion of national security does not imply that all security threats can be investigated through intrusive methods that infringe constitutional rights. Many threats to the security of citizens, such as poverty and poor health conditions, must be addressed through the normal business of government. Extreme measures should be reserved for extreme threats where other methods are inadequate, they should be essential given the nature of the threat, they should be regulated by legislation and they should be subject to executive control. Some of the intrusive methods used by the intelligence services in South Africa are not governed by legislation and are not subject to executive control (Chapter 7).

### *2.6.2 Authority for national security*

The Constitution states that "to give effect to the principles of transparency and accountability, multi-party committees must have oversight of all security services in a manner determined by national legislation or the rules and orders of Parliament".[28] The Constitution also provides that "national security is subject to the authority of Parliament and the national executive".[29]

These assertions have three important implications for the security services. First, there is a hierarchy of governance in terms of which the services are subordinate and accountable to Parliament and the Executive. This is achieved in practice by various means, including the issuing of laws, regulations and ministerial directives; the exercise of ministerial responsibility and control; parliamentary oversight; and parliamentary approval of security legislation and budgets.

[27] In Chapter 6 we consider these problems in relation to the mandate of NIA.
[28] Section 199(8) of the Constitution.
[29] Section 198(d) of the Constitution.

In Section 4.7 we highlight the problem that intrusive operations and other politically sensitive intelligence activities are not governed by ministerial regulations.

Second, the security services must undertake their functions within the parameters and according to the prescripts of policy and legislation approved by the Executive and Parliament. They may not act outside these parameters or contrary to these prescripts.

Third, the priorities in relation to national security and the security services must be determined by the Executive and Parliament. Prioritising is necessary because the security services cannot attend equally to all threats, and priorities might change from time to time as a result of changes in the security environment. The security services should advise government on threats and threat priorities but they are not responsible for decision-making in this regard.[30]

## 2.7 External Control and Oversight

### *2.7.1 Overview*

The civilian intelligence organisations in South Africa are subject to the following external control and oversight mechanisms:

- Parliamentary oversight of intelligence activities and approval of legislation and budgets.

- Political control exercised by the Minister for Intelligence Services (Chapter 4).

[30] We comment on Cabinet's National Intelligence Priorities in Section 12.3.1.

- The monitoring, review and investigative functions of the Inspector-General of Intelligence (Chapter 5).

- Judicial authorisation for the interception of private communication by the intelligence services (Chapter 7).

- Annual financial audits conducted by the Auditor-General (Chapter 10).

These mechanisms are intended to ensure that the intelligence services are subordinate and accountable to the Executive and Parliament; that the services comply with the Constitution, legislation and government policy; that they do not behave in a partisan and unreasonable manner; and that they do not abuse their powers, funds and other resources.[31]

These aims apply similarly to the control and oversight mechanisms governing other government departments and organs of state. In the case of intelligence services, however, the aims are difficult to achieve because of the secrecy that characterises the services and their operations. The secrecy prevents fully transparent reviews, inhibits public scrutiny and can facilitate the hiding of misconduct by intelligence officers.

In order to mitigate the problems associated with secrecy, it is essential that the control and oversight bodies have the following features: their authority and powers as provided for in legislation must be strong enough to enable them to carry out their functions effectively; they must have sufficient information about the activities of the intelligence services; they must have expertise in intelligence matters; they must have adequate resources to fulfil their mandates; and they must enjoy the co-operation of the services.[32]

[31] In Section 9.4 we consider the question of whether the intelligence services are subject to too much regulation and oversight.
[32] In Section 5.4 we highlight the problem that the Office of the Inspector-General of Intelligence does not have sufficient resources.

Where intelligence abuses have been exposed publicly in various countries over the past decades, it has frequently been the case that the culpability lay chiefly with politicians. The control and oversight bodies described above must therefore serve as checks and balances not only in relation to the intelligence agencies but also in relation to each other.

Individuals and organisations that believe that their rights have been infringed by the intelligence organisations can seek protection and redress in several ways. Depending on the nature of their complaint, they can approach the JSCI; the Inspector-General of Intelligence; the Human Rights Commission;[33] the Public Protector;[34] other institutions established by Chapter 9 of the Constitution; and the courts. The Constitutional Court is the final arbiter of whether legislation, regulations, policy and state actions comply with the Constitution or are invalid for lack of compliance.

### *2.7.2 Accountability to citizens*

Whereas the accountability of the intelligence services to the Executive and Parliament is strong, the accountability of the services and the intelligence oversight and control bodies to the public is less strong. This is a consequence of insufficient transparency. By way of example, ministerial regulations governing the services are secret; the Auditor-General's reports on the services are secret; the budgets of the services and most of their annual reports are secret; and there is too little public information about the activities and findings of the Inspector-General of Intelligence (Chapter 12).

The high level of secrecy is inconsistent with the Constitution, which insists that all spheres of government and all organs of state must be transparent

[33] In terms of section 184(2) of the Constitution, the Human Rights Commission has the power to investigate and report on the observance of human rights and to take steps to secure appropriate redress where rights have been violated.
[34] In terms of section 182(1) of the Constitution, the Public Protector has the power to investigate any conduct in state affairs that is alleged or suspected to be improper or to result in any impropriety or prejudice, and to take appropriate remedial action.

and accountable.[35] In relation to Parliament, the Constitution states that the National Assembly must facilitate public involvement in the legislative and other processes of the Assembly and its committees, conduct its business in an open manner and hold its sittings and those of its committees in public.[36] The National Assembly may not exclude the public, including the media, from a sitting of a committee unless it is reasonable and justifiable to do so in an open and democratic society.[37]

The JSCI holds all its meetings in secret.[38] As a result, the public is unable to learn much about the Committee's oversight of the intelligence organisations, its assessment of their performance and its efforts to address problems that it identifies. The reports that are presented to the JSCI by the Minister, the Inspector-General and the heads of the services are classified and are therefore not tabled in the National Assembly.[39] The JSCI presents annual reports to Parliament and has also tabled in Parliament its reports on controversial intelligence incidents, but these reports are not readily accessible to the public.[40] There is very little debate on intelligence matters in the National Assembly, and parliamentarians other than members of the JSCI rarely participate in the debates that do take place. We discuss the question of secrecy and transparency further in Section 2.9 and Chapter 12.

## 2.8 Internal Controls and Institutional Culture

Notwithstanding the importance of parliamentary, executive and other forms of external control and oversight, the most effective means of preventing malpractice by intelligence officers lie within the intelligence services

[35] Section 41(1) of the Constitution.
[36] Section 59(1) of the Constitution.
[37] Section 59(2) of the Constitution.
[38] Section 2(7) of the Intelligence Services Oversight Act No. 40 of 1994 states that no person other than members of the JSCI and its staff may be present during the proceedings of the Committee, except with its permission.
[39] By contrast, the website of the United States Senate Select Committee on Intelligence contains a vast amount of information, including speeches by intelligence officials and senators (http://intelligence.senate.gov/index.html).
[40] The JSCI's reports that were obtained by the Commission are listed in the Bibliography.

themselves. Internal controls, self-discipline and personal integrity are critical qualities in any organisation. They have even greater salience where the members of the organisation have the power to infringe constitutional rights and operate secretly.

Intelligence agencies must have comprehensive internal controls that are designed to ensure, and that in practice do ensure, strict compliance by their members with the Constitution, legislation, ministerial directives and departmental policies. The key control mechanisms include thorough procedures and recordkeeping; proper systems of authorisation, decision-making and supervision of staff; monitoring and audit systems to detect non-compliance; and a disciplinary system for addressing any breaking of the rules.

The intelligence organisations must also have an institutional culture of respect for the law, the imperative of political non-partisanship and other constitutional principles. Ideally, they should abide by the rules because they view ethical and lawful conduct as an intrinsic component of professionalism and regard the constitutional principles not as burdensome impediments but as vital safeguards of democracy. In this sense, intelligence officers must themselves be committed democrats.

The South African intelligence services have numerous internal controls, they are engaged in a virtually continuous process of strengthening these controls and their operational policies emphasise the necessity to comply with the Constitution and legislation (Chapters 9 and 10). This is indicative of their professionalism. However, the controls and the emphasis on compliance are undermined by the absence of adequate legal expertise in the intelligence community (Section 11.7), and by the belief of some senior officials that it is legitimate to break the rules when dealing with serious security threats (Section 11.6). It is essential that there be unanimous support for the position of the senior officials who advocate a policy of zero-tolerance of misconduct

(Section 11.1) and for the Minister's insistence on adherence to the principle of legality (Section 11.2).

## 2.9 Transparency and Public Discussion on Intelligence

### *2.9.1 Transparency*

The Constitution emphasises the principle of transparent governance.[41] The Bill of Rights goes so far as to provide that "everyone has the right of access to any information held by the state" and that national legislation must be enacted to give effect to this right.[42]

The relevant legislation is the Promotion of Access to Information Act No. 2 of 2000. The Act describes a causal relationship between secrecy and abuse of power and human rights: "… the system of government in South Africa before 27 April 1994, amongst others, resulted in a secretive and unresponsive culture in public and private bodies which often led to an abuse of power and human rights violations".[43] The legislation was enacted so as to "actively promote a society in which the people of South Africa have effective access to information to enable them to more fully exercise and protect all of their rights".[44]

The intelligence services pose a particular dilemma in this regard. On the one hand, excessive secrecy is contrary to good governance and provides an environment in which illegality, corruption and abuse of power can flourish. On the other hand, excessive openness would compromise intelligence operations and could thereby prejudice the security of citizens and the state.

---

[41] See the Preamble and sections 1(d), 36(1), 39(1), 41(1)(c), 59 and 199(8) of the Constitution.
[42] Section 32 of the Constitution.
[43] Preamble of the Promotion of Access to Information Act.
[44] Ibid.

We believe that the intelligence community has not yet shed sufficiently the obsession with secrecy that wracked the security services in the apartheid era. Whereas the current emphasis of the intelligence organisations is on secrecy with some exceptions, the emphasis ought to be on openness with some exceptions. In Chapter 12 we make recommendations on enhancing transparency in ways that would not undermine the intelligence services or the security of the country.

### *2.9.2 Public debate of intelligence*

In a democratic country there ought to be informed public debate about all aspects of security. Security policies and laws lead to the prioritising of threats and allocation of resources, they confer and regulate special powers and they sometimes limit basic rights. It is therefore essential that citizens engage with these issues. Their engagement deepens democracy, strengthens a culture of accountability and can be a powerful avenue for influencing decisions that have a significant impact on their lives.

South Africans talk constantly about policing, prisons and the judiciary but there is little debate on intelligence apart from occasional bursts of attention at times of controversy. Although the absence of sustained discussion is due partly to the fact that intelligence operations and reports are secret, this cannot be the only reason. Public documents that can be accessed easily include the White Paper on Intelligence of 1994, all the intelligence legislation, speeches on intelligence by the President and the Minister, and a great deal of research on intelligence in other countries.[45]

The lack of debate on intelligence issues might also be due to a perception that intelligence is so sensitive that it lies outside the public domain. This is not a healthy state of affairs in a democracy. Parliament, government,

[45] The intelligence legislation, presidential and ministerial speeches on intelligence, parliamentary questions and answers and other material can be found on the website of the Ministry for Intelligence Services (www.intelligence.gov.za). Comparative research on intelligence can be viewed, for example, on the website of the Geneva Centre for the Democratic Control of Armed Forces (www.dcaf.ch).

research bodies and other civil society groups should take steps to raise awareness and facilitate discussion on intelligence. We have written this Report in a manner that we hope will stimulate and contribute to a process of public dialogue.

## CHAPTER 3: THE WHITE PAPER ON INTELLIGENCE

### 3.1 Introduction

The objective of South Africa's White Paper on Intelligence of 1994 is to provide a framework for understanding the philosophy, mission and role of intelligence in the new democratic dispensation.[1] The document states that its goal is "the creation of an effective, integrated and responsive intelligence machinery that can serve the Constitution and the government of the day, through the timeous provision of relevant, credible and reliable intelligence".[2]

This Chapter first outlines the two themes of the White Paper, namely democracy and the rule of law, and a holistic approach to security. These themes were intended to guide the transformation of intelligence in the new democracy. We then present our concerns with the White Paper: it has sound principles and norms but they are not translated adequately into policies, strategies and institutional arrangements; and the mandate of NIA is defined too broadly. We conclude by recommending that a new White Paper be prepared.

The Chapter covers the following topics:

- The scope of the White Paper (Section 3.2).
- The definition and purpose of intelligence (Section 3.3).
- Democracy and the rule of law (Section 3.4).
- A holistic approach to security (Section 3.5).

[1] White Paper on Intelligence, 1994, pg. 1. The White Paper can be viewed at www.intelligence.gov.za/Legislation/white_paper_on_intelligence.htm.
[2] White Paper on Intelligence, pg. 1.

- An overall assessment of the White Paper (Section 3.6).

- The overly broad domestic intelligence mandate (Section 3.7).

- Recommendations (Section 3.8).

### 3.2 Scope of the White Paper

The White Paper focuses on the civilian intelligence services and does not deal with the intelligence divisions of the SANDF and the SAPS.

The White Paper is divided into the following sections:

- A Philosophy of Intelligence, which considers the definition, purpose and mission of intelligence and outlines a new national security doctrine.

- The Basic Principles of Intelligence, which includes a code of conduct.

- The Composition of the Intelligence Community, which refers to the establishment of NIA and SASS.

- Control and Co-ordination of Intelligence, which covers mechanisms of control and describes the functions of NICOC.

- Transforming Intelligence Methodology, which deals with training; effectiveness and standards; secrecy and declassification; covert action; and the secret intelligence budget.

- External and Internal Realities Facing South Africa and the Intelligence Community, which offers a perspective on the international, regional and domestic dimensions of security.

The White Paper has two annexures that emanate from the Transitional Executive Council's Sub-Council on Intelligence: a code of conduct for intelligence workers and a set of basic principles and guidelines on national intelligence.

### 3.3 The Definition and Purpose of Intelligence

The White Paper defines intelligence as follows:

> Intelligence refers to 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. Modern intelligence can thus be described as 'organised policy related information', including secret information.[3]

Intelligence is intended to contribute to the successful implementation of domestic and foreign policy. To be of value in this regard, it must have the following attributes: accuracy; relevance; predictive capacity; an element of warning; and timeliness.[4]

To be relevant in the modern world, intelligence must have the following purposes:

- To provide policy-makers with timeous, critical and sometimes unique information to warn them of potential risks and dangers.

- To identify opportunities in the international environment by assessing actual or potential competitors' intentions and capabilities.

[3] White Paper on Intelligence, pg. 2.
[4] Ibid, pg. 2.

- To assist good governance by providing honest, critical intelligence that highlights the weaknesses and errors of government.[5]

### 3.4 Democracy and the Rule of Law

The first major theme of the White Paper is democracy and the rule of law. The document asserts that "a new mission is being set for the South African intelligence community in line with the new, non-racial, democratic order, in which much weight is given to the rights of the individual".[6] This mission is derived from an understanding of the international, regional and domestic environments and from a new moral code and organisational culture governing intelligence.[7]

The security apparatus of the apartheid government was "over-accentuated with virtually no institutional checks and balances".[8] By contrast, the White Paper asserts repeatedly the necessity for the new intelligence services to comply with the rule of law and other democratic norms, including subordination and accountability to Parliament. This imperative is regarded as an essential component of the transformation of the intelligence community.

The White Paper insists that the intelligence services should accept the primacy and authority of the democratic institutions of society and the constitutional bodies that are mandated to participate in and/or monitor the determination of intelligence priorities. The services should accept that no changes will be made to the doctrines, structures and procedures of the national security framework unless approved of by the people and their representative bodies. They should also bind themselves to a contract entered into with the electorate through a mutually agreed set of norms and code of conduct.

[5] White Paper on Intelligence, pg. 2.
[6] Ibid, pg. 1.
[7] Ibid, pg. 1.
[8] Ibid, pg. 1.

The Code of Conduct for intelligence officers provides for "obedience to the laws of the country and subordination to the rule of law"; "compliance with democratic values such as respect for human rights"; and "adherence to the principle of political neutrality".[9]

In relation to covert action, the White Paper states the following:

> Measures designed to deliberately interfere with the normal political processes in other countries and with the internal workings of parties and organisations engaged in lawful activity within South Africa must be expressly forbidden. Intelligence agencies or those within them guilty of such breaches must be disciplined in the severest terms.[10]

### 3.5 A Holistic Approach to Security

The second major theme of the White Paper revolves around a holistic approach to security. The White Paper rejects the militaristic and state-centric approach to security, prevalent in many countries during the Cold War, which emphasised military threats, internal law and order, and the security, independence and territorial integrity of the state. Instead, the White Paper endorses a comprehensive model that recognises the non-military aspects of security, appreciates the importance of international interdependence and puts people at the heart of security.[11] Security is now defined less in military terms and more in the broader sense of freedom from the vulnerability of modern society.[12]

---

[9] White Paper on Intelligence, pg. 5.
[10] Ibid, pg. 8. In Chapters 6 and 11 we discuss the question of adherence to this prohibition on interference in political activity.
[11] White Paper on Intelligence, pg. 3.
[12] Ibid, pg. 3.

The White Paper states that 'new thinking on security' has the following key features, which should form an integral part of the government's philosophical outlook on intelligence:

- Security is conceived as a holistic phenomenon that incorporates political, social, economic and environmental issues.

- The objectives of security policy go beyond achieving an absence of war to encompass the pursuit of democracy, sustainable economic development and social justice.

- Regional security policy seeks to advance the principles of collective security, non-aggression and peaceful settlement of disputes.[13]

National security objectives should "encompass the basic principles and core values associated with a better quality of life, freedom, social justice, prosperity and development".[14] The Reconstruction and Development Programme forms the core of the country's emerging national security doctrine.[15] This doctrine "must promote the creation of a societal environment that is free of violence and instability. It must engender, within the context of a transformed judicial system, respect for the rule of law and human life".[16]

### 3.6 Overall Assessment of the White Paper

The main strength of the White Paper is that it lays out a democratic vision, philosophy and set of principles on security, intelligence and intelligence transformation in the post-apartheid dispensation. This was a vital task since the apartheid security services were geared principally to internal repression and external aggression in the maintenance of minority rule.

[13] White Paper on Intelligence, pg. 4.
[14] Ibid, pg. 4.
[15] Ibid, pg. 4.
[16] Ibid, pg. 4.

The main weakness of the White Paper is that it does not translate the new philosophy and principles into meaningful policies. The emphasis is almost exclusively on values and norms, with scarcely any attention paid to strategy and institutional development and consolidation. There are many crucial assertions whose policy, strategic and organisational implications are not addressed in the fashion required of a White Paper.

Some examples of this tendency are presented below:

- The White Paper states that in a democracy the government must exercise control over the intelligence community through a range of measures that include the separation of intelligence functions, controlling access to the Executive, and differentiating the functions of collection, reporting, co-ordinating and review.[17] No information is provided on any of these measures, however, and it is therefore unclear what they entail in practice. The question of 'controlling access to the Executive' is especially important but the White Paper provides no perspective on the matter.[18]

- The White Paper notes that the new control mechanisms will also include ministerial accountability, a mechanism for parliamentary oversight and an independent Inspector-General of Intelligence.[19] Nothing further is said about ministerial accountability. In relation to the Inspector-General, the document simply states that the functions of this official will include reviewing the activities of the intelligence services and monitoring their compliance with policy guidelines. In relation to parliamentary oversight, the White Paper merely provides a four-line summary of the draft legislation on this subject.

- In the section entitled "Transforming Intelligence Methodology", the White Paper deals with a number of critical topics in a cursory fashion, offering

[17] White Paper on Intelligence, pg. 5.
[18] We discuss this issue in Section 4.4.
[19] White Paper on Intelligence, pp. 6-7.

bland normative assertions rather than meaningful policy positions.[20] These topics include training, which is dealt with in four lines; effectiveness and standards, which is covered in eight lines; secrecy and declassification, which receives five lines; covert action, which gets only four lines; and the "secret intelligence budget", which gets two lines.

- The White Paper does not provide an adequate policy perspective on the following topics: strategies for transformation; political and economic intelligence; intelligence relations with other states; covert operations; counter-intelligence; interception of communication and other infringements of the right to privacy; the intrusive powers of the intelligence services; and the relationship between the intelligence services and the Executive.

One of the purposes of a White Paper, which is issued by a government and often submitted to Parliament for comment or approval, is to set out national policy on a particular sector of governance with sufficient clarity and detail to guide the medium- to long-term development of legislation, strategies, departmental policies, institutional relationships and organisational structures.

If a White Paper has major gaps, there is a risk that departmental policies and activities will lack focus and cohesion. There is also a risk that policy positions which ought to be taken by the Executive and approved by Parliament will instead be determined by government officials without parliamentary and public input. This problem has in fact occurred. Many critical policy issues – concerning relations with foreign intelligence services (Section 4.7); political and economic intelligence (Section 6.3); counter-intelligence (Section 6.6); intrusive measures (Chapter 7); and electronic surveillance (Chapter 8) – have been addressed only in ministerial regulations or departmental policies that are secret.

[20] White Paper on Intelligence, pp. 7-8.

## 3.7 An Overly Broad Domestic Intelligence Mandate

### *3.7.1 Defining security and the mandate of the security services*

When the holistic model of security became prominent in the early 1990s, a number of analysts warned that its broadness, elasticity and lack of specificity were potentially dangerous. They argued that a broad approach to security could have several undesirable consequences: an inappropriate expansion of the focus and role of the security services; an increased security budget; the encroachment of the security services into governance, politics and social and economic life; and a process of 'securitising' political and social problems, thereby justifying security measures that infringe human rights.

It is possible to avoid these dangers by defining the mandate and functions of each of the security services narrowly and precisely. Even if the concepts of 'security' and 'national security' are defined broadly, it does not follow that any of the security services should have a broad mandate.

By way of example, the White Paper on Defence of 1996 adopts a holistic approach to security but insists that this "does not imply an expanded role for the armed forces. The SANDF may be employed in a range of secondary roles as prescribed by law, but its primary and essential function is service in defence of South Africa, for the protection of its sovereignty and territorial integrity".[21]

### *3.7.2 The White Paper on Intelligence*

The White Paper on Intelligence does not define the intelligence mandate with any precision. It states that the mission of the intelligence community is to provide evaluated information with the following responsibilities in mind: safeguarding the Constitution; upholding individual rights; promoting the interrelated elements of security, stability, co-operation and development;

[21] White Paper on National Defence for the Republic of South Africa, 1996, section 2.8.

achieving national prosperity while contributing to global peace and other global priorities; promoting South Africa's ability to face foreign threats; and enhancing the country's international competitiveness.[22]

The White Paper defines NIA's mission as follows: "to conduct security intelligence within the borders of the Republic of South Africa in order to protect the Constitution. The overall aim shall be to ensure the security and stability of the State and the safety and well-being of its citizens".[23]

This definition requires explanation and elaboration, which are not provided in the White Paper. What does 'protect the Constitution' actually mean? This is an abstract notion, capable of different interpretations, whose political and operational implications ought to be spelt out. What criteria will be used to determine threats to the 'stability' of the state? What does NIA's mission to 'ensure security' entail? Is 'security' to be understood here having political, economic, social, technological and environmental dimensions and as relating to 'freedom from the vulnerability of modern society'? What are the implications of so broad and vague a mission for NIA's priorities and activities?

The National Strategic Intelligence Act No. 39 of 1994, which stipulates the functions of the national intelligence structures in South Africa, does not define NIA's mandate narrowly and precisely. On the contrary, as discussed in Chapter 6, it codifies in law the breadth and generality that appears in the White Paper.

### *3.7.3 The problems associated with a broad mandate*

We discuss NIA's mandate in Chapter 6. For present purposes the problems associated with a broad domestic intelligence mandate can be summarised as follows:

[22] White Paper on Intelligence, pg. 3.
[23] Ibid, pg. 6.

Problems of overreach. If the mandate encompasses all dimensions of security, then the intelligence agency has to cover too much ground. This can lead to a lack of clear and consistent focus and to difficulty in determining priorities and ranking the seriousness of security threats. The broad mandate creates pressure for analytical breadth rather than depth, duplicates the analysis being done by other government departments and leaves the agency constantly over-extended. There is a danger that the agency ends up neglecting its most important and difficult task, which is to identify, analyse and forewarn government about potential violence and other extreme threats that entail criminality.

Problems of politicisation. An overly broad definition of security and overly broad intelligence mandate can lead the intelligence agency to focus in an inappropriate manner on lawful political and social activities. It can also lead to the politicisation of the agency, which has to assess whether lawful activities are actually or potentially destabilising. These problems are extremely serious where the agency has the power to infringe constitutional rights and is able to operate secretly.[24]

Problems of interpretation and prioritisation. A broad intelligence mandate can be interpreted in various ways and requires substantial prioritising. The danger here is that the processes of interpretation and prioritisation occur solely within the state, without the outcomes being transparent and debated by Parliament. NIA has in fact re-interpreted its mandate three times since 1994, the results of which have not been subject to an open and vigorous parliamentary and public debate (Chapter 6).

In Section 6.8 we present NIA's own concerns about its broad mandate. In Section 6.9 we recommend that the mandate be narrowed to focus on organised violence, organised crime and serious criminal offences such as

[24] As presented in Section 6.5.1, similar concerns about the broadness of NIA's mandate have been expressed by Minister Kasrils.

terrorism, sabotage, espionage, drug trafficking and smuggling of weapons of mass destruction. We also explain how this mandate would differ from that of the police.

### *3.7.4 Determining high-level intelligence priorities*

No intelligence organisation can focus on every actual and potential threat to the security of the state and its people. Even if the organisation has massive resources at its disposal, the number of political, social, economic and environmental threats is simply too vast. It is therefore necessary to establish priorities for intelligence agencies. Prioritising is required for the additional reason that different types of threat have different impacts and many threats to the well-being of citizens can be tackled by government bodies other than the security services.

It is legitimate for an intelligence service to determine its operational priorities but the service should do this within the parameters of higher level policy priorities set by the Executive in consultation with Parliament. Two kinds of high-level prioritising are needed. The first is contingent and of a short- to medium-term nature: the Executive must periodically make judgements on intelligence priorities in the light of national priorities and relevant domestic and foreign developments. In South Africa this kind of prioritising takes the form of the National Intelligence Priorities approved annually by Cabinet (Section 12.3.1).

The second kind of high-level intelligence prioritising is of a more general and abiding nature. It occurs through the determination of the mandate and functions of the intelligence services and entails major conceptual, normative and political decisions. This determination ought to be expressed in both legislation and a White Paper, the former providing legal definitions and prescriptions, the latter providing the policy motivation and elaboration, and both providing an opportunity for parliamentary and public engagement. The White Paper of 1994 does not fulfil this function.

### 3.8 Recommendations

In its 2006 report to the Minister, the Task Team on the Review of Intelligence-Related Legislation, Regulation and Policies stated that a review of the White Paper was not a priority for the moment. The Task Team recommended that this issue be revisited once the National Security Strategy and any other relevant review processes had been finalised.[25]

In our view, a new White Paper is required for the following reasons:

- The 1994 White Paper is strong in terms of philosophy and principles but weak in terms of policy, strategy and institutional arrangements. There is a need for more elaborate policy perspectives on a range of issues, including the mandate of the domestic intelligence agency.

- The White Paper was written more than ten years ago. Since then, the domestic, regional and international security environments have changed markedly. In addition, there is much to learn from the experiences of local and foreign intelligence services over the past decade.

- Over the past five years in South Africa, intelligence reviews of various kinds have been conducted by ministers, the intelligence services, the Inspector-General of Intelligence and other bodies. It would be beneficial to consolidate the conclusions and recommendations of these reviews in a new White Paper.

We recommend that the following topics be covered in a new White Paper:

- The mandates, functions and powers of the intelligence organisations, including oversight of, and controls over, their powers to infringe constitutional rights.

[25] Task Team on the Review of Intelligence-Related Legislation, Regulation and Policies, 'Final Report of the Task Team on the Review of Intelligence-Related Legislation, Regulation and Policies', April 2006, pg. 60.

- Executive control and accountability, and the relationship between the intelligence services and the President, Cabinet and the Minister for Intelligence Services.

- Civilian oversight, including oversight by the JSCI and the Inspector-General of Intelligence.

- The relationship between the different intelligence organisations in South Africa, the co-ordination of intelligence and the functions of NICOC.

- Relations with foreign intelligence services and sharing intelligence about South African citizens with foreign governments.

- Secrecy and transparency, covering both the provision of information and the protection of information.

- The institutional culture of the intelligence services and ensuring respect for the Constitution and the rule of law.

The process of preparing a new White Paper should include consultation by the Minister and parliamentary hearings and debate following a call for public submissions. This would provide an opportunity for the Executive, Parliament, the intelligence services, non-governmental organisations and citizens to debate intelligence issues that impact on national security, constitutional rights and public life. The process would also serve to inform the citizenry about the intelligence services and enhance the legitimacy of the services and their mandates.

## CHAPTER 4: MINISTERIAL CONTROL AND RESPONSIBILITY

### 4.1 Introduction

The Minister for Intelligence Services (hereafter "the Minister") is a key actor in efforts to ensure that the intelligence services comply with the Constitution and legislation, do not abuse their power and resources, and do not behave in an improper manner. Like other Cabinet ministers, the Minister is empowered to introduce legislation and regulations, formulate policy and issue ministerial directives. As discussed in this Chapter, legislation confers on the Minister specific powers and functions in relation to the intelligence services.

The Minister is an important office-bearer not only because he or she exercises executive control over the intelligence services but also because of the doctrine of ministerial accountability. The Minister is accountable to the President, Cabinet and Parliament for the exercise of his or her powers and functions.

It should be noted at the outset that ministerial control and responsibility lie at the political and executive levels. Operational control and responsibility, on the other hand, lie with the heads of the intelligence services. In general, a Minister is the political head of a government department, responsible for policy matters and overall policy outcomes, whereas a Director-General is the administrative head and accounting officer of a department, responsible for implementing government programmes and for outputs towards the achievement of policy outcomes.[1]

This Chapter focuses on ministerial control and responsibility. It covers the following topics:

[1] 'Reply from President Thabo Mbeki to questions for oral reply in the National Assembly, 26 March 2003, Question Number 1', retrieved from www.thepresidency.gov.za on 5 November 2007.

- Constitutional provisions (Section 4.2).

- The powers and functions of the Minister (Section 4.3).

- The adequacy of the legislative provisions on the supply of intelligence to the Minister and the President (Section 4.4).

- The adequacy of the legislative provisions on authority for tasking the intelligence structures (Section 4.5).

- The dismissal, suspension and transfer of a Director-General of an intelligence service (Section 4.6).

- The adequacy of ministerial regulations and directives (Section 4.7).

- Ministerial accountability and means of addressing ministerial abuse of power (Section 4.8).

- Recommendations (Section 4.9).

The Chapter focuses on the following Acts: the Intelligence Services Act No. 65 of 2002 (hereafter "the Intelligence Services Act"); the National Strategic Intelligence Act No. 39 of 1994 (hereafter "the National Strategic Intelligence Act"); and the Intelligence Services Oversight Act No. 40 of 1994 (hereafter "the Intelligence Services Oversight Act").[2]

## 4.2 Constitutional Provisions

As noted in Section 1.6.1, the Constitution states that the President must appoint the head of each intelligence service established in terms of the

[2] The observations and recommendations in this Chapter are informed by our discussions with the President, the Minister for Intelligence Services, the Inspector-General of Intelligence and the intelligence officials who made submissions to the Commission.

Constitution, and must either assume political responsibility for the control and direction of any of those services or designate a member of the Cabinet to assume that responsibility.[3]

The constitutional provisions on ministerial accountability and responsibility are also relevant:

- Ministers are responsible for the powers and functions of the Executive assigned to them by the President.[4]

- Members of Cabinet are accountable collectively and individually to Parliament for the exercise of their powers and the performance of their functions.[5]

- Members of Cabinet must provide Parliament with full and regular reports concerning matters under their control.[6]

## 4.3 Powers and Functions of the Minister

In this section we present the powers and functions of the Minister as stipulated in the intelligence legislation and then provide an assessment of the legislation in this regard.

### *4.3.1 Intelligence Services Act*

The Intelligence Services Act regulates the establishment, organisation and control of NIA, SASS and SANAI. NIA and SASS are collectively referred to as "the intelligence services".[7]

[3] Section 209(2) of the Constitution.
[4] Section 92(1) of the Constitution.
[5] Section 92(2) of the Constitution.
[6] Section 92(3)(b) of the Constitution.
[7] Section 1 of the Intelligence Services Act.

The Act gives the Minister a range of powers and functions:

- The Minister must, for each of the intelligence services, create posts of Deputy Director-General and Assistant Director-General; establish chief directorates and directorates and prescribe the functions and post structures thereof; and establish divisions and prescribe the functions and post structures thereof.[8] The creation by the Minister of Deputy Directors-General posts must be done in consultation with the President.[9] The President appoints the Directors-General of NIA and SASS.[10]

- The management and administration of SANAI is under the control of the Minister.[11] The Minister must appoint the deputy head of the Academy.[12] The President is responsible for appointing the head of the Academy.[13]

- The Minister may appoint any person as a member of the intelligence services or the Academy and may promote, discharge, demote or transfer any member.[14] An appointment, promotion, discharge or transfer in respect of a Deputy Director-General or equivalent post may only be effected in consultation with the President.[15]

- If a member of NIA, SASS or SANAI is discharged or demoted by the head of the organisation, he or she may appeal against that decision to the Minister.[16]

- The heads of NIA, SASS and SANAI must exercise command and control of their respective organisations subject to the directions of the Minister.[17]

[8] Section 4(1) of the Intelligence Services Act.
[9] Section 4(2) of the Intelligence Services Act.
[10] Section 209(2) of the Constitution and section 3(3)(a) of the Intelligence Services Act.
[11] Section 5(1) of the Intelligence Services Act.
[12] Section 6(2) of the Intelligence Services Act.
[13] Section 6(1) of the Intelligence Services Act.
[14] Section 8(1) of the Intelligence Services Act.
[15] Section 8(1) of the Intelligence Services Act.
[16] Sections 15(c), 16(2), 17(2) and 18(3) of the Intelligence Services Act.

- The Minister must approve the functional directives issued by the heads of NIA, SASS and SANAI in relation to conditions of service and any other matter the head deems expedient for the efficient command and control of the organisation.[18]

- The Minister must approve the functional directives issued by the heads of NIA and SASS in relation to physical security, computer security, communication security, protection of classified information and any other matter that is necessary for the intelligence and counter-intelligence functions of the services.[19]

- Subject to the Act, the Minister may do or cause to be done all things which are necessary for the efficient superintendence, control and functioning of the intelligence services and the Academy.[20]

- The Minister may acquire and dispose of immovable and movable property relating to the functioning of the services and the Academy.[21]

- The Minister may, after consultation with the JSCI, make regulations regarding, amongst other things, the employment, training, promotion, posting, transfer, resignation, discharge, dismissal, suspension or demotion of members; the numerical establishment of NIA, SASS and SANAI; the conditions of service of their members; the establishment and maintenance of training institutions; all matters relating to discipline, command and control of the services and SANAI; the control over and administration of funds appropriated to SANAI, NIA and SASS; all matters relating to representivity and equity; and a code of conduct for members.[22]

---

[17] Section 10(1) of the Intelligence Services Act.
[18] Section 10(2) of the Intelligence Services Act.
[19] Section 10(3) of the Intelligence Services Act.
[20] Section 12(1) of the Intelligence Services Act.
[21] Section 12(2) of the Intelligence Services Act.
[22] Section 37(1) of the Intelligence Services Act.

### *4.3.2 National Strategic Intelligence Act*

The National Strategic Intelligence Act defines the functions of the national strategic intelligence structures, namely NICOC, NIA, SASS and the intelligence divisions of the SAPS and the SANDF, and provides for the appointment of a Co-ordinator for Intelligence as the chairperson of NICOC.[23]

The Minister's powers and functions include the following:

- The Co-ordinator for Intelligence must manage the functions of NICOC subject to the directions and supervision of the Minister.[24]

- The Minister shall do everything necessary for the efficient functioning, control and supervision of the co-ordination of intelligence supplied by the national intelligence structures.[25]

- The Minister shall advise the President and National Executive on national strategic intelligence and the co-ordination of intelligence.[26]

- The Minister may, after consultation with the JSCI, make regulations regarding the protection of information and intelligence; security screening investigations; co-ordination of intelligence; production and dissemination of intelligence for consideration by Cabinet and the Executive; the co-ordination of counter-intelligence by NIA; the co-ordination of crime intelligence; and any other matter necessary for the effective administration of the Act.[27]

[23] Section 1 of the National Strategic Intelligence Act.
[24] Section 5(1) of the National Strategic Intelligence Act.
[25] Section 5A(1) of the National Strategic Intelligence Act.
[26] Section 5A(5) of the National Strategic Intelligence Act.
[27] Section 6 of the National Strategic Intelligence Act.

### *4.3.3 Intelligence Services Oversight Act*

The Intelligence Services Oversight Act provides for the establishment and functions of the JSCI and for the appointment and functions of the Inspector-General of Intelligence (hereafter the "Inspector-General"). The Act gives the Minister a number of powers and functions, which include the following:

- The Minister may designate functions to the Inspector-General.[28]

- The Minister may, after consultation with the Inspector-General, appoint such number of persons to the office of the Inspector-General as may be necessary for the performance of the functions of that office.[29]

- The Minister, acting with the concurrence of the JSCI, may make regulations regarding, amongst other things, the performance of his or her functions by the Inspector-General; the reports to be submitted by the Inspector-General and the heads of the intelligence services; the suspension or removal from office of the Inspector-General; the procedure for appointing staff to the office of the Inspector-General; and the procedures for investigations undertaken by the Inspector-General.[30]

### *4.3.4 Summary assessment of ministerial 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 for the control and direction of the intelligence services. The main problems relate to significant issues that are not covered, or not covered adequately, in the legislation. There are four major problems in this regard:

[28] Section (7)(7)(c) of the Intelligence Services Oversight Act.
[29] Section 7(12) of the Intelligence Services Oversight Act.
[30] Section 8(1) of the Intelligence Services Oversight Act.

- The legislative provisions on the supply of intelligence to the Minister, the President and government departments are unsatisfactory (Section 4.4).

- There are no legislative provisions on authority to task the intelligence services (Section 4.5).

- The legislation does not provide for the dismissal, suspension, demotion or transfer of the Director-General of an intelligence service (Section 4.6).

- The legislation does not provide for ministerial approval of intrusive operations undertaken by the intelligence services (Section 7.6).

## 4.4 The Supply of Intelligence to the Minister and the President

This Section first defines some key terms and presents the sections of the National Strategic Intelligence Act that deal with the supply of intelligence by the intelligence structures. We then discuss the supply of intelligence to the Minister; ministerial powers in relation to intelligence reports; the supply of departmental intelligence; and reporting to the President.

### *4.4.1 Definitions*

'Domestic intelligence' is defined as "intelligence on any internal activity, factor or development which is detrimental to the national stability of the Republic, as well as threats or potential threats to the constitutional order of the Republic and the safety and the well-being of its people".[31]

'Foreign intelligence' is defined as "intelligence on any external threat or potential threat to the national interests of the Republic and its people, and intelligence regarding opportunities relevant to the protection and promotion

[31] Section 1 of the National Strategic Intelligence Act.

of such national interests irrespective of whether or not it can be used in the formulation of the foreign policy of the Republic".[32]

'National strategic intelligence' is defined as "comprehensive, integrated and estimative intelligence on all the current and long-term aspects of national security which are of special concern to strategic decision-making and the formulation and implementation of policy and strategy at the national level".[33]

'Departmental intelligence' means "intelligence about any threat or potential threat to the national security and stability of the Republic which falls within the functions of a department of State, and includes intelligence needed by such department in order to neutralise such a threat".[34] 'Department' is defined as "a national department, a provincial administration or a provincial department".[35]

'Intelligence' is defined as "the process of gathering, evaluation, correlation and interpretation of security information, including activities related thereto, as performed by the Services".[36]

*4.4.2 Legislative provisions on the supply of intelligence*

The National Strategic Intelligence Act stipulates the following relationships regarding the supply of intelligence:

- NIA must supply domestic intelligence regarding any threat or potential threat to the security of the Republic or its people to NICOC.[37]

[32] Section 1 of the National Strategic Intelligence Act.
[33] Section 1 of the National Strategic Intelligence Act.
[34] Section 1 of the National Strategic Intelligence Act.
[35] Section 1 of the National Strategic Intelligence Act refers in this regard to the definition of 'department' in the Public Service Act No. 103 of 1994.
[36] Section 1 of the Intelligence Services Oversight Act.
[37] Section 2(1)(a)(ii) of the National Strategic Intelligence Act.

- NIA must inform the President of any threat or potential threat to the security of the Republic or its people.[38]

- NIA must supply (where necessary) intelligence relating to any threat or potential threat to the security of the Republic or its people to the SAPS for the purposes of investigating an offence,[39] and to the Department of Home Affairs for the purposes of fulfilling any immigration function.[40]

- NIA must supply intelligence relating to national strategic intelligence to NICOC.[41]

- At the request of any interested department of state, NIA must supply departmental intelligence to that department and to NICOC.[42]

- SASS must supply foreign intelligence relating to any threat or potential threat to the security of the Republic or its people to NICOC.[43]

- At the request of any interested department of State, SASS must supply departmental intelligence to that department and to NICOC.[44]

- The SAPS must supply crime intelligence relating to national strategic intelligence to NICOC.[45]

- The SANDF must supply foreign and domestic military intelligence relating to national strategic intelligence to NICOC.[46]

[38] Section 2(1)(b)(ii) of the National Strategic Intelligence Act.
[39] Section 2(1)(b)(iii) of the National Strategic Intelligence Act.
[40] Section 2(1)(b)(iv) of the National Strategic Intelligence Act.
[41] Section 2(1)(b)(v) of the National Strategic Intelligence Act.
[42] Section 2(1)(c) of the National Strategic Intelligence Act.
[43] Section 2(2)(a)(ii) of the National Strategic Intelligence Act.
[44] Section 2(2)(c) of the National Strategic Intelligence Act.
[45] Section (2)(3)(c) of the National Strategic Intelligence Act.
[46] Sections 2(4)(a) and (b) of the National Strategic Intelligence Act.

- NICOC must disseminate intelligence regarding national interests and threats and potential threats to national security to Cabinet.[47]

- NICOC must co-ordinate the flow of national strategic intelligence between the departments of state entrusted with the maintenance of security.[48]

- At the request of any state department, NICOC must provide departmental intelligence to that department.[49]

- NICOC must make recommendations to Cabinet on intelligence priorities.[50]

- The Minister must advise the President and the national executive on national strategic intelligence and the co-ordination of intelligence.[51]

*4.4.3 The supply of intelligence to the Minister*

The legislative provisions presented above reveal a striking anomaly in relation to the supply of intelligence. NIA, SASS and the intelligence divisions of the SAPS and the SANDF must provide intelligence relating to national strategic intelligence to NICOC; NICOC, in turn, must provide intelligence and advice on intelligence priorities to Cabinet; the Minister must advise the President and National Executive on national strategic intelligence; but there is no requirement that any of the intelligence structures must provide intelligence directly to the Minister.

It could be argued that the provision of strategic intelligence to the Minister is implied in the legislation: since the Minister must advise the President and the National Executive on national strategic intelligence, it follows that the Minister must necessarily receive that intelligence. This is a logical inference

[47] Section 4(2)(c) of the National Strategic Intelligence Act.
[48] Section 4(2)(d) of the National Strategic Intelligence Act.
[49] Section 4(2)(e) of the National Strategic Intelligence Act.
[50] Section 4(2)(f) of the National Strategic Intelligence Act.
[51] Section 5A(5) of the National Strategic Intelligence Act.

but it is unsatisfactory because there is no indication of who should provide intelligence to the Minister and there is no legal obligation on any official or intelligence structure to provide intelligence to the Minister.

According to NIA officials, it is possible that this odd situation is an inadvertent consequence of historical developments.[52] Following the establishment of South Africa's democratic dispensation in 1994, there was no appointment of a full Minister for intelligence. At Cabinet level, the Minister of Justice held the intelligence portfolio. A Deputy Minister for Intelligence was appointed and he also held the post of Co-ordinator of NICOC. Since the Deputy Minister was the NICOC Co-ordinator, the reporting relationships specified in the legislation were not unsound.

In 1999 new ministerial arrangements were introduced. The President appointed a full Minister for Intelligence Services, the post of Deputy Minister was dropped and the position of NICOC Co-ordinator was filled by a senior civil servant. The intelligence legislation was not amended adequately in the light of these changes, with the result that the Minister is not a designated recipient of intelligence. In terms of the express provisions of the legislation, he or she only receives intelligence when NICOC reports to the Cabinet.

Even if the Minister does in practice receive intelligence reports, as is currently the case, this legal situation is untenable. If there is no legal obligation to provide the Minister with intelligence reports, then the following serious problems could arise:

- The Minister might be unable to assume political responsibility for the control and direction of the intelligence services, as required by section 209(2) of the Constitution.

[52] Meeting with NIA, 12 October 2007.

- The Minister might be unable to advise adequately the President and National Executive on national strategic intelligence, as required by section 5A(5) of the National Strategic Intelligence Act.

- The Minister might be unable to do everything necessary for the efficient functioning, control and supervision of the co-ordination of intelligence supplied by the national intelligence structures, as required by section 5A(1) of the National Strategic Intelligence Act.

- The Minister might be unable to report and account adequately to Parliament, as required by section 92(3)(b) of the Constitution.

- The Minister could not be held accountable politically if the intelligence services produced intelligence that was consistently partisan or of a poor quality.

In short, it would not make sense for any member of Cabinet, let alone the Minister for Intelligence Services, to be in the dark about the primary outputs of the organisations that fall under his or her political control.

Our comments about the supply of intelligence to the Minister do not imply that the Minister should be given raw intelligence or voluminous intelligence reports. Depending on government priorities, the severity of a security threat and the political sensitivity of the matter, the Minister may want concise summaries on certain issues and more comprehensive briefings on others. As is currently the case, the arrangements in this regard should be determined by the Minister.

*4.4.4 Ministerial powers in relation to intelligence reports*

As noted in Section 4.1, the Minister bears political and executive responsibility for the intelligence services and the outcome of their efforts. The Minister should not be involved in operations or interfere with operations

but he or she is entitled to question the quality and veracity of an intelligence report and to request the intelligence service responsible for the report to take further steps to confirm its accuracy, completeness and conclusions. The Minister may also task an intelligence service to investigate a particular matter.

On the other hand, it would be completely improper for the Minister to ask for an intelligence report to be falsified in any way, such as by including inaccurate or irrelevant information, excluding relevant information, omitting doubts about the reliability of information or sources, or exaggerating or downplaying the importance of certain facts without a sound justification.

*4.4.5 The supply of departmental intelligence*

We noted in Section 4.4.2 that NIA and SASS, if so requested by a national department, provincial administration or provincial department, must supply departmental intelligence to that body and to NICOC. Similarly, NICOC must supply departmental intelligence to a department that requests such intelligence.

The intelligence structures are not obliged in law to seek ministerial approval for the supply of departmental intelligence or even to inform the Minister for Intelligence Services that they have provided intelligence to another department. Nor does the Act indicate which official in a department is entitled to request intelligence.

There are no regulations or ministerial directives governing these matters. Consequently, the supply of departmental intelligence lies, inappropriately, outside the ambit of ministerial control and responsibility.

### *4.4.6 Reporting to the President*

The National Strategic Intelligence Act contains only one provision that permits an intelligence structure to report directly to the President: NIA must inform the President of any threat or potential threat to the security of the Republic or its people.[53] There is no provision for NICOC, SASS and the intelligence divisions of the SAPS and the SANDF to report directly to the President.

We were informed that in practice, the heads of the intelligence structures have in the past often reported directly to the President and there were times when the relevant minister was excluded from this process. This has the potential to generate confusion and conflict, it can be misused for political mischief and it can undermine the Minister's political responsibility and control.

As the head of the National Executive, the President is a 'primary client' of the intelligence structures. He or she must receive intelligence relating to serious security threats and presidential projects and missions. Depending on the circumstances, the intelligence might be given to the President directly by the head of an intelligence structure or via the relevant minister or the Director-General in the Presidency. The Minister or Director-General would play a quality assurance role and ensure that the President is not swamped with information. The President does not need to receive all intelligence that is relevant to the Executive since the Minister for Intelligence Services and other ministers are also 'primary clients' of the intelligence structures.

Two questions emerge from these observations. First, should the legislation specify in greater detail the arrangements for providing intelligence to the President? Regulating the matter in law would have the benefit of minimising the potential for confusion, conflict and intrigue arising from the provision of intelligence to the President.

[53] Section 2(1)(b)(ii) of the National Strategic Intelligence Act.

Alternatively, the matter could be regulated through ministerial regulations.[54] Another option would be to regulate the provision of intelligence to the President through a presidential directive. This would allow for greater flexibility in so far as the directive could be amended more easily than legislation or regulations.

The second question is whether the heads of NIA, SASS and NICOC should be obliged to brief the Minister for Intelligence Services if they have briefed the President.[55] For the reasons presented in Section 4.4.3 above, the answer must surely be yes. The Minister cannot be expected to fulfil his or her constitutional and legal functions adequately if he or she is in the dark about certain strategic intelligence.

It is relevant in this regard that the President is not obliged to appoint a Minister for Intelligence Services. As noted previously, the Constitution requires the President either to assume political responsibility for the control and direction of the intelligence services or to appoint a Minister to assume this responsibility.[56] If the President chooses to appoint a Minister, then the Minister must be able to fulfil fully his or her responsibility.

It could be argued that certain intelligence supplied to the President might be too sensitive to be given to the Minister. Yet the Minister is appointed by the President and is therefore mandated and trusted by the President to receive sensitive information. If the Minister loses the President's trust, then he or she can be dismissed by the President.

It is of course possible that the intelligence services might have reason to believe that the Minister is a threat to national security. Nevertheless, this

[54] Section 6(d) of the National Strategic Intelligence Act provides that the Minister may make regulations regarding the production and dissemination of intelligence for consideration by Cabinet and the Executive.
[55] We do not deal here with the intelligence divisions of the SAPS and the SANDF since they lie outside our terms of reference.
[56] Section 209(2) of the Constitution.

extraordinary scenario, as where the head of state is a security threat, cannot be the basis for determining *general* policy and procedures on the relationship between the intelligence services, the Minister and the President.

### 4.5 Authority for Tasking the Intelligence Services

The intelligence legislation is silent on the question of who is authorised to task the intelligence services to gather and supply intelligence. It could be inferred from the National Strategic Intelligence Act that the bodies to which the intelligence structures must supply intelligence are also entitled to ask these structures to gather and supply intelligence. In practice, however, the situation is somewhat more complicated.

The National Strategic Intelligence Act specifies the functions of each of the intelligence organisations and thereby fixes the legal parameters of their focus and tasks. On an annual basis Cabinet issues a set of National Intelligence Priorities, which provide overall executive direction for the intelligence organisations' focus, priorities and allocation of resources for the year. From time to time the Executive and the intelligence organisations might also identify a need to focus on an unanticipated threat or issue.

In addition to the above, ad hoc requests for intelligence might emanate from an official or department outside the intelligence community. It is here that the legislative silence on authorisation for tasking the intelligence structures can be problematic. For example, in previous years it was possible for a provincial Premier to request a provincial head of NIA to supply him or her with intelligence regarding political stability in the province, and there was no requirement that the Minister be informed thereof.[57] NIA has now tightened these arrangements in its internal policies.[58]

[57] Meeting with NIA, 12 October 2007.
[58] Ibid.

The issue of authorisation for tasking goes to the heart of political control of the intelligence organisations and is thus sufficiently important to be covered in legislation. In Section 4.9.4 we make recommendations in this regard.

## 4.6 Dismissal, Suspension and Transfer of a Director-General

The power of the President and/or the Minister to deal with misconduct by the head of an intelligence service, and the grounds on which the head of a service can be dismissed, are of great relevance to our terms of reference. This is not only because the heads should face disciplinary action if they engage in misconduct but also because they should have some protection against a politically motivated dismissal or threat of dismissal.

The legislative provisions on these matters are unclear and unsatisfactory. The Intelligence Services Act states that the Minister may discharge, demote or transfer any member of an intelligence service, provided that the discharge, demotion or transfer of a Deputy Director-General or equivalent post may only be effected in consultation with the President.[59] The Act does not provide for the discharge, demotion or transfer of the heads of NIA, SASS, NICOC and SANAI and does not indicate the grounds on which such action can be taken.

As a result of the intelligence crisis of 2005/6, the President dismissed the head of NIA, who appealed against his dismissal to the Constitutional Court. The Court's findings and observations that are relevant for present purposes are as follows:

- The terms of employment of the head of an intelligence service are regulated by both the Intelligence Services Act and the Public Service Act No. 103 of 1994 but "regrettably, the interplay between the provisions of

[59] Section 8(1) of the Intelligence Services Act.

these two statutes in this particular context is complex and less than clear".[60]

- Neither the Intelligence Services Act nor the Public Service Act gives the Minister the power to suspend or dismiss the Director-General of an intelligence service.[61] The power to dismiss the Director-General lies instead with the President and derives implicitly from section 209(2) of the Constitution, which gives the President the power to appoint that person.[62]

- An irretrievable breakdown in the relationship of trust between the President and the head of an intelligence service is a lawful basis for dismissing the latter.[63]

- In a minority judgement, Mr Justice Sachs stated that "the provisions of the Intelligence Services Act (ISA), and regulations made under them, appear not to be helpful [in relation to the dismissal of the head of an intelligence service]. Many of the regulations are in fact so secret that even a court of law would not ordinarily have access to them".[64]

Although the Constitutional Court judgement provides clarity on the dismissal of the head of an intelligence service, it does not enumerate the grounds on which such dismissal can take place. Nor does it deal with disciplinary measures against, and the demotion or transfer of, this official. Further, the Court did not consider these issues in relation to the heads of SANAI and NICOC who, like the heads of NIA and SASS, are appointed by the President.

The legislative silence on these matters ought to be filled so as to provide for greater clarity and certainty. This would be in the interests of the incumbent

[60] *Masetlha v President of the Republic of South Africa and Another* 2008 (1) SA 566 (CC), para 38.
[61] *Masetlha v President of the Republic of South Africa*, op cit, paras 36 and 42.
[62] Ibid, para 68.
[63] Ibid, paras 87-91.
[64] Ibid, para 229, footnotes omitted.

officials as well as the President and the Minister, and might reduce the potential for conflict and litigation in the future.

## 4.7 Adequacy of Ministerial Regulations and Directives

As noted in Section 4.3, the intelligence legislation empowers the Minister to make regulations on a range of topics. This Section provides an assessment of the ministerial regulations and directives that are currently in force.

### *4.7.1 Summary of ministerial regulations and directives*

In 2003 the Minister issued the Intelligence Services Regulations in accordance with section 37 of the Intelligence Services Act.[65] This document comprises twenty-eight chapters that deal mainly with conditions of service in the intelligence services. The topics include organisation and structures; working environment; evaluation, recruitment and selection; appointment and termination of service; remuneration and service benefits; leave; performance management; promotions; training and development; employment equity; consultation; and grievance and disciplinary procedures.

In 2003 the Minister issued two documents, one each for NIA and SASS, entitled “Ministerial Delegation of Powers and Direction of Payment”. Acting in terms of section 20 of the Intelligence Services Act, the Minister delegated authority for expenditure within specified limits to the directors-general and other senior officials of NIA and SASS.

In 2006 the Minister issued a directive on the conduct of signals intelligence operations, instructing that South African telephone numbers could not be monitored by the NCC without the permission of a judge (Section 8.5.2).

[65] Government Notice No. R.1505, *Government Gazette* No. 25592, 16 October 2003.

In 2007 the Minister issued the Regulations on Liaison with Foreign Intelligence Services in accordance with section 6 of the National Strategic Intelligence Act and section 12 of the Intelligence Services Act.

There is currently under consideration a document entitled "Draft Regulations on the Coordination of Intelligence as an Activity: Determination of Intelligence Priorities and Prescripts Relating to the Conduct of Intelligence Services", undated (hereafter "Draft Regulations on the Coordination of Intelligence").[66]

*4.7.2 Comment*

We have three major concerns about the ministerial regulations described above. First, the regulations are confidential in whole or in part. The Regulations on Liaison with Foreign Intelligence Services is an entirely confidential document. Several chapters of the Intelligence Services Regulations were published in the *Government Gazette* but most of the content was excluded from this publication.[67]

It is therefore doubtful that these documents meet the legal test of 'regulations'. Regulations are subordinate legislation that a Minister is empowered to make under an Act and that must be published in the *Government Gazette* in order to have any legal effect.[68] The confidential status of the regulations is also contrary to the Constitution, which states that "proclamations, regulations and other instruments of subordinate legislation must be accessible to the public".[69] We discuss this further in Section 12.3.2.

Our second concern relates to the relative absence of regulations and ministerial directives. There is a considerable gap between the intelligence

[66] This document was at an early stage of development when it was given to us, and it has not been published.
[67] Government Notice No. R.1505, *Government Gazette* No. 25592, 16 October 2003.
[68] Correspondence to the Commission from the Office of the Chief State Law Adviser, 3 December 2007.
[69] Section 101(3) of the Constitution.

legislation and the operational directives issued by the heads of the intelligence services. What is missing is an intervening layer of ministerial regulations and directives that contain rules and guidelines flowing from the legislation and government policy.

This gap is most problematic with respect to intelligence functions that are politically significant and sensitive, like intrusive operations, counter-measures, political intelligence and the decision to target individuals and organisations for investigation. Policies and rules on these matters that ought to be determined at the level of the Executive have instead been determined by the heads of the services. Later in the Report we discuss this problem more extensively in relation to NIA's mandate (Chapter 6) and intrusive operations (Chapter 7).

The Inspector-General of Intelligence observes correctly that the regulations at present have a strong administrative focus as opposed to an operational focus.[70] The Draft Regulations on the Coordination of Intelligence are intended to fill some of the operational gaps by providing ministerial direction on the following topics: target setting; authorisation and management of intrusive collection and investigative techniques; general principles governing the conduct of intelligence operations; and ministerial authorisation for intrusive operations. In our view there are a number of additional issues that ought to be covered by regulations (Section 4.9.6).

Our third concern relates to section 6(c) of the Regulations on Liaison with Foreign Intelligence Services, which states that intelligence shall not be exchanged on South African citizens or citizens of other countries living in South Africa unless there is a reasonable belief that such citizens may be involved in acts which constitute or may constitute a threat to the national security of the RSA or their countries of origin if they are non-South African citizens.

[70] Office of the Inspector-General of Intelligence, 'Submission to the Ministerial Review Commission. The Concept of the Control of the Civilian Intelligence Services', presented to the Commission on 29 January 2007, pg. 22.

Providing foreign intelligence services with information and intelligence on citizens and other people living in South Africa is obviously an extremely sensitive political issue. In our view, ministerial approval should therefore be required for such exchange of information and intelligence, and the focus of any exchange should be confined to the planning or commission of a crime.

### 4.8 Ministerial Accountability and Ministerial Abuse of Power

This Chapter has thus far concentrated on ministerial control of the intelligence services. This is a crucial mechanism for preventing misconduct, illegality and abuse of power by the services. Yet is also possible that the Minister might abuse his or her power for political or other reasons. The intelligence crises that have rocked various countries over the past two decades have frequently been a consequence of mischief, manipulation or outright illegality by politicians at the highest level of the state.

The Minister for Intelligence Services is subject to all the constitutional principles and mechanisms designed to ensure executive accountability:

- The Minister is accountable to the President, the Cabinet and Parliament.
- The Minister's budget has to be approved by Parliament.
- The Minister must provide Parliament with full and regular reports about the matters that are under his or her control.
- The Minister's decisions can be taken on review to a court.
- Complaints against the Minister can be lodged with the Human Rights Commission and the Public Protector.

The rest of this Section focuses on the powers of the JSCI in relation to the Minister; complaints against the Minister; and protection of members of the intelligence services.

### *4.8.1 The JSCI*

The Intelligence Services Oversight Act contains the following provisions on the powers of the JSCI in relation to the Minister:

- The Minister must present to the JSCI an [annual] report regarding the budget of each of the services and entities for which he or she is responsible.[71] The JSCI may request the Minister to explain any aspect of this report.[72]

- The JSCI may, for the performance of its functions, require the Minister to appear before it to give evidence, to produce any document or thing and to answer questions put to him or her.[73]

- The Minister must act with the concurrence of the JSCI when making regulations under this Act.[74]

- The JSCI is empowered to review and make recommendations on regulations issued by the Minister in terms of the National Strategic Intelligence Act and the Intelligence Services Act.[75]

In addition, section 37(1) of the Intelligence Services Act and section 6 of the National Strategic Intelligence Act require the Minister to consult the JSCI before making regulations in terms of these Acts.

[71] Section 3(a)(iv) of the Intelligence Services Oversight Act.
[72] Section 3(i) of the Intelligence Services Oversight Act.
[73] Section 4(3) of the Intelligence Services Oversight Act.
[74] Section 8(1) of the Intelligence Services Oversight Act.
[75] Section 3(d) of the Intelligence Services Oversight Act.

*4.8.2 Complaints against the Minister*

The Inspector-General of Intelligence plays an ombuds role in relation to the intelligence structures and is empowered to investigate complaints against them by members of the public and members of the structures.[76] There is no express provision enabling the Inspector-General to investigate a complaint against the Minister.

In our view the Inspector-General is not a good instrument for investigating complaints against the Minister because he or she is not sufficiently independent of the Minister. Although the Inspector-General is accountable to the JSCI for the overall functioning of his or her office,[77] the Minister is entitled to make regulations on the performance of the Inspector-General's functions, the procedures for investigations undertaken by the Inspector-General and the suspension and removal from office of the Inspector-General.[78]

We should stress here that we are not questioning the integrity or independence of the individual who holds the post of Inspector-General currently or in the future. Our concern relates rather to the relationship in law between the Inspector-General and the Minister for Intelligence Services.

We believe that there are adequate alternative mechanisms for raising complaints against the Minister. Such complaints could be referred to a court, the Public Protector or the Human Rights Commission. One or more of these bodies would be appropriate where political parties, other organisations or members of the public seek protection and redress against the Minister or wish to challenge the constitutionality of the Minister's decisions or actions. A complaint could also be submitted to the JSCI, which could investigate the matter itself or refer the matter to the Human Rights Commission or the Public Protector.

[76] Section 7(7)(cA) of the Intelligence Services Oversight Act.
[77] Section 7(6) of the Intelligence Oversight Act.
[78] Section 8(1) of the Intelligence Oversight Act.

### *4.8.3 Protection of members of the intelligence services*

Members of the intelligence services must obey all lawful directions received from a person having the authority to give such directions.[79] Consequently, they might question the appropriateness of a lawful instruction from the Minister but they are obliged to comply with it.

If, however, the Minister's request or instruction is unlawful because it exceeds the Minister's authority or requires unconstitutional or criminal conduct, then it should not be obeyed. The Constitution states categorically that "no member of any security service may obey a manifestly illegal order".[80] This injunction requires members of the intelligence services to be conversant with the relevant law and constitutional provisions.

## 4.9 Recommendations

### *4.9.1 Supply of intelligence to the Minister*

The Minister for Intelligence Services must be a designated recipient of national strategic intelligence and of intelligence relating to threats to the security of the Republic or its people. Accordingly, the National Strategic Intelligence Act should be amended to include the following provisions:

- NIA must inform the Minister of any domestic threat or potential threat to the security of the Republic or its people.[81]

- SASS must inform the Minister of any foreign threat or potential threat to the security of the Republic or its people.

[79] Section 11(1) of the Intelligence Services Act.
[80] Section 199(6) of the Constitution.
[81] This wording is consistent with section 2(1)(b)(ii) of the National Strategic Intelligence Act, which provides that NIA must inform the President of any threat or potential threat to the security of the Republic or its people.

- NICOC must provide the Minister with national strategic intelligence and with intelligence regarding national interests and threats and potential threats to national security.[82]

The powers of the Minister in relation to intelligence reports, and limitations on the exercise of those powers, should be covered in a ministerial directive that is drawn up in consultation with and approved by the JSCI.

*4.9.2 Supply of departmental intelligence*

In relation to the supply of departmental intelligence, the National Strategic Intelligence Act should be amended to reflect the following positions:

- NIA, SASS and NICOC may only supply departmental intelligence, or enter into a standing arrangement to supply departmental intelligence, with the approval of the Minister and subject to any conditions that he or she might set.

- A request for NIA, SASS or NICOC to provide departmental intelligence or enter into a standing arrangement to provide departmental intelligence must be made by the responsible minister in the case of a national department and by the Premier in the case of a provincial administration or department. The request must be made to the Minister for Intelligence Services.

The Minister should issue guidelines that regulate and expedite the supply of departmental intelligence.

[82] This wording is consistent with section 4(2)(c) of the National Strategic Intelligence Act, which provides that NICOC must disseminate intelligence regarding national interests and threats and potential threats to national security to the Cabinet.

*4.9.3 Supply of intelligence to the President*

The supply of intelligence and intelligence reports to the President by NIA, SASS and NICOC, and access to the President by the heads of these bodies, should be regulated by the National Strategic Intelligence Act, ministerial regulations or a presidential directive.

The rules should state that intelligence and intelligence reports which are given to the President by NIA, SASS or NICOC must also be given to the Minister for Intelligence Services.

*4.9.4 Authority for tasking the intelligence services*

The National Strategic Intelligence Act should be amended to include the following provisions on authorisation for tasking the intelligence services:

- NIA, SASS and NICOC may only be tasked to gather and supply intelligence by the President, Cabinet, a Cabinet security cluster, the Minister for Intelligence Services and the Co-ordinator of NICOC. Any such tasking must be directed to the head of the intelligence body.

- NIA may request SASS to gather and provide it with any foreign intelligence that is required to fulfil the functions of NIA, and SASS may request NIA to gather and supply it with any domestic intelligence that is required to fulfil the functions of SASS.

- As recommended above, a request for NIA, SASS or NICOC to provide departmental intelligence to a government department must be made by the responsible Minister in the case of a national department and by the Premier in the case of a provincial administration or department, and the request must be made to the Minister for Intelligence Services.

- If a parliamentary committee (other than the JSCI) or a parastatal organisation requires an intelligence briefing on a topic related to its business, the head of the committee or organisation must make the request via the Minister for Intelligence Services.

*4.9.5 Dismissal, suspension and transfer of a Director-General*

The Minister should introduce legislative provisions and regulations that cover disciplinary measures against, and the dismissal, suspension, demotion and transfer of, the heads of the intelligence services, NICOC and SANAI.

In preparing the legislative provisions and regulations, the Minister should consider the following issues:

- Whether the authority to conduct a disciplinary inquiry and take disciplinary action against the head of an intelligence structure should lie with the President or with the Minister subject to the approval of the President.

- Whether the grounds for dismissing a Director-General of a government department outside the intelligence community should apply equally to the head of an intelligence structure.

- Whether a breakdown in trust between the Minister and the head of an intelligence structure should constitute grounds for dismissing the head.

- Whether demotion and transfer are viable options in the case of the head of an intelligence structure.

As noted in Section 4.6, the Constitutional Court has observed that the terms of employment of the head of an intelligence service are regulated by both the Intelligence Services Act and the Public Service Act but the interplay between the provisions of these two statutes is complex and unclear. In consultation

with the Minister for Public Service and Administration, the Minister for Intelligence Services should fix the gaps and ambiguities through legislative amendments.

*4.9.6 Ministerial regulations*

The Minister should issue regulations on the following topics:

- The conduct of intrusive operations, counter-intelligence operations and counter-measures.[83]

- The supply of intelligence to the Minister.

- The supply of departmental intelligence to government departments.

- The production and dissemination of intelligence for consideration by Cabinet and the Executive.

- Authority for tasking NIA, SASS and NICOC to gather and produce intelligence.

- Disciplinary measures against, and the dismissal, suspension, demotion and transfer of, the heads of the intelligence services, NICOC and SANAI.

- The Inspector-General's investigations, inspections and certification of the reports issued by the heads of the intelligence services.[84]

As noted in this Chapter and elsewhere in the Report, some of the issues listed above should also be addressed in legislation.

[83] In Chapter 9 we discuss the Legislative Review Task Team's recommendations on regulations governing intelligence operations.
[84] We discuss these issues in Section 5.5.

The existing regulations and those issued by the Minister in the future should be published in full in the *Government Gazette*. Rules that must be kept confidential for operational reasons should be issued as ministerial directives.

Ministerial approval should be required for the provision of information and intelligence on citizens and other people living in South Africa to foreign intelligence services, and the focus of any such information and intelligence should be confined to the planning or commission of a crime.

## CHAPTER 5: THE INSPECTOR-GENERAL OF INTELLIGENCE

### 5.1 Introduction

The Inspector-General of Intelligence (hereafter "the Inspector-General") has a vital role to play in the intelligence community. He or she has the legal mandate and powers to investigate complaints of misconduct, illegality or abuse of power by the intelligence organisations. Such complaints can be lodged with the Inspector-General by a member of the public, a member of an intelligence organisation or the JSCI.

The significance of the Office of the Inspector-General of Intelligence (OIGI) is heightened by three features that are not shared by other statutory bodies, such as the Public Protector and the Human Rights Commission, which might be called to act on a complaint against one of the intelligence services. First, the staff of the OIGI have experience and expertise in intelligence. This enhances their ability to detect misconduct and illegality that might otherwise escape the attention of external investigators.

Second, the Inspector-General may not be denied access to any intelligence, information or premises under the control of the intelligence services, and any such denial constitutes a criminal offence. These are essential legal requirements when investigating the propriety of operations and activities that are classified as secret and top secret.

Third, the Inspector-General's ombuds role is not confined to reactive investigations of complaints. He or she has an on-going statutory responsibility to monitor compliance by the intelligence services with the Constitution and relevant laws and policies.[1]

[1] In Section 11.5 we present the Inspector-General's perspective on the institutional culture of the intelligence organisations.

In this Chapter we recommend that the mandate of the Inspector-General be narrowed to focus exclusively on the ombuds role; that the budget of the OIGI be increased substantially; that the OIGI become a fully independent organisation; that the Minister for Intelligence Services issue regulations governing the OIGI and its activities; and that the Minister initiate an evaluation of the investigation undertaken by the Inspector-General during the intelligence crisis of 2005/6.

The Chapter covers the following topics:

- The legal powers and functions of the Inspector-General (Section 5.2).
- Refining the mandate of the Inspector-General (Section 5.3).
- Increasing the budget of the OIGI (Section 5.4).
- The recommendations of the Legislative Review Task Team regarding the Inspector-General (Section 5.5).
- The Inspector-General's investigation during the intelligence crisis of 2005/6 (Section 5.6).
- Recommendations (Section 5.7).

## 5.2 Functions and Powers of the Inspector-General

Section 210 of the Constitution states, among other things, that national 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 adopted by the National Assembly with a supporting vote of at least two-thirds of its members.

The relevant legislation is the Intelligence Services Oversight Act No. 40 of 1994 (hereafter "the Act"), which provides for the appointment of an Inspector-General of Intelligence who is nominated by the JSCI and must be approved by the National Assembly on the terms stipulated in the Constitution.[2] The Inspector-General may be removed from office by the President but only on the grounds of misconduct, incapacity, withdrawal of his or her security clearance, poor performance or incompetence as prescribed.[3]

The Inspector-General is accountable to the JSCI for the overall functioning of his or her office and at least once a year must report to the Committee on his or her activities and the performance of his or her functions.[4]

The Inspector-General's jurisdiction over the intelligence organisations covers NIA, SASS and the intelligence divisions of the SAPS and the SANDF.[5] The NCC's operational activities are also subject to the oversight of the Inspector-General.[6]

In terms of section 7(7) of the Act, the Inspector-General has the following functions in relation to the intelligence services:

- To monitor compliance by any service with the Constitution, applicable laws and relevant policies on intelligence and counter-intelligence.

- To review the intelligence and counter-intelligence activities of any service.

- To perform all functions designated to him or her by the President or any Minister responsible for a service.

[2] Section 7(1) of the Intelligence Services Oversight Act.
[3] Section 7(5) of the Intelligence Services Oversight Act.
[4] Section 7(6) of the Intelligence Services Oversight Act.
[5] Section 1 of the Intelligence Services Oversight Act.
[6] National Communications Centre, 'Briefing to Ministerial Review Commission', 30 January 2007.

- To receive and investigate complaints from members of the public and members of the intelligence services on alleged maladministration; abuse of power; transgressions of the Constitution, applicable laws and relevant policies on intelligence and counter-intelligence; the commission of offences specified in the Prevention and Combating of Corrupt Activities Act No. 12 of 2004; and improper enrichment of any person through an act or omission of a member of a service.

- To submit reports to the relevant Ministers pursuant to the performance of the above functions and to the President in relation to functions designated to the Inspector-General by the President.

- To undertake an investigation ordered by the JSCI where the Committee has received a complaint about an intelligence service from a member of the public,[7] and to submit reports accordingly to the JSCI.[8]

The head of each intelligence service must give the relevant Minister a report on the activities of that service for every period of twelve months, and a copy of the report must be given to the Inspector-General. The Inspector-General must submit to the Minister a certificate stating the extent to which he or she is satisfied with the report and whether anything done by the service was unlawful, contravened any directions issued by the Minister or involved an unreasonable or unnecessary exercise of power by that service. The Ministers must provide the JSCI with the reports submitted by the services and the certificates issued by the Inspector-General.[9]

Each head of an intelligence service is obliged to report to the Inspector-General any unlawful intelligence activity or significant intelligence failure of that service and any corrective action that has been taken or is intended to be taken in connection with such unlawful activity or intelligence failure.[10]

[7] Section 3(f) of the Intelligence Services Oversight Act.
[8] Section 7(7)(e) of the Intelligence Services Oversight Act.
[9] Sections 7(11)(a), (c) and (d) of the Intelligence Services Oversight Act.
[10] Section 7(11)(b) of the Intelligence Services Oversight Act.

Once the NCC has been established by legislation,[11] the Inspector-General must report annually to Parliament on its activities and in such report must indicate any contraventions by the NCC of the provisions of the Regulation of Interception of Communications and Provision of Communication-Related Information Act No. 70 of 2002.[12]

The Inspector-General has access to any intelligence, information or premises under the control of an intelligence service if such access is required for the performance of his or her functions under section 7 of the Act, and he or she may demand from the head of the service and its employees such intelligence, information, reports and explanations as are necessary for the performance of these functions.[13] No access to intelligence, information or premises under the control of an intelligence service may be withheld from the Inspector-General on any ground.[14]

The Inspector-General also has access to any intelligence, information or premises that are not under the control of an intelligence service, and is entitled to demand such access from any person, if this is necessary for the performance of his or her functions under section 7 of the Act. In order to gain this access, the Inspector-General must first obtain a warrant issued in terms of the Criminal Procedure Act No. 51 of 1977.[15]

Failure to comply with the Inspector-General's request for access to intelligence, information or premises is a criminal offence and can lead on conviction to imprisonment of up to five years.[16]

---

[11] The Intelligence Services Amendment Bill [B 37-2008] and the National Strategic Intelligence Amendment Bill [B 38-2008], which provide for the establishment and functions of the NCC, were published in June 2008.
[12] Section 2 of the National Strategic Intelligence Amendment Bill [B 38-2008].
[13] Section 7(8)(a) of the Intelligence Services Oversight Act.
[14] Section 7(9) of the Intelligence Services Oversight Act.
[15] Section 7A of the Intelligence Services Oversight Act.
[16] Section 7(8)(c) of the Intelligence Services Oversight Act.

The Inspector-General must serve impartially and independently and perform his or her functions in good faith and without fear, favour, bias or prejudice.[17]

As noted in Section 4.3.3, the Minister for Intelligence Services may assign functions to the Inspector-General;[18] appoint such number of persons to the OIGI as may be necessary for the performance of its functions;[19] and, acting with the concurrence of the JSCI, make regulations regarding, amongst other things, the performance by the Inspector-General of his or her functions, the reports to be submitted by the Inspector-General and the heads of the services, the suspension or removal from office of the Inspector-General, and the procedures for investigations undertaken by the Inspector-General.[20]

### 5.3 Refining the Mandate of the Inspector-General

The Inspector-General's mandate revolves around three roles. The first is the compliance or ombuds role, which entails monitoring compliance by the intelligence organisations with the Constitution and applicable legislation and policies, investigating complaints of non-compliance, abuse of power, misconduct and illegality by these organisations, and certifying the reports submitted by the heads of the organisations. The ombuds function is dominant in the Act and is spelt out clearly.

The second role relates to 'significant intelligence failures'. The heads of the services must report such failures and any corrective action to the Inspector-General.[21] However, the Act does not define 'significant intelligence failure' and, despite the legislation having been promulgated over a decade ago, the

[17] Section 7(10)(b) of the Intelligence Services Oversight Act.
[18] Section (7)(7)(c) of the Intelligence Services Oversight Act.
[19] Section 7(12) of the Intelligence Services Oversight Act.
[20] Section 8(1) of the Intelligence Services Oversight Act.
[21] Section 7(11)(b)(i) of the Intelligence Services Oversight Act.

Inspector-General and the heads of the services have yet to reach agreement on the meaning of this term.[22]

Nor does the Act indicate explicitly what the Inspector-General must do in relation to an intelligence failure. Presumably, he or she must investigate the matter for the purpose of certifying the report produced by the head of the service. Inspectors-general of intelligence in other countries are not charged with investigating intelligence failures.[23]

The third role of the Inspector-General is ill-defined. Section 7(7)(b) of the Act states that he or she must "review the intelligence and counter-intelligence activities of any service". Given the wording of the legislation, this review is different from the review of compliance and significant intelligence failures but its focus and purpose are unclear. The Inspector-General interprets section 7(7)(b) to mean an evaluation of the performance of the intelligence and counter-intelligence programmes and activities of the services in order to determine their effectiveness and efficiency.[24]

In our view the mandate of the Inspector-General should be confined to the ombuds role. The main reason for this is the limited capacity and resources of the OIGI. As discussed in Section 5.4, the staff contingent of the OIGI is not nearly large enough to deal adequately with the ombuds function, investigations of significant intelligence failures and reviews of the operational effectiveness of five intelligence organisations.

There is consequently a danger that the scope of activities impairs the Inspector-General's ability to perform the ombuds function, which is onerous and complex, particularly with respect to covert operations. It is also the most important aspect of the Inspector-General's mandate. The primary motivation for creating the post of Inspector-General was to prevent and detect abuse of

[22] South African Secret Service, 'Presentation to the Ministerial Review Commission', 31 January 2007, pg. 25.
[23] Meeting with the Inspector-General of Intelligence, 10 May 2007.
[24] Letter to the Commission from the Inspector-General of Intelligence, 31 May 2007.

power by the intelligence services and thereby avoid a recurrence of the abuses committed by the apartheid security services.[25]

Given this motivation, we agree with the Inspector-General's proposal that the ombuds function should also cover the South African National Academy of Intelligence (SANAI).[26] The Inspector-General should be empowered to review the extent to which the training conducted by SANAI is consistent with and helps to inculcate respect for constitutional rights and the rule of law.

If the investigation of significant intelligence failures were removed from the Inspector-General's mandate, then the President, the relevant Ministers, the JSCI or Parliament could determine the most appropriate means of investigating such failures on a case-by-case basis. In some instances they might choose to request the Inspector-General to undertake the investigation but in other cases a different form of review might be more suitable.

We must note that the Inspector-General and his staff do not agree with our view that the OIGI's mandate should be confined to the ombuds role. They believe that the various roles are interlinked and that reviewing the operational effectiveness of the intelligence services allows the OIGI to make constructive proposals which balance the criticisms emanating from the compliance function and thereby help to build positive relations with the services.[27] We are not convinced that this is essential, and there is nothing in the ombuds role that precludes constructive proposals being made.

[25] Task Team on the Review of Intelligence-Related Legislation, Regulation and Policies, 'Final Report of the Task Team on the Review of Intelligence-Related Legislation, Regulation and Policies', April 2006, pg. 28.
[26] Office of the Inspector-General of Intelligence, 'Submission to the Ministerial Review Commission. The Concept of the Control of the Civilian Intelligence Services', presented to the Commission on 29 January 2007, pg. 18.
[27] Meeting with the Inspector-General of Intelligence, 10 May 2007.

## 5.4 Increasing the Budget of the OIGI

There is a substantial gap between the OIGI's legislative mandate and its organisational capacity to implement that mandate. In May 2007, as a result of budgetary constraints, the OIGI had only fourteen staff. It had just received funds to increase that number to twenty, although its approved plans provided for twenty-eight staff. If all these posts were filled, the OIGI would be able to fulfil 70% of its mandate. To comply fully with all its legislative obligations, a staff complement of forty members is needed. This would require a doubling of the current budget.[28]

Because of the lack of capacity, the OIGI has only been able to carry out its oversight function at a minimum level of performance and reduced scope.[29] Both quality and quantity are bound to have suffered. The OIGI is meant to play a major role in preventing and detecting misconduct and illegality in the intelligence community but this is not possible to a satisfactory extent without additional resources.

## 5.5 Recommendations of the Legislative Review Task Team

The Task Team on the Review of Intelligence-Related Legislation, Regulation and Policies (hereafter the "Task Team"), established by Minister Kasrils in 2005, considered a number of topics regarding the Inspector-General and the OIGI.[30] In this section we present the Task Team's conclusions and recommendations and our own views on the issues in question.

[28] Letter to the Commission from the Inspector-General of Intelligence, 31 May 2007.
[29] Office of the Inspector-General, 'Submission to the Ministerial Review Commission', op cit, pg. 25.
[30] Task Team, 'Final Report', op cit, pp. 13, 28-31 and 65-67.

### *5.5.1 The independence of the OIGI*

The budget of the OIGI is appropriated in the intelligence services budget. One of the consequences of this arrangement is that the OIGI has to account financially and administratively to NIA, which is among the intelligence services it oversees, and the Director-General of NIA has ultimate authority in relation to administrative decisions of the OIGI. The Inspector-General insists that this undermines the OIGI's independence and is inappropriate.[31]

The Task Team recommended that the OIGI be given independent organisational status, allowing it to receive and manage its budget independently of NIA and affording the Inspector-General full control over the resources and activities of the Office. The OIGI could be established as either a government agency or a Schedule 3 organisation in terms of the Public Service Act No. 103 of 1994. The Inspector-General would remain functionally accountable to the JSCI but would be financially and administratively accountable to the Minister for Intelligence Services for the purposes of the Public Finance Management Act No. 1 of 1999.

We agree that the OIGI should have independent status. The process of establishing this status was underway in August 2008.[32]

### *5.5.2 Regulations governing aspects of the Inspector-General's work*

There are currently no ministerial regulations governing the investigations and inspections undertaken by the Inspector-General. There has consequently been uncertainty about the following matters: the question of whether the Inspector-General can subpoena witnesses; the rights to legal representation of a person under investigation; the enforceability of the findings of the Inspector-General; and the discretion of the Inspector-General to indemnify witnesses against self-incrimination.

[31] Office of the Inspector-General, 'Submission to the Ministerial Review Commission', op cit, pg. 25.
[32] Letter to the Commission from Minister Kasrils, 18 August 2008.

The Task Team concluded that there is an urgent need to issue ministerial regulations on the Inspector-General's investigations and inspections.

The Commission agrees with this position. We also agree with the Inspector-General's recommendation that the Minister urgently issue regulations on the reporting obligations of the heads of the services and the certification process that must be conducted by the Inspector-General.[33] In August 2008 we were informed that the Minister had submitted draft regulations on the Inspector-General to the JSCI for its consideration.[34]

*5.5.3 Aspects of the Inspector-General's investigations and inspections*

As noted above, there are a number of critical questions regarding the Inspector-General's investigations and inspections that are unclear:

- Should the Inspector-General have the power to subpoena witnesses? The Task Team argued that subpoena powers are unnecessary because the Act already makes it an offence to fail to co-operate with the Inspector-General.

  We agree with this position.

- Are the Inspector-General's findings enforceable? The Task Team maintained that the findings are not enforceable. The Inspector-General presents findings and recommendations to the heads of the services, the relevant Ministers and/or the JSCI, and these bodies must determine whether and how to act on the findings and recommendations.

  We agree with this position.

[33] Office of the Inspector-General, 'Submission to the Ministerial Review Commission', op cit, pg. 25.
[34] Letter to the Commission from Minister Kasrils, 18 August 2008.

- If the Inspector-General uncovers criminal activity by a member of an intelligence service, is he or she obliged to report this to the SAPS? The Task Team argued that the Inspector-General should inform the law enforcement authorities only in the event of a breach of the Intelligence Services Oversight Act. With respect to other laws, the Inspector-General should report a breach to the managers of the relevant intelligence service and they would be responsible for referring the matter to the law enforcement authorities.

  In our view the Inspector-General should report all offences to the SAPS. If this position is not accepted and the Inspector-General is expected to report certain offences to the managers of the relevant intelligence service, then it should be mandatory for them to report the matter to the police. Failure to do so should constitute an offence.

- Should persons appearing before the Inspector-General in the course of an investigation have the right to legal representation? The Task Team proposed that this right should not apply since the Inspector-General does not constitute a court, tribunal or disciplinary committee, his or her findings are not enforceable, and the issues under investigation are often extremely sensitive.

  We disagree with the Task Team's position. As a matter of natural justice, the right to legal representation should apply where the Inspector-General uncovers criminality and there is consequently the possibility of criminal charges being laid against a member of an intelligence service.

- Should the Inspector-General be able to indemnify witnesses whose evidence during an investigation might incriminate them? The Task Team stated that this would not be appropriate as the Inspector-General functions as an inspectorate rather than as a court.

We agree with this conclusion on the grounds that the Inspector-General is not a prosecuting authority or a judicial authority.

### *5.5.4 Consultation with the Inspector-General in drafting legislation and regulations*

The OIGI believes that the Inspector-General should be formally consulted when intelligence-related legislation, legislative amendments and regulations are being prepared. The motivation is that the OIGI's work provides it with insight into weaknesses in the legislative and regulatory framework.

The Task Team felt that making it compulsory to consult the Inspector-General in the drafting or amending of legislation and regulations would be an unnecessary additional burden on the legislation-making processes. However, such consultation should take place as a matter of good practice wherever possible.

In our opinion, consultation with the Inspector-General should be mandatory. We would go further and propose that the Inspector-General be consulted not only in relation to legislation and regulations but also in relation to the operational policies of the intelligence services. As explained in Section 11.7, a number of these policies reflect a poor grasp of the relevant legislative and constitutional provisions and this can result in unlawful and unconstitutional activity by intelligence officers.

### *5.5.5 Investigation of human resource complaints*

As noted in Section 5.2, the Inspector-General's functions include receiving and investigating complaints from members of the intelligence services about alleged maladministration, abuse of power and transgressions of the Constitution, applicable laws and relevant policies on intelligence and counter-intelligence. This has often been interpreted by members of the services to cover complaints and disputes relating to human resource issues.

The Task Team insisted that this is inappropriate because it takes time and effort away from the Inspector-General's main task, which is to conduct inspections and investigations relating to the *intelligence* legislation. In addition, there are adequate mechanisms for addressing human resource complaints. The Task Team recommended that the Inspector-General's legislative mandate be amended to exclude investigations into human resource complaints.

The Inspector-General has a less favourable perspective on the quality of human resource management in the intelligence services and maintains that the mechanisms for addressing staff grievances and disputes are not adequate (Section 11.5).[35]

The Commission has not examined the mechanisms for dealing with human resource grievances by members of the intelligence services. Nevertheless, we agree with the Task Team's recommendation. As discussed in Section 5.3, we believe that the Inspector-General's mandate should focus exclusively on the intelligence ombuds function.

## 5.6 The Inspector-General's Role in the Intelligence Crisis of 2005/6

As noted in Section 1.2, the Inspector-General played a prominent role in the intelligence crisis of 2005/6. Following the receipt of a complaint against NIA from Mr Saki Macozoma, a prominent businessman and political figure, Minister Kasrils requested the Inspector-General to investigate the matter. The Inspector-General issued a report that contained findings of misconduct and illegality by the head of NIA, Mr Billy Masetlha, and other senior officials. This led to their suspension and subsequent dismissal. In addition, criminal charges were laid against Mr Masetlha.

[35] Office of the Inspector-General, 'Submission to the Ministerial Review Commission', op cit, pp. 23-24.

The Inspector-General's investigation attracted negative comment from the JSCI, which criticised certain of the procedures followed in the investigation.[36] The JSCI's report was debated in Parliament and Minister Kasrils responded to the Committee's concerns.[37]

The Inspector-General's report was also criticised in a minority judgement of the Constitutional Court. Mr Justice Yacoob said that the public version of the report contained a number of amendments to the original classified report, some of which amendments deceived the public. The "conduct of the agency in producing the public version is as an exercise of public power inconsistent with the values mandated by our Constitution and is therefore, at the very least, regrettable".[38]

In November 2007 Mr Masetlha was acquitted on the charge of contravening the Intelligence Services Oversight Act by unlawfully and intentionally withholding information from the Inspector-General. Mr Masetlha claimed that he had sent the relevant information to the OIGI. The Court found that it was probable that his letter had gone astray in the Inspector-General's Office because evidence existed that the information had been received by the OIGI's staff.[39]

We have not conducted our own investigation into these matters since they were the subject of several court proceedings during the period of our review. For this reason, we have also refrained from expressing any judgement on the investigative methods and procedures used by the Inspector-General.

---

[36] Joint Standing Committee on Intelligence, 'Special Report of the Joint Standing Committee on Intelligence – On the Reports of the Inspector-General of Intelligence', 15 August 2006.
[37] Minister Ronnie Kasrils, 'Debate on the Report of the Joint Standing Committee on Intelligence (JSCI) in Response to the Investigation by the Inspector General', address in the National Assembly, 21 September 2006, available at www.intelligence.gov.za/Speeches/JSCI%20Response%2021%20Sept%202006.docv5.docFINAL2.doc.
[38] *Independent Newspapers (Pty) Ltd v Minister for Intelligence Services* CCT 38/07 [2008] ZACC 6, para 129.
[39] *Judgement in the District Court of Pretoria between the State and Billy Lesedi Masetlha*, Hatfield, case number 222/3511/2006, 28 November 2007, pg. 39.

Nevertheless, it seems clear from the events described above that a thorough evaluation of the Inspector-General's investigation is necessary. The evaluation would be valuable in identifying areas for improvement in the procedures and practices of the OIGI.

The evaluation should be initiated by the Minister for Intelligence Services once the relevant court proceedings have been concluded and should take account of the judgements emanating from these cases.

### 5.7 Recommendations

The Intelligence Services Oversight Act of 1994 should be amended so that the mandate of the Inspector-General is confined to the ombuds role, which entails monitoring compliance by the intelligence structures with the Constitution and applicable legislation and policies; investigating complaints of non-compliance, abuse of power, misconduct and illegality by these structures; and certifying the reports submitted by the heads of the structures. The mandate should not cover significant intelligence failures, the effectiveness and efficiency of intelligence and counter-intelligence operations, and human resource complaints.

If the investigation of significant intelligence failures were removed from the Inspector-General's mandate, then the President, the relevant ministers, the JSCI or Parliament could determine the most appropriate means of investigating such failures on a case-by-case basis.

The Inspector-General's ombuds role should be extended to cover SANAI. The Inspector-General should be empowered in law or by ministerial directive 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 budget of the OIGI should be increased so that the Inspector-General is able to employ sufficient staff to fulfil his or her legislative mandate in a satisfactory manner.

The OIGI should be given independent organisational status, allowing it to receive and manage its budget independently of NIA and affording the Inspector-General full control over the resources and activities of the Office. The Inspector-General would remain functionally accountable to the JSCI but would be financially and administratively accountable to the Minister for Intelligence Services for the purposes of the Public Finance Management Act No. 1 of 1999.

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

With respect to the Inspector-General's investigations and inspections:

- The Inspector-General should not have the power to subpoena witnesses.

- The Inspector-General should be obliged to report criminal conduct by a member of an intelligence service to the SAPS.

- The right to legal representation should apply where the Inspector-General uncovers criminality and there is consequently the possibility of criminal charges being laid against a member of an intelligence service.

- The Inspector-General should not be authorised to indemnify witnesses against criminal 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 for Intelligence Services 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. Amongst other things, it should have a website that provides contact details and describes its functions, activities and findings. This is necessary because the Office is intended to provide a mechanism for investigating complaints by members of the public and for assuring the Executive and the public that the intelligence services are conducting their activities within the parameters of the law.

## CHAPTER 6: THE MANDATE OF NIA

### 6.1 Introduction

In its submission to the Commission, NIA stated that its most important feature is its mandate.[1] This is because the mandate provides a fundamental basis for the Executive's determination of the Agency's priorities and for ministerial directions, funding, allocation of resources, targeting, planning and operations.

We share this view. NIA's mandate has a crucial bearing on its orientation and effectiveness and on the risk that it will interfere in the political process, infringe constitutional rights and subvert democracy.

In this Chapter we focus on the intelligence, departmental intelligence and counter-intelligence components of NIA's mandate. We discuss three major problems: NIA's mandate is too broad and ill-defined; its political intelligence function as currently conceived is inappropriate in a democracy; and there is an alarming absence of rules and executive guidelines in relation to NIA's counter-intelligence function.

The Chapter covers the following topics:

- The domestic intelligence function as provided for in legislation (Section 6.2).

- NIA's policy on its intelligence mandate (Section 6.3).

- The political and other problems associated with an overly broad mandate (Section 6.4).

[1] National Intelligence Agency, 'Base Document for Presentation on Matters Relating to the Terms of Reference of the Ministerial Review Commission', 24 January 2007.

- The dangers arising from NIA's political intelligence focus (Section 6.5).

- NIA's counter-intelligence function as provided for in legislation (Section 6.6).

- Departmental intelligence (Section 6.7).

- NIA's recommendations on its mandate (Section 6.8).

- Recommendations (Section 6.9).

## 6.2 The Domestic Intelligence Function as Defined in Law

One of NIA's primary functions is to gather, correlate, evaluate and analyse domestic intelligence in order to identify any threat or potential threat to the security of the Republic or its people and supply intelligence regarding such threats to NICOC.[2] 'Domestic intelligence' means "intelligence on any internal activity, factor or development which is detrimental to the national stability of the Republic, as well as threats or potential threats to the constitutional order of the Republic and the safety and well-being of its people".[3]

Two initial observations can be made about these provisions. First, NIA's mandate is extremely broad. The Agency is expected 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. This would give rise to an expansive agenda in any country. In South Africa, whose features include intense political competition, sporadic violence, chronic poverty and

[2] Section 2(1)(a) of the National Strategic Intelligence Act No. 39 of 1994.
[3] Section 1 of the National Strategic Intelligence Act.

underdevelopment in many sectors, a vast array of issues could be included under the intelligence mandate.

As discussed in Chapter 3, the White Paper on Intelligence of 1994 broadens the mandate considerably by defining 'security' as having political, economic, social, technological and environmental dimensions and as relating to "freedom from the vulnerability of modern society".[4] The White Paper goes so far as to state that one of the purposes of intelligence is "to assist good governance through providing honest critical intelligence that highlights the weaknesses and errors of government".[5]

Second, a number of the key terms in the legislative provisions referred to above are imprecise and ambiguous. The meaning of the terms 'security of the Republic and its people', 'national stability' and 'threats to the constitutional order' depends on one's conceptual and political perspective. Consequently, NIA's legal mandate can be interpreted in different ways. The mandate has in fact been reinterpreted three times since 1994.[6] The process of interpretation and reinterpretation has occurred exclusively within the state, however, and has not been subject to vigorous public and parliamentary debate.

The following Section presents NIA's policy on its mandate, which has not been presented to the National Assembly.

### 6.3 NIA's Policy on Its Intelligence Mandate

In the period 1994 to 1999 NIA interpreted its mandate narrowly, concentrating on terrorism, sabotage, subversion and organised crime. It subsequently broadened its focus in a manner deemed necessary in light of

[4] White Paper on Intelligence, 1994, pg. 3.
[5] White Paper on Intelligence, section 3.2.3.
[6] National Intelligence Agency, 'Base Document', op cit, para 3.5.

the White Paper on Intelligence of 1994 and the National Strategic Intelligence Act of 1994.

The new interpretation was contained in an operational directive entitled "NIA's Mandate and Operational Philosophy", issued in 2003.[7] It adopts a comprehensive approach to security that encompasses political, social, economic and environmental issues and is not limited to threats but also includes the identification of opportunities. The Directive interprets the mandate so broadly that "the Agency must inform decision-makers about every aspect of human endeavour upon which good order and the prospects for a prosperous future depend".[8]

Under the heading "Broad Areas of Interest and Focus", the Directive presents five categories: political intelligence; economic intelligence; organised crime and corruption; border intelligence; and special events. The focus on political and economic intelligence was included at the instruction of Cabinet and the President.[9]

The Directive's section on political intelligence begins by noting that in order to fulfil its mandate effectively, NIA must have a clear picture of political processes and dynamics in the country. This "calls amongst others for an understanding of the strengths and weaknesses of political formations, their constitutions and plans, political figures and their roles in governance, etc".[10] The development of this political understanding does not call for the application of intrusive or covert methods, however. Intrusive methods "shall only be applied where there is demonstrable reason to believe that criminal or unconstitutional acts are about to be committed or have already been committed".[11]

---

[7] National Intelligence Agency, 'NIA's Mandate and Operational Philosophy', Operational Directive OD.01, 2003.
[8] Ibid, para 2.4.3.
[9] National Intelligence Agency, 'Base Document', op cit, paras 3.6.3 and 3.6.4.
[10] National Intelligence Agency, 'NIA's Mandate', op cit, para 3.1.1.
[11] Ibid, para 3.1.1.

The focal areas under the heading “Political Intelligence” are listed as follows:

- Transformation and related issues within government and its constituent departments. This includes tensions that arise from the drive for representivity, or the lack thereof, and might result in deliberate subversion or sabotage within government departments.

- Competition between and within political parties that affects delivery. Such competition may negatively affect delivery of crucial services and result in security risks.

- Factors, issues and developments subverting the process of governance.

- The impact of political policy decisions and processes on national security and stability. The purpose of monitoring political decisions and processes is to advise political clients on the effectiveness of the decisions and indicate possible alternative ways of dealing with specific conflict situations.

- Imported issues, which include issues that could cause South Africa diplomatic embarrassment; foreign groups settling their disputes in South Africa; and the use of South Africa as a base from which to destabilise other countries.

- Activities such as terrorism, subversion and sabotage that are directly related to the destabilisation or overthrow of the constitutional order.

The Directive states that NIA’s focus on economic intelligence covers the following sub-categories:

- Macro economic issues, including domestic economic trends; threats to economic development; economic opportunities; strategic industries;

strategic parastatals; the impact of macro-economic policies; and trade agreements and relations.

- Socio-economic issues, which relate to social and economic development matters that impact on security and stability at national, provincial and local levels. This includes access to services and resources; poverty levels; the impact of HIV/AIDS; and employment trends.

- Technological issues, including strategic technologies; policy issues; opportunities; chemical, biological and defence industries; and patents and copyright.

- Environmental issues, including plunder of natural resources; environmental destruction; and environmental issues that could have economic implications for emerging sectors of the economy such as tourism and the fishing industry.

The category of organised crime and corruption includes major crimes that impact on national security and stability; transnational criminal structures and activities; and corruption of political authorities or government officials that perverts public administration, impairs good governance or deprives the citizenry of their needs.

The category 'border intelligence' covers criminal and unconstitutional activities that are perpetrated at or through the country's points of entry and exit.

'Special events' are events that are hosted in South Africa and have national or international significance. NIA's responsibilities include assistance with security arrangements and accreditation of participants.

NIA informed us that the targeting of persons and organisations for intelligence collection is subject to high level approval and must be motivated

on reasonable suspicion that the target has unconstitutional political intent. Information gathering is aimed at uncovering activities that do or could result in violent conflict, criminality or the undermining of the constitutional order. The positioning of political parties could be subversive if they undermine government initiatives in order to gain political support. Although the positioning of political parties and groups is part of the democratic process, it could become a security risk if contentious political and economic issues are used to fuel violence and cause instability in a region for the short-term advantage of a particular political party.[12]

NIA also told us that its political intelligence focus had caused some difficulties in ascertaining and pinpointing the Agency's exact mandate. After intensive discussion with the Minister in the wake of the intelligence crisis of 2005/6, the organisation decided to "move away from political intelligence *per se*" and "rephrase its 'political focus' to Social Stability Intelligence as part of the incorporation of South Africa as a developmental state into the intelligence mandate debate".[13] The aim is to meet the human security challenges of South Africa as a developmental state by focusing on two components, namely threats and risks to political stability and threats and risks to social stability.[14]

### 6.4 The Problems with an Overly Broad Intelligence Mandate

NIA's broad mandate derives from the National Strategic Intelligence Act of 1994 and is almost identical to the mandate of the apartheid-era National Intelligence Service as defined in the Bureau for State Security Act No. 104 of 1978.[15] NIA's interpretation of its mandate is informed by the concept of human security, which is the focus of the White Paper on Intelligence of 1994. Although human security is a progressive concept, there are severe problems

[12] National Intelligence Agency, 'Base Document', op cit, para 3.6.3.1.
[13] Ibid, para 3.6.3.2.
[14] Ibid.
[15] Information provided to the Commission by Dr Sandy Africa.

associated with the broad mandate. In this section we discuss problems of overreach, duplication and lack of focus; political problems; and problems relating to interpretation and prioritisation.

### *6.4.1 Problems of overreach, duplication and lack of focus*

If the domestic intelligence mandate is defined broadly and includes all dimensions of security, then the intelligence agency has to cover too much ground. NIA's thematic focus is so wide that it encompasses the focus of virtually every state department. This is patently impractical and unnecessary. NIA's staff cannot conceivably acquire a professional level of expertise in all facets of governance. They can consult the relevant experts but they will not themselves have comparable proficiency and there is consequently no reason to believe they can add anything of value.

By way of illustration, poverty, unemployment, HIV/Aids and other diseases are among the most serious threats to human security in South Africa. These issues are the subject of research and analysis by many governmental and non-governmental bodies. NIA is not able to supplement or even match their depth of knowledge. Nor should it be required to alert decision-makers to the importance and severity of the threats. The responsibility for identifying and addressing socio-economic threats to the security of our people lies with the Executive and with all government departments according to their respective mandates and areas of focus.

NIA's expertise and special powers to infringe the right to privacy are geared principally to gathering *secret* information about domestic security threats. More specifically, the organisation is designed and equipped to anticipate, detect and analyse major threats that are clandestine and entail criminality. Since this function is not undertaken by other government departments, it makes no sense for NIA to duplicate their work at the expense of pursuing its own most vital responsibility. Instead, as argued further below, it should concentrate on serious criminal offences. It would still have to analyse

political, social and economic dynamics but the purpose would be to anticipate and identify the planning and execution of these offences.

### *6.4.2 Political problems*

An overly broad domestic intelligence mandate can lead to NIA focusing in an inappropriate manner on lawful political and social activities. It can also lead to the politicisation of the Agency, which has to assess whether lawful political and social activities are actually or potentially destabilising. These problems are especially serious since NIA is able to operate secretly and has the power to infringe constitutional rights.

The risk of politicisation and interference in politics is heightened by the fact that domestic intelligence must cover "threats or potential threats to the constitutional order of the Republic".[16] This imprecise term is not defined in the intelligence legislation. It could be construed narrowly to refer only to major crimes such as terrorism and treason. NIA uses the term vaguely, however, seeking to detect activities that "do or could result in violent conflict, criminality or the undermining of the constitutional order".[17] In this formulation, undermining the constitutional order is different from violence and criminality and must therefore include certain lawful activities. NIA's policy provides no indication of what these activities might be.

In a democracy it is wholly inappropriate for an intelligence service to make judgements on whether lawful activities are threats to the constitutional order. By way of comparison, the definition of security threats in the Canadian intelligence legislation expressly excludes "lawful advocacy, protest or dissent" unless such activity is undertaken in conjunction with one of the designated security threats.[18]

---

[16] Section 1 of the National Strategic Intelligence Act.
[17] National Intelligence Agency, 'Base Document', op cit, para 3.6.3.1.
[18] Section 2 of the Canadian Security Intelligence Service Act of 1984, available at http://laws.justice.gc.ca/en/showtdm/cs/C-23. An example of a 'designated security threat' is the 'destruction or overthrow by violence of the constitutionally established system of government in Canada'.

The perceived role of the intelligence community as policy advisers to the Executive is also unacceptable. As noted in Section 6.2, the White Paper on Intelligence maintains that intelligence must assist good governance by highlighting the errors and weaknesses of government. According to NIA's operational directive discussed in Section 6.3, the Agency must monitor the impact of political policy decisions and processes in order to advise government on the effectiveness of its decisions and indicate alternative ways of dealing with conflict situations.

This approach is unsound, if not dangerous. In addition to Parliament and the critical role played by the media and civil society groups, the Constitution establishes independent bodies that have oversight functions in relation to government. NIA is not among these bodies. In terms of the Constitution, it is one of the security services. There is no indication in the Constitution or legislation that it should operate as an elite policy organisation advising government on its mistakes and weaknesses. If it played this role in earnest, it would become a shadow and shadowy watchdog of government business.

The problems arising from NIA's political intelligence focus are examined further in Section 6.5.

### *6.4.3 Prioritisation and interpretation problems*

Regardless of the resources at its disposal, NIA cannot possibly focus on every actual and potential threat to the constitutional order, the security of the country and the well-being of its people. A broad mandate makes it necessary to determine not only the Agency's operational priorities but also its higher level policy priorities. Various criteria can be used to establish these priorities, such as the severity and impact of a threat, whether the threat entails violence, whether it is clandestine and whether it is directed at the overthrow of the state.

The responsibility for determining the policy criteria and policy priorities should lie with the Executive. In a constitutional democracy where "national security is subject to the authority of Parliament and the national executive",[19] this responsibility should be exercised in consultation with Parliament. This is currently not the case. As discussed in Section 12.3.1, the National Intelligence Priorities approved annually by Cabinet are confidential.

The interpretation of NIA's mandate should similarly be subject to parliamentary consideration and public debate. Given the Constitution's emphasis on accountability and transparency as fundamental tenets of governance, it is unacceptable that NIA's mandate has been reinterpreted three times since 1994 without discussion in the National Assembly and without the results being disclosed publicly.

More specifically, it is inappropriate that NIA's political intelligence function is addressed only in a confidential departmental directive and is not even mentioned, let alone regulated, in the intelligence legislation or any public policy document. For several years an intelligence function that carried the risk of subverting the democratic process thus lay outside the realm of public knowledge. This changed only when, as described in the following Section, the Inspector-General of Intelligence questioned the propriety of political intelligence in his report on the intelligence crisis of 2005/6.

The question of whether NIA should monitor a particular individual or organisation involved in criminal activity is not a matter for parliamentary and public debate. Yet the larger policy question of whether NIA should be allowed to monitor and spy on political organisations engaged in lawful activity and, if so, with what oversight and controls, is a matter that demands the attention of Parliament and the public.

[19] Section 198(d) of the Constitution.

## 6.5 The Dangers of Political Intelligence

In this Section we examine at greater length the dangers of political intelligence and conclude that, as currently conceived, it should be abandoned. We take account of the perspectives of the Minister for Intelligence Services, the Inspector-General of Intelligence and the Task Team on the Review of Intelligence-Related Legislation, Regulation and Policies (hereafter "the Task Team").

### *6.5.1 The Minister's perspective*

In July 2008 Minister Kasrils delivered a speech in which he cautioned against an overly broad intelligence mandate:

> 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 those issues is not only inefficient, but also may 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, where a general complaint about the ubiquitousness of NIA members was raised by trade unionists, political parties, community organizations and the media alike.
>
> The experience of such protests, as well as 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...
>
> My contention… 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.[20]

### *6.5.2 The Inspector-General's perspective*

NIA's political intelligence focus lay at the heart of the intelligence crisis that occurred in 2005/6. In his report on the crisis, as noted previously, the Inspector-General of Intelligence found that the head of NIA had unlawfully ordered the interception of the communication of parliamentarians and other politicians.[21] The interception formed part of an intelligence project whose objective was to assess the impact of the presidential succession debate on the political climate and stability of the country.[22]

The Inspector-General emphasised the significant risks associated with political intelligence, namely "the risk of undermining constitutionally protected party political freedoms and of descending into the abyss of abuse of state resources and compromise of intelligence mandate integrity".[23] He concluded that "in a young democracy such as ours", the question is whether political

[20] Minister Ronnie Kasrils, 'To Spy or Not to Spy? Intelligence and Democracy in South Africa', Institute for Security Studies Public Dialogue Series, Pretoria, 3 July 2008, pp. 10-12, available at www.intelligence.gov.za/Speeches/2008/ISSSpeech03July2008.doc.
[21] Office of the Inspector-General of Intelligence, 'Executive Summary of the Final Report on the Findings of an Investigation into the Legality of the Surveillance Operations Carried out by the NIA on Mr S Macozoma. Extended Terms of Reference Report on the Authenticity of the Allegedly Intercepted E-Mails', media briefing, 23 March 2006.
[22] Ibid, pp. 15-16.
[23] Ibid, pg. 18.

intelligence "should be practiced at all, and if so, what the parameters should be that define and encompass national security interests".[24]

### *6.5.3 Special Report of the Legislative Review Task Team*

In light of the Inspector-General's reports on the intelligence crisis of 2005/6, Minister Kasrils requested the Task Team to prepare a special report and recommendations on the governance of political intelligence.[25]

The Task Team's report stated that political intelligence is intended to enable NIA to provide a general picture of the political stability of the country, as well as to identify issues that might potentially undermine national security and stability.[26] The report added the following in this regard:

> In a young democracy such as our own, where our new society is built over the racial, class, ethnic and ideological fault-lines of our difficult past, it can validly be said that many of the potential threats to national security on the domestic front will emanate from the political terrain. The line between legitimate political activity and illegal or unconstitutional political activity is still somewhat shaky. In order, therefore, for intelligence to provide forewarning to government on threats to security, it needs to monitor this shaky line and be able to quickly adapt its collection methods when this line is crossed.[27]

The report concluded that the conduct of political intelligence by NIA is a legitimate activity because the National Strategic Intelligence Act of 1994 mandates the Agency to gather, correlate, evaluate and analyse domestic

---

[24] Office of the Inspector-General, 'Executive Summary', op cit.
[25] The Task Team is described in Section 1.6.
[26] Task Team on the Review of Intelligence-Related Legislation, Regulation and Policies, 'Special Report of the Legislative Review Task Team on the Superintendence and Oversight of the Conceptualisation, Planning and Execution of Political Intelligence', May 2006, pg. 4.
[27] Ibid, pg. 5.

intelligence in order to identify any threat or potential threat to the security of the Republic or its people.

The bulk of the Task Team's report is devoted to the prevention of unjustified resort to intrusive methods that infringe the right to privacy. The Task Team's proposals in this regard are discussed in Chapter 9. The key issue for present purposes is the Task Team's assertion that intrusive methods are justified in relation to the threat of "large-scale political instability"[28] and "reasonable suspicion of threats to national security and stability".[29]

In our view this perspective highlights one of the dangers of NIA's political intelligence focus: it opens the door to spying on and infringing the constitutional rights of people and organisations that are engaged exclusively in lawful activity. We argue in Chapter 7 that intrusive methods should only be used where there are reasonable grounds to believe that illegal actions have been committed or are being planned.

### *6.5.4 The risk of abuse*

Intelligence officers and members of the Executive can easily abuse the political intelligence function in a manner that politicises intelligence, confers an unfair advantage on some politicians and subverts the democratic process. The report of the Task Team does not consider these problems but there are numerous ways in which they can occur:

- Intelligence officers might present political information and analysis in a fashion that deliberately favours one party, faction or politician and prejudices others. This can happen if the intelligence officers want to enhance their influence or if they have an allegiance to certain politicians.

[28] Task Team, 'Special Report', op cit, pg. 7.
[29] Ibid, pg. 11.

- One of the clients of the intelligence agency might request and/or use political intelligence with the aim of gaining an advantage over an opposition party or an opponent within the same party.

- If the Executive is concerned about political instability, it is more likely to request the intelligence agency to monitor and investigate its opponents than monitor and investigate its own behaviour.

- Political intelligence reports might cover a number of political parties and factions within a party but the reports are not made available to all of them. This is not illegal but in the competitive world of politics it might confer an unfair advantage on the recipients of the reports.

- In order to prepare comprehensive and accurate political intelligence reports, intelligence officers might be tempted to use intrusive methods when there are no legitimate grounds for doing so.

- Intelligence officers and their clients might leak political intelligence to the media in order to spread misinformation and cast suspicion over political opponents.

- A political intelligence focus ineluctably draws the intelligence agency into the arena of party politics and creates or increases the risk of politicising the agency and its members. When the agency is politicised, there is a greater risk that it will interfere in the political process.

- A political intelligence focus can give rise to public suspicion that the intelligence agency is interfering in politics. If the agency is caught doing this, its reputation will suffer lasting damage.

The intelligence services are prohibited from advancing or prejudicing the interests of political parties. This prohibition appears in NIA's operational directive on its mandate and is also contained in the Constitution, legislation,

intelligence regulations and the White Paper on Intelligence (Section 11.3). Nevertheless, the risk of political abuse exists and is heightened by the fact that intelligence officers can operate secretly and interact informally with politicians. They can interfere in politics in surreptitious and subtle ways, reducing substantially the ability of control and oversight bodies to detect and stop transgressions.

It must be emphasised that the political problems identified in this Section are not hypothetical. They have materialised in South Africa and other democratic countries, severely undermining public confidence in the intelligence services.

*6.5.5 Conclusions*

NIA should abandon its political intelligence focus as currently conceived. Regardless of whether our democracy is young or old, it is not appropriate in any democracy for an intelligence agency to monitor and report on transformation within government departments, on competition between and within political parties and on the impact of political policy decisions and processes. Nor is it appropriate for an intelligence agency to violate the rights of persons and organisations that are acting lawfully.

As reported in Section 6.8, NIA shares many of these concerns about its political intelligence focus.

We are convinced that NIA's intelligence mandate should be narrowed to focus primarily on major crimes like terrorism, treason, organised crime, large-scale violence and systemic corruption. We discuss this approach at greater length in Section 6.9, which contains our recommendations.

Abandoning its political intelligence focus would not mean that NIA should ignore the political terrain. It must at all times have a good understanding of political and social dynamics at national and local levels. But it would not be acting as a secret watchdog over political activity, political parties and

government. Instead, it would monitor the political and social environment for the following purposes: to identify the potential for large-scale violence; to detect and contribute to the prevention of criminal activity and violence; to gather intelligence on the plans, methods and motivation of persons engaged in serious crime; to forewarn and advise the Executive on these threats to security; and to contribute to law enforcement.

In a democracy everyone is equal before the law and subject to the rule of law. Members of political organisations should enjoy no special protection if they engage in crime. If they are involved in the criminal activities that fall within NIA's mandate, then they should be the target of intelligence monitoring. This is a high level crime intelligence function rather than a political intelligence function.

## 6.6 NIA's Counter-Intelligence Function as Defined in Law

### *6.6.1 The National Strategic Intelligence Act*

The National Strategic Intelligence Act states that NIA shall fulfil the national counter-intelligence responsibilities and for this purpose shall conduct and co-ordinate counter-intelligence and gather, correlate, evaluate, analyse and interpret information regarding counter-intelligence in order to i) identify any threat or potential threat to the security of the Republic or its people; ii) inform the President of any such threat; iii) supply (where necessary) intelligence relating to any such threat to the police for the purpose of investigating an offence; iv) supply intelligence relating to any such threat to the Department of Home Affairs for the purpose of fulfilling any immigration function; and v) supply intelligence relating to national strategic intelligence to NICOC.[30]

'Counter-intelligence' means "measures and activities conducted, instituted or taken to impede and to neutralise the effectiveness of foreign or hostile

[30] Section 2(1)(b) of the National Strategic Intelligence Act.

intelligence operations, to protect intelligence and any classified information, to conduct security screening investigations and to counter subversion, treason, sabotage and terrorism aimed at or against personnel, strategic installations or resources of the Republic".[31]

*6.6.2 Comment*

Counter-intelligence entails four functions, two of which are clear and properly regulated: to protect intelligence and classified information, and to conduct security screening operations.[32]

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. What is meant by 'impede', 'neutralise' and 'counter'? Which counter-intelligence measures and activities are legitimate and which are illegitimate? NIA's submission to the Commission notes with concern that the legislation does not provide clear guidelines in relation to countermeasures.[33] In fact, the Act does not provide any guidelines at all.

By way of comparison, the Regulation of Interception of Communications and Provision of Communication-Related Information Act No. 70 of 2002 provides that the security services may not intercept private communication without judicial authorisation. The Act contains detailed guidelines, criteria and procedures for obtaining this permission (Section 8.4.1). The level of authorisation is high and the criteria for obtaining judicial permission are strict because interception of communication violates the constitutional right to privacy. Counter-intelligence, which might similarly entail infringements of rights, is covered by only a few lines in the National Strategic Intelligence Act.

[31] Section 1 of the National Strategic Intelligence Act.
[32] We discuss the protection of classified information in Chapter 12. Security screening is covered in section 2A of the National Strategic Intelligence Act.
[33] National Intelligence Agency, 'Base Document', op cit, para 3.7.1.

It is a matter of great concern that offensive countermeasures, which carry the risk of infringing constitutional rights and interfering in lawful political and social activities, are not subject to proper rules and legislative constraints. This creates two dangers: that NIA develops an inappropriate interpretation of its counter-intelligence mandate; and that NIA's countermeasures infringe constitutional rights without proper oversight and without sufficient cause and sense of caution. The relevant rights include the rights to freedom of association[34], to campaign for a political party or cause,[35] and to assemble, demonstrate, picket and present petitions.[36]

We therefore support NIA's view that there must be clear guidelines, principles, authorisation and criteria governing the use of countermeasures. According to NIA, "intrusive and clandestine collection techniques must be conducted in a legal and ethical manner and must be weighed against possible damage to constitutional rights, basic democratic principles as well as diplomatic and international relations. The need to protect national security must be balanced by respect for individual rights and freedom".[37]

The White Paper on Intelligence of 1994 contains two important constraints on countermeasures, which should be incorporated into the intelligence legislation:

> Measures designed to deliberately interfere with the normal political processes in other countries and with the internal workings of parties and organisations engaged in lawful activity within South Africa, must be expressly forbidden.
>
> No intelligence or security service/organisation shall be allowed to carry out any operations or activities that are intended to undermine, promote or influence any South African political party or

[34] Section 18 of the Constitution.
[35] Section 19(1)(c) of the Constitution.
[36] Section 17 of the Constitution.
[37] National Intelligence Agency, 'Base Document', op cit, para 3.8.2(i).

> organisation at the expense of another by means of any acts (e.g. 'active measures' or 'covert action') or by means of disinformation.[38]

Another set of problems arises from the definition of 'subversion' in the National Strategic Intelligence Act. Subversion entails "any activity intended to destroy or undermine the constitutionally established system of government in South Africa".[39] It is not at all clear what 'undermining' the system of government means. Since the definition does not require subversive activity to be illegal, it is possible that lawful political action might be adjudged to be 'undermining' and thus subversive. In a democracy such judgements are dangerous and should not be made by an intelligence agency. The solution to these problems is to define subversive activities as having a violent or otherwise criminal character.[40]

### 6.7 Departmental intelligence

The National Strategic Intelligence Act provides that NIA must gather departmental intelligence at the request of any interested department of State and, without delay, evaluate and transmit such intelligence and any other intelligence at the disposal of the Agency which constitutes departmental intelligence to the department concerned and to NICOC.[41]

As noted in Section 4.4.1, 'departmental intelligence' means "intelligence about any threat or potential threat to the national security and stability of the

---

[38] Quoted in National Intelligence Agency, 'Base Document', op cit, para 3.7.1.
[39] Section 1 of the National Strategic Intelligence Act.
[40] This is the case with the Canadian Security Intelligence Service Act of 1984. Section 2 of the Act defines "threats to the security of Canada" to include, among other things, "activities directed towards undermining by *covert unlawful* acts, or directed toward or intended ultimately to lead to the destruction or overthrow by *violence* of, the constitutionally established system of government in Canada" (emphasis added).
[41] Section 2(1)(c) of the National Strategic Intelligence Act.

Republic that falls within the functions of a department of State, and includes intelligence needed by such department in order to neutralise such a threat".[42]

We have three concerns about NIA's departmental intelligence function. First, the legislation does not indicate who is entitled to request NIA to provide departmental intelligence, to whom the request should be directed, and whether the Minister for Intelligence Services should be informed of such requests (Section 4.4.5).

Second, there are no regulations or ministerial directives governing the provision of departmental intelligence. The gaps in the legal and regulatory framework create the risk of political mischief and abuse of intelligence (Section 4.4.5).

Third, our misgivings about the overly broad and poorly defined legislative provisions on NIA's domestic intelligence function apply equally to the legislative provisions on the departmental intelligence function. Both of these functions need to be narrowed and made clearer (Section 6.9).

## 6.8 NIA's Recommendations

In this Section we present NIA's concerns and recommendations regarding its mandate. These concerns and recommendations appear in the Agency's submission to the Commission.[43]

### *6.8.1 NIA's concerns about its mandate*

NIA believes that its mandate is ambiguous, insufficiently clear and open to interpretation. The mandate does not provide a clear definition of 'threats to the Republic' and 'threats to national security'. This leads to incoherent

[42] Section 1 of the National Strategic Intelligence Act.
[43] National Intelligence Agency, 'Base Document', op cit, pp. 33-35.

interpretations of the mandate and creates difficulties in prioritising and targeting.

A further problem is that Executive tasking of NIA across the broad spectrum of human security and political issues could impact on the neutrality of the Agency and create tension between NIA and the Executive. The risk of tension increases if NIA is unable to satisfy the intelligence requirements of its Executive clients because of its limited resources and capacities.

NIA maintains that its mandate should not be to monitor and report on the performance of the state and social and economic delivery programmes. This can lead to perceptions that social, development and economic issues have been securitised. The Agency should not have an oversight role with regard to social and development matters and should not be the social watchdog of society.

NIA believes that is problematic for it to monitor the consequences of political and policy decisions and processes, to monitor the impact of political rivalry on national security and stability, to advise the Executive on the effectiveness of its decisions and to indicate alternative ways of dealing with conflicts. These functions might be abused and/or interpreted as efforts by a party political apparatus to deal with political opponents in an undemocratic manner. Such abuse and perceptions would compromise NIA's credibility. NIA must limit its focus within the political arena to suspected unconstitutional activities by political parties or their members, subject to the constitutional obligation that the security services do not behave in a partisan manner.

### *6.8.2 NIA's recommendations*

Given the many problems associated with a broad interpretation of the domestic intelligence mandate, NIA recommends that the national security policy of government should provide a more unambiguous definition of security threats and adopt a more narrow/traditional approach to the

interpretation of the Agency's mandate. This would be in alignment with international practice, as in the case of MI5 in Britain and the Canadian Security Intelligence Service.

NIA's mandate should be redefined to stipulate that the Agency will focus primarily on, and have the national responsibility for, the following:

- Countering terrorism, sabotage, subversion and proliferation [of weapons of mass destruction] as the principal threats to national security.

- The full spectrum of counter-intelligence measures, including personnel and information security within government departments and institutions as provided for in the National Strategic Intelligence Act of 1994.

- Organised crime and corruption, provided that NIA's involvement in the collection of crime intelligence remains, to the greatest extent possible, limited to the end result of intelligence processes (i.e. evaluated strategic or tactical information) and/or to conduct countermeasures and/or to provide crime intelligence to the SAPS for the purposes of investigating an alleged offence.

- The provision of economic intelligence with the aim of providing intelligence in support of government's economic initiatives and policies that will also be adequate to protect and promote South Africa's national economic interests.

This more classical approach to the interpretation of NIA's mandate would still require non-intrusive environmental scanning to be done in order to contextualise the root causes of terrorism, subversion, sabotage and organised crime as well as to identify in a timely manner the signals/indicators that these security problems are developing. NIA would have to prioritise the fields and levels of environment scanning/monitoring on the basis of a careful

analysis and estimation of the security risks and the potential or opportunities for anti-constitutional actions.

## 6.9 Recommendations

### *6.9.1 The domestic intelligence mandate*

We support NIA's view that the concept of 'security threats' should be defined more clearly and that the Agency should have a narrower mandate.

More specifically, we agree with NIA's recommendation that its mandate should focus on terrorism, sabotage, subversion, espionage, proliferation of weapons of mass destruction, organised crime and corruption. In addition, we believe that the mandate should cover large-scale violence and drug trafficking. These threats have common features: they are illegal; they are organised secretly; they entail some kind of conspiracy; and they can inflict extensive damage on the state, society, the economy and/or individuals. They therefore warrant the attention of the domestic intelligence agency, which has legal powers that enable it to uncover secret conspiracies.

The term 'unconstitutional activity' as a security threat should either be defined properly or dropped. It is currently used to mean something different from 'illegal activity' but there is no indication of the kind of activities that are covered by the term.

We support the retention of 'border intelligence' as part of NIA's mandate. South Africa's borders are porous, border posts are sometimes areas of concentrated cross-national criminal activity, harbours and airports are complex systems and there is the possibility of corruption among customs officials. It consequently makes sense for NIA to retain its specialised understanding and monitoring of borders and border posts.

We do not endorse NIA's recommendation that it should retain its focus on economic intelligence in support of government's economic policies and initiatives. As argued in Section 6.4.1, there is no need for the Agency to duplicate the work and expertise of other government departments and non-governmental specialists on the economy. If NIA is to have an economic focus, it should be limited to crimes that have an economic or financial character or a severe impact on the economy.[44]

The National Strategic Intelligence Act should be amended to reflect the preceding recommendations. NIA's intelligence mandate should not be based on imprecise terms like threats to 'national stability', the 'constitutional order' and the 'well-being of the people'. Instead, the mandate should be defined more concretely and specifically with reference to terrorism, sabotage, subversion, espionage, proliferation of weapons of mass destruction, drug trafficking, organised crime, large-scale violence, corruption and specified financial and economic crimes (hereafter the 'designated security threats').

The term 'subversion' should be redefined to cover activities that are intended to destroy or undermine the constitutional system of government through the use of violence or by other criminal means.

The legislation should state that security threats exclude lawful advocacy, protest, dissent or other activity unless undertaken in conjunction with one of the designated security threats.

In relation to the designated security threats, NIA should have the following functions:

- to predict, detect and analyse the threats;

[44] At a meeting held on 12 October 2007, NIA informed the Commission that it had abandoned its economic intelligence focus. The targeted focus in this area is now on economic crimes, such as the financing of terrorism.

- 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 about the threats;

- to provide strategic intelligence to NICOC; and

- to contribute to law enforcement and preventive action by providing intelligence to the SAPS, the Department of Home Affairs and other government departments.

It will evident from this list of functions that NIA's mandate, despite focusing on serious crimes, would be completely different from the mandate of the SAPS. Whereas the emphasis of the police is on law enforcement and criminal investigation for the purpose of prosecution, the emphasis of the domestic intelligence agency would be on analysis, prediction, prevention, forewarning and advising the Executive.

It will be necessary to determine priorities within some of the designated threat categories, such as organised crime and corruption. As is currently the practice, on an annual basis Cabinet should identify National Intelligence Priorities based on the National Intelligence Estimate conducted by NICOC, and NIA should determine its operational priorities accordingly.

We agree with NIA that it should abandon its political intelligence focus as currently conceived. The Agency will still have to undertake non-intrusive monitoring of the political and socio-economic environment. In order to avoid any relapse into 'political intelligence', the aims of the monitoring should be spelt out clearly: to predict and detect the designated threats that fall within NIA's mandate; to understand the dynamics and causes of these threats; to

forewarn and advise the Executive about the threats; and to provide intelligence to NICOC, the SAPS and other relevant departments.

As discussed further in Chapter 7, the intelligence legislation should prohibit the use of intrusive methods where there are no reasonable grounds to believe that the target has committed or is about to commit an unlawful act.

*6.9.2 The counter-intelligence mandate*

NIA should continue to perform the counter-intelligence functions of security screening, protection of intelligence and classified information, and any other defensive function that is provided for in law.

The National Strategic Intelligence Act should define more precisely, and should regulate, the functions of impeding and neutralising the effectiveness of foreign or hostile intelligence operations and countering the designated threats.

The legislation should prohibit the intelligence services from interfering with, and using countermeasures in relation to, lawful political and social activities in South Africa and other countries.

The legislation should also prohibit the intelligence services from disseminating false or misleading information to the public.

In addition to tighter legislative provisions, there is a need for ministerial regulations. The National Strategic Intelligence Act provides that the Minister for Intelligence Services may, after consultation with the JSCI, make regulations regarding the co-ordination of counter-intelligence by NIA.[45] The regulations should cover guidelines, principles and authorisation for the use of countermeasures.

[45] Section 6(1)(e) of the National Strategic Intelligence Act.

*6.9.3 The departmental intelligence mandate*

In Section 4.9 we make recommendations on departmental intelligence. These recommendations can be summarised as follows:

- The Minister for Intelligence Services should issue policy and procedural guidelines that regulate and expedite the provision of departmental intelligence.

- The provision of departmental intelligence should be subject to the Minister's approval and any conditions that he or she might set.

- 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 Premier in the case of a provincial administration or department, and the request must be made to the Minister for Intelligence Services.

In addition, we recommend that the focus of departmental intelligence be narrowed in accordance with our preceding recommendations on narrowing NIA's intelligence mandate. Departmental intelligence should be confined to intelligence regarding security arrangements and the designated security threats and would be provided to a department where this is necessary, and only to the extent that it is necessary, for the department to take action in accordance with its mandate.

## CHAPTER 7: INTRUSIVE OPERATIONS

### 7.1 Introduction

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. This is principally because these methods entail an infringement of the right to privacy. This right is covered by section 14 of the Constitution as follows:

> Everyone has the right to privacy, which includes the right not to have a) their person or home searched; b) their property searched; c) their possessions seized; or d) the privacy of their communications infringed.

Intrusive measures also infringe the Constitution's provision on dignity, which states that "everyone has inherent dignity and the right to have their dignity respected and protected".[1] In addition, intrusive methods that are used against politicians, activists and organisations might breach the constitutional rights to freedom of association[2]; to campaign for a political party or cause;[3] or to assemble, demonstrate, picket and present petitions.[4]

Intrusive methods of investigation can play a crucial role in uncovering criminal activities and conspiracies but they can also be misused to subvert the democratic process, interfere with lawful political and social activity and create an unfair advantage for some politicians and parties.

Our central concern in this Chapter is that certain intrusive methods employed by the intelligence organisations are not covered by legislation and are

[1] Section 10 of the Constitution.
[2] Section 18 of the Constitution.
[3] Section 19(1)(c) of the Constitution.
[4] Section 17 of the Constitution.

therefore unconstitutional. In the absence of legislation with adequate safeguards determined by Parliament, citizens and foreign nationals in South Africa are not protected against unwarranted infringements of their constitutional rights by the intelligence services. We propose that legislation be introduced to regulate the use of all intrusive methods in a consistent fashion. Informed by judgements of the Constitutional Court, we identify the key elements that ought to be contained in the legislation.

The Chapter covers the following topics:

- The constitutional necessity for legislation and safeguards (Section 7.2).
- Constitutional Court judgements on infringements of the right to privacy (Section 7.3).
- The grounds for permitting the use of intrusive methods by the intelligence services (Section 7.4).
- Judicial authorisation for intrusive methods (Section 7.5).
- Ministerial approval of intrusive methods (Section 7.6).
- Recommendations (Section 7.7).

The interception of electronic communication undertaken by the NCC is dealt with separately in Chapter 8. The operational controls of the intelligence services with respect to intrusive measures are discussed in Chapter 9.

## 7.2 The Constitutional Necessity for Legislation and Safeguards

South African intelligence officers have defined intrusive methods as follows:

> Intrusive methods of intelligence collection include any methods that infringe on the constitutional right to privacy such as communication interception, physical and electronic surveillance, infiltration of organisations, searches, etc.[5]

Because intrusive methods infringe the right to privacy, they may only be used in a manner that complies with the provisions on limitation of rights as set out in section 36(1) of the Constitution.[6] Intrusive methods are thus unconstitutional unless they are employed in terms of law of general application. The legislation must specify the circumstances that warrant the use of intrusive methods and must include safeguards that protect the right to privacy.

The Inspector-General of Intelligence puts the matter in the following way:

> A limitation of [constitutional] rights may be justified on grounds of threats to national security. Such limitation should meet the test of proportionality which includes the nature of the right and the importance of the purpose of the limitation. As such the capacity to gather intelligence *should be matched by equally strong safeguards that protect the constitutional rights of citizens and sustain an open and democratic society* (emphasis in the original).[7]

> Any special powers or immunities granted to members of an intelligence agency to gather domestic intelligence, which are not possessed by ordinary citizens, must be *specifically authorised and documented* by a democratically elected authority. Except in cases

[5] Task Team on the Review of Intelligence-Related Legislation, Regulation and Policies, 'Final Report of the Task Team on the Review of Intelligence-Related Legislation, Regulation and Policies', April 2006, pg. 55.
[6] Section 36(1) of the Constitution is reproduced in Section 2.3 of the Report.
[7] Office of the Inspector-General of Intelligence, 'Submission to the Ministerial Review Commission. The Concept of the Control of the Civilian Intelligence Services', presented to the Commission on 29 January 2007, pg. 8.

of national emergency, the granting authority shall be the legislative branch (emphasis in the original).[8]

While all intrusive methods employed by organs of state are constitutionally and politically sensitive, the use of these methods by intelligence services is especially sensitive and should be treated with particular caution. There are several reasons for this:

- The intelligence services employ intrusive measures secretly and the person under scrutiny is unlikely to ever learn of the investigation. As a result, the targeted person cannot object to the measures and challenge their validity in court. Unable to mount a legal challenge to the intrusion, the person is effectively deprived of his or her rights relating to just administrative action[9] and access to courts.[10]

- The high level of secrecy also reduces substantially the efficacy of oversight mechanisms and the possibility of detecting illegality and abuse of power by intelligence officers.

- Intrusive operations might uncover intimate personal information that has nothing to do with the security of the country. Consequently, the extent to which the right to privacy is violated might be far greater than is necessary or intended.

- Intrusive measures invariably encroach on the privacy of individuals with whom the targeted person has contact but who are not themselves the subject of any intelligence investigation.

- The gathering of information about a targeted person is not a fleeting event and the collected information is not forgotten once the investigation is over. Sensitive information about the targeted person, and possibly also

[8] Office of the Inspector-General, 'Submission', op cit, pg. 11.
[9] Section 33 of the Constitution.
[10] Section 34 of the Constitution.

his or her family members, friends and colleagues, is recorded in files that are retained by the intelligence service.

Legislation currently permits the intelligence services to intercept communication and enter and search premises. The use of these measures is covered in considerable detail in the Regulation of Interception of Communications and Provision of Communication-Related Information Act No. 70 of 2002. The Intelligence Services Act No. 65 of 2002 also contains provisions on entry, search and seizure.

Other intrusive methods – such as infiltration of an organisation, physical and electronic surveillance, and recruitment of an informant who reports on the private affairs of an individual or organisation – are not regulated by legislation and are therefore unconstitutional. In addition, as discussed in Chapter 8, the communication interceptions undertaken by the NCC are not compliant with the Constitution in all respects.

Some of the intelligence officials who made presentations to the Commission argued that the intrusive methods of physical surveillance, infiltration of an organisation and recruitment of sources do not amount to an infringement of the right to privacy and consequently do not need to comply with the requirements of section 36(1) of the Constitution.[11] The officials also argued that individuals lose their right to privacy when they venture outside their homes into public spaces.

These arguments are not correct. There is no material difference between intercepting a person's private communication by bugging her phone, secretly entering her house, recruiting a member of her staff as an informant or planting an agent in her home or organisation. Further, as discussed below, the Constitutional Court has held that people do not lose their right to privacy when leaving their homes. The right applies whenever a person has the ability

[11] For example, memorandum prepared for the Commission by the legal adviser in the Ministry for Intelligence Services, August 2007, pp. 1-2.

to decide what he or she wishes to disclose to the public and has a reasonable expectation that his or her decision will be respected.[12]

### 7.3 Constitutional Court Judgements on Infringements of the Right to Privacy

Our perspective on intrusive measures is informed by the Constitutional Court's judgements regarding infringements of the right to privacy. Legislation governing the use of intrusive measures by the intelligence services must take account of these judgements. We present below some of the key observations and findings of the Court.

In *Bernstein v Bester* the Constitutional Court observed that breaches of the common law right to privacy through wrongful intrusion or disclosure of information have been held to include entry into a private residence, the reading of private documents, listening in to private conversations, the shadowing of a person, the disclosure of private facts which have been acquired by a wrongful act of intrusion, and the disclosure of private facts contrary to the existence of a confidential relationship.[13] This comment by the Court reinforces our view that infiltration of an organisation, recruitment of an informant and surveillance by the intelligence services are indeed infringements of the right to privacy.

In the *Bernstein* case the Court made the following statement regarding the right to privacy:

> A very high level of protection is given to the individual's intimate personal sphere of life and the maintenance of its basic preconditions and there is a final untouchable sphere of human

[12] *Investigating Directorate: Serious Economic Offences and Others v Hyundai Motor Distributors (Pty) Ltd and Others: In Re Hyundai Motor Distributors (Pty) Ltd and Others v Smit NO and Others*, 2001 (1) SA 545 (CC).
[13] *Bernstein and Others v Bester and Others NNO*, 1996 (2) SA 751 (CC), para 69.

> freedom that is beyond interference from any public authority. So much so that, in regard to this most intimate core of privacy, no justifiable limitation thereof can take place. But this most intimate core is narrowly construed. This inviolable core is left behind once an individual enters into relationships with persons outside this closest intimate sphere; the individual's activities then acquire a social dimension and the right of privacy in this context becomes subject to limitation.[14]

In the *Hyundai* case the Constitutional Court made clear that this statement should not be understood to mean that beyond the 'intimate core of privacy' an individual loses his or her right to privacy. The Court commented as follows on the *Bernstein* passage quoted above:

> The right [to privacy], however, does not relate solely to the individual within his or her intimate space. Ackermann J did not state in the above passage that when we move beyond this established 'intimate core', we no longer retain a right to privacy in the social capacities in which we act. Thus, when people are in their offices, in their cars or on mobile telephones, they still retain a right to be left alone by the state unless certain conditions are satisfied. Wherever a person has the ability to decide what he or she wishes to disclose to the public and the expectation that such a decision will be respected is reasonable, the right to privacy will come into play.[15]

Where the Constitutional Court has been called on to judge the constitutionality of legislation that permits infringements of the right to privacy, it has emphasised the necessity for safeguards to protect that right. For example, in the *Mistry* case, which dealt with search and seizure powers in

[14] *Bernstein v Bester*, op cit, para 77.
[15] *Investigating Directorate v Hyundai*, op cit, para 16.

the Medicines and Related Substances Control Act No. 101 of 1965, the Court said the following:

> The existence of safeguards to regulate the way in which state officials may enter the private domains of ordinary citizens is one of the features that distinguish a constitutional democracy from a police state. South African experience has been notoriously mixed in this regard. On the one hand, there has been an admirable history of strong statutory controls over the powers of the police to search and seize. On the other, when it came to racially discriminatory laws and security legislation, vast and often unrestricted discretionary powers were conferred on officials and police. Generations of systematised egregious violations of personal privacy established norms of disrespect for citizens that seeped generally into the public administration and promoted amongst a great many officials habits and practices inconsistent with the standards of conduct now required by the Bill of Rights. Section 13 [i.e. the right to privacy in the interim Constitution of 1993], accordingly, requires us to repudiate the past practices that were repugnant to the new constitutional values, while at the same time re-affirming and building on those that are consistent with these values.[16]

In the *Hyundai* case the Court was concerned with search and seizure provisions in the National Prosecuting Authority Act No. 32 of 1998. The Court held that these provisions were not unconstitutional. Central to this decision was the Court's view that the legislation contained substantial safeguards protecting the right to privacy. The safeguards included the following:

[16] *Mistry v Interim Medical and Dental Council of South Africa* 1998 (4) SA 1127 (CC), para 25.

- No search of premises and seizure of property could be effected without prior judicial authorisation.

- The Act prescribes the information that must be considered by the judicial officer before a warrant for the search and seizure may be issued.

- This information must be given to the judicial officer on oath or affirmation.

- There must be reasonable grounds for believing that an object connected with a preparatory investigation is or is suspected to be on the targeted premises.

- The judicial officer must apply his or her mind to whether the suspicion that led to the need for the search and seizure is sufficient to justify the invasion of privacy and, on the basis of that information, must make an independent evaluation and determine whether or not there are reasonable grounds to suspect that an object that might have a bearing on a preparatory investigation is on the targeted premises.

- The Act requires the execution of a search warrant to be conducted with strict regard to decency and order, including respect for a person's rights to dignity, to personal freedom and security and to personal privacy.[17]

In the case of *Powell v Van der Merwe*, the Supreme Court of Appeal reviewed the decisions of our courts on the validity of search warrants and said that these cases established the following:

- Because of the great danger of misuse in the exercise of authority under search warrants, the courts examine their validity with a jealous regard for the liberty of the subject and his or her rights to privacy and property.

[17] *Investigating Directorate v Hyundai*, op cit.

- This applies to both the authority under which a warrant is issued, and the ambit of its terms.

- The terms of a search warrant must be construed with reasonable strictness. Ordinarily there is no reason why it should be read otherwise than in the terms in which it is expressed.

- A warrant must convey intelligibly to both searcher and searched the ambit of the search it authorises.

- If a warrant is too general, or if its terms go beyond those the authorising statute permits, the Courts will refuse to recognise it as valid, and it will be set aside.

- It is no cure for an over-broad warrant to say that the subject of the search knew or ought to have known what was being looked for: the warrant must itself specify its object, and must do so intelligibly and narrowly within the bounds of the empowering statute.[18]

There is no reason to believe that our courts would view the use of intrusive methods by the intelligence services with anything other than a "jealous regard for the liberty of the subject and his or her rights to privacy and property".[19] It is therefore necessary for the Minister for Intelligence Services to introduce legislation that regulates the use of these methods in a manner consistent with court decisions on the right to privacy.

### 7.4 The Grounds for Permitting the Use of Intrusive Methods

In this Section we review the grounds on which the use of intrusive methods by the intelligence services is permitted in terms of the Regulation of

[18] *Powell NO v Van der Merwe NO* 2005 (5) SA 62 (SCA), para 59.
[19] Ibid.

Interception of Communications and Provision of Communication-Related Information Act No. 70 of 2002 (hereafter "RICA"), the Intelligence Services Act No. 65 of 2002 and various intelligence policies. As summarised in Section 7.4.4, the grounds differ markedly among these documents. The lack of consistency creates a significant risk of unjustified infringements of constitutional rights.

### *7.4.1 RICA*

RICA contains a general prohibition on the interception of private communication but allows a member of an intelligence service, the police service, the defence force and other specified organisations to apply to a designated judge for an interception direction permitting a member of that organisation to intercept a person's communication without the knowledge of that person. The judge may issue an interception direction for a period of up to three months if he or she is satisfied that the requirements of the Act have been met. A 'designated judge' is a retired judge designated by the Minister for Intelligence Services for the purposes of the Act.

The Act stipulates the grounds on which the judge may issue an interception order and specifies which of these grounds can be invoked by each of the security services and law enforcement organisations.[20]

In the case of an intelligence service, the judge may issue an interception direction if he or she is satisfied, on the facts alleged in the application, that there are reasonable grounds to believe that "the gathering of information concerning an actual threat to the public health or safety, national security or compelling national economic interests of the Republic is necessary" or that "the gathering of information concerning a potential threat to the public health or safety or national security of the Republic is necessary".[21]

[20] Sections 16(3) and 16(5) of RICA.
[21] Sections 16(3)(b) and 16(5)(a)(ii) and (iii) of RICA.

The judge may also issue an interception direction to an intelligence officer if there are reasonable grounds to believe that "the making of a request for the provision, or the provision to the competent authorities of a country or territory outside the Republic, of any assistance in connection with, or in the form of, the interception of communications relating to organised crime or any offence relating to terrorism or the gathering of information relating to organised crime or terrorism, is in a) accordance with an international mutual assistance agreement; or b) the interests of the Republic's international relations or obligations".[22] The application by the intelligence officer must be for the purpose of gathering information rather than investigating an offence.[23]

The Act regards the interception of communication as a method of last resort. Before issuing an interception order, the judge must be satisfied that non-intrusive methods are inadequate or inappropriate. He or she must be satisfied that:

> …other investigative procedures have been applied and have failed to produce the required evidence or reasonably appear to be unlikely to succeed if applied or are likely to be too dangerous to apply in order to obtain the required evidence and that the offence therefore cannot adequately be investigated, or the information therefore cannot adequately be obtained, in another appropriate manner.[24]

An applicant who applies for an interception direction may also apply for an entry warrant.[25] The warrant authorises entry into premises for the purposes of intercepting a postal article or communication or installing, maintaining or removing an interception device.[26] In addition to satisfying the judge that the interception direction is justified, the applicant must satisfy the judge that a) entry of the premises is necessary for one of the above purposes; or b) there

[22] Sections 16(5)(a)(iv) of RICA.
[23] Section 16(3)(c)(ii) of RICA.
[24] Section 16(5)(c) of RICA.
[25] Section 22 of RICA.
[26] Section 1(1) of RICA.

are reasonable grounds to believe that it would be impracticable to intercept a communication under the interception direction other than by the use of an interception device installed on the premises.[27]

### *7.4.2 The Intelligence Services Act*

Section 11 of the Intelligence Services Act deals with entry, search and seizure by the intelligence services. It provides that a designated judge as defined in RICA may issue an intelligence service with a direction authorising a member when reasonably necessary to enter and search premises and examine, copy and remove any article, document or other material.[28]

The judge must be satisfied, on the grounds mentioned in a written application, that: a) there is on the premises in question information which has or could probably have a bearing on the functions of the intelligence services as contemplated in section 2 of the National Strategic Intelligence Act No. 39 of 1994, which information is of substantial importance and is necessary for the proper discharge of the functions of the intelligence services; and b) such information cannot reasonably be obtained by other means.[29]

### *7.4.3 The policies and perspectives of the intelligence organisations*

A number of internal intelligence policies indicate the grounds on which intrusive operations can take place:

- NIA's Operational Policy, which covers principles, responsibilities and authority for intrusive operations and other activities, permits resort to intrusive methods on broadly stated grounds. It declares that these methods may be used where intelligence is necessary to protect the Republic and/or its people against any real or potential security threat; to

[27] Section 22(4) of RICA.
[28] Sections 11(2)(i)-(iv) of the Intelligence Services Act No. 65 of 2002.
[29] Sections 11(2)(a) and (b) of the Intelligence Services Act.

prevent or detect crime or prevent disorder; and in the interest of public health or safety.[30]

In October 2007 NIA informed the Commission that it had revised its Operational Policy, which now includes the following restrictive principles regarding intrusive measures:

- The use of intrusive techniques must be proportionate to the threat posed and the probability of its occurrence. The least intrusive means feasible must be used to achieve an intelligence objective.

- Intrusive techniques must not be used in relation to lawful advocacy, protest or dissent unless reasonably believed to be carried out in conjunction with threats.

- The more intrusive the technique and the higher the risk in the conduct of an operation, the higher the authority that must be required to approve its use.[31]

- NIA's operational directive on communications monitoring and interception is intended to ensure compliance with RICA. However, it extends the grounds on which an interception operation may be conducted beyond the grounds specified in RICA. For example, the directive states that interception methods are justified where they are necessary to investigate serious crimes.[32] In terms of RICA, this ground can be invoked by a member of the police service but not by a member of the intelligence services.[33]

[30] National Intelligence Agency, 'Operational Policy of NIA', 25 February 2003, pg. 19.
[31] National Intelligence Agency, untitled and undated document summarising changes to NIA's operational directives, presented to the Commission on 12 October 2007.
[32] National Intelligence Agency, 'Operational Directive (OD.08): Authorisation and Management of Communications Monitoring and Interception', 11 February 2008, section 12.1.
[33] Sections 16(3) and 16(5) of RICA.

- NIA's operational directive on its mandate and operational philosophy contains a narrow formulation: "Intrusive means shall only be applied where there is demonstrable reason to believe that criminal or unconstitutional acts are about to be committed or have already been committed".[34]

- The SASS policy on surveillance does not indicate expressly the grounds on which surveillance can be undertaken.[35] Instead, it states that surveillance operations must be aligned with the legal mandate of SASS. This mandate includes a) to gather, correlate, evaluate and analyse foreign intelligence in order to identify any threat or potential threat to the security of the Republic or its people; and b) to institute counter-intelligence measures within SASS and, in consultation with NIA, outside the Republic.[36]

  The SASS document states that the policy on surveillance is informed by the Constitution but it does not mention any specific constitutional provision and does not explain how the Constitution effects surveillance operations. It consequently provides no constitutional guidance to the officials responsible for authorising and carrying out these operations.

- The SASS policy on interception of communication includes as one of its principal objectives the regulation of communication interception in accordance with RICA.[37] Attached to the policy is a template for applying for a judicial direction in terms of RICA.

- The Task Team on the Review of Intelligence-Related Legislation, Regulation and Policies prepared two reports for the Minister for

[34] National Intelligence Agency, 'Operational Directive OD.01: NIA's Mandate and Operational Philosophy', 27 February 2003, section 3.1.1.
[35] South African Secret Service, 'Surveillance Policy and Procedural Manual', 13 June 2006.
[36] Sections 2(2)(a) and (b) of the National Strategic Intelligence Act.
[37] South African Secret Service, 'Technical Intelligence Policy and Procedural Manual', 13 June 2006, section 1.3.

Intelligence Services, neither of which contains precise criteria for the use of intrusive methods.

The Final Report of the Task Team states that "intrusive measures should be used when information exists that creates a reasonable ground for suspicion that a serious enough threat exists and where other, non-intrusive, methods of intelligence collection are inadequate to uncover and understand the threat".[38] The Special Report of the Task Team states that these methods are justified in relation to the threat of "large-scale political instability"[39] and "reasonable suspicion of threats to national security and stability".[40]

- The White Paper on Intelligence of 1994 is silent on the question of intrusive measures and the right to privacy. On the related topic of covert operations, the White Paper makes the following important points:

> Measures designed to deliberately interfere with the normal political processes in other countries and with the internal workings of parties and organisations engaged in lawful activity within South Africa must be expressly forbidden. Intelligence agencies or those within them guilty of such breaches must be disciplined in the severest terms.[41]

### *7.4.4 Summary*

The discrepancies regarding justifiable grounds for the use of intrusive methods by the intelligence services are evident in the table on the following page.

[38] Task Team, 'Final Report', op cit, pg. 55.
[39] Task Team on the Review of Intelligence-Related Legislation, Regulation and Policies, 'Special Report of the Legislative Review Task Team on the Superintendence and Oversight of the Conceptualisation, Planning and Execution of Political Intelligence', May 2006, pg. 7.
[40] Ibid, pg. 11.
[41] White Paper on Intelligence, 1994, pg. 8. We discuss countermeasures in Section 6.6.

Grounds for the Use of Intrusive Methods by the Intelligence Services

| SOURCE | METHODS | REASONABLE GROUNDS TO BELIEVE THAT: |
|---|---|---|
| Regulation of Interception of Communications Act | Interception, entry, search and seizure | There is an actual threat to the public health or safety, national security or compelling national economic interests of RSA; there is a potential threat to the public health or safety or national security; or assistance to the authorities of another country regarding organised crime or terrorism is in the interests of RSA's foreign relations. |
| Intelligence Services Act | Entry, search and seizure | There is information which has or could have a bearing on the functions of the services, is of substantial importance and is necessary for the proper discharge of the functions of the services. |
| NIA Operational Policy | Intrusive methods | Intelligence necessary to protect RSA and/or its people against any real or potential security threat; to prevent or detect crime or prevent disorder; or in the interest of public health or safety. Intrusive methods may not be used in relation to lawful advocacy, protest or dissent unless reasonably believed to be carried out in conjunction with threats. |
| NIA Operational Directive OD.01 | Intrusive methods | Criminal or unconstitutional acts are about to be committed or have already been committed. |
| NIA Operational Directive OD.08 | Communications monitoring and interception | RICA grounds plus investigation of serious crimes. |
| SASS Surveillance Policy | Surveillance | Not specified. Must be aligned with SASS legal mandate. |
| SASS Technical Intelligence Policy | Interception of communication | RICA grounds. |
| Task Team Final Report | Intrusive methods | A serious enough threat exists. |
| Task Team Special Report | Intrusive methods | Threat of large-scale political instability. |

### 7.4.5 *Comment*

There is a glaring lack of consistency regarding the grounds on which intrusive measures are permitted. We note with concern the differences between the legislation and the operational directives as well as the differences between the two Acts. Both the Intelligence Services Act and RICA allow the intelligence services to enter and search premises with the approval of the designated judge but they provide different grounds on which the judge may grant permission.

The inconsistencies do not appear to derive from any sound criteria or deliberate policy. They indicate a haphazard approach that is inattentive to the need to safeguard the right to privacy and define with precision and circumspection the grounds on which the right can be infringed. There is a danger that the inconsistencies generate confusion and uncertainty and they might also increase the risk of unjustified violations of privacy.

The absence of coherent policy reflects a general problem in the civilian intelligence community. As discussed in Chapter 4, there is a dearth of executive policies on critical intelligence issues. Between the intelligence legislation and the operational directives issued by the heads of the intelligence services, there ought to be an intervening layer of ministerial regulations and policies. Fundamental policy positions on the use of intrusive measures, which ought to be taken by the Minister, have instead been determined by the heads of the services.

### 7.4.6 *The way forward*

The intelligence services should not be allowed to infringe the right to privacy on grounds that are imprecise or overly broad. We doubt the constitutionality of the current legislation where it enables the services to use intrusive measures on such grounds. Moreover, we are convinced that the services

should not be allowed to violate the privacy of persons who are involved solely in lawful activities.

Of the various laws, policies and directives cited above, we favour the narrow approach adopted in NIA's directive on its mandate and operational policy. As noted in Section 7.4.3, the directive states that "intrusive means shall only be applied where there is demonstrable reason to believe that criminal or unconstitutional acts are about to be committed or have already been committed".[42] We support this formulation save for the reference to 'unconstitutional acts'. This term is used in many intelligence policies to mean something different from criminal acts but it has not been defined and its meaning is therefore unclear.

We also favour the White Paper prohibition on interference in lawful politics and we support the revision to NIA's Operational Policy which states that "intrusive techniques must not be used in relation to lawful advocacy, protest or dissent unless reasonably believed to be carried out in conjunction with threats". However, the term 'threats' requires a more precise definition than is currently the case.

By way of comparison, the Australian intelligence legislation provides the following formulation:

> This Act shall not limit the right of persons to engage in lawful advocacy, protest or dissent and the exercise of that right shall not, by itself, be regarded as prejudicial to security, and the functions of the [Australian Security Intelligence] Organisation shall be construed accordingly.[43]

In the case of Germany, the Basic Law states that secrecy of mail, post and telecommunications is inviolable. Legislation permits the interception of these

[42] National Intelligence Agency, 'Operational Directive OD.01', op cit, section 3.1.1.
[43] Section 17A of the Australian Security Intelligence Organisation Act No. 113 of 1979.

methods of communication only where there is a factual basis for suspecting a person of planning, committing or having committed certain criminal acts that are punishable under the Criminal Code.[44]

Our conclusion is that South African legislation should limit the use of intrusive methods by the intelligence services 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 services to obtain the necessary intelligence; and c) the gathering of that intelligence is essential for the services to fulfil their functions as defined in law. We believe that this formulation would meet the test of proportionality set by section 36(1) of the Constitution.

In Chapter 6 we propose that NIA's mandate should be narrowed to focus on terrorism, organised crime, organised violence and other serious offences. If this recommendation were accepted, then the grounds on which the Agency is allowed to use intrusive measures would necessarily have to be narrowed in the manner proposed above. Even if NIA retains its broad mandate, however, its use of intrusive measures should be confined to the arena of serious crimes.[45]

## 7.5 Judicial Authorisation for Intrusive Methods

In the *Hyundai* case referred to Section 7.3, the Constitutional Court held that the National Prosecuting Authority Act of 1998 was constitutional despite its provisions on search and seizure which infringe the right to privacy. A primary reason for this decision was that the Act stipulates that a search and seizure may only be carried out if it is sanctioned by a warrant issued by a judicial

[44] Judgement of the European Court of Human Rights in *Klass and Others v Germany* (1978) 2 EHRR 214, paras 16 and 17.
[45] In Section 6.9.1 we explain how NIA's functions in relation to serious crime differ from those of the police.

officer.[46]

The Court observed that the National Prosecuting Authority Act had repealed the Investigation of Serious Economic Offences Act No. 117 of 1991, which had been the subject of litigation in the *Park-Ross* case.[47] In this case, the Court held that a provision authorising searches to be carried out without the sanction of a judicial officer was unconstitutional. The Court added that the spirit and purport of the Constitution would be met if the legislation required prior authorisation for a search or seizure to be obtained from a magistrate or judge and required an application for such authorisation to set out, at the very least, under oath or affirmed declaration, information as to the nature of the inquiry, the suspicion having given rise to that inquiry, and the need, in regard to that inquiry, for a search and seizure.[48]

As noted in Section 7.4, RICA and the Intelligence Services Act oblige the intelligence services to obtain prior judicial approval for intercepting communication and for entry, search and seizure. We are convinced that this approach should apply to all intrusive operations undertaken by the intelligence services. There is no sound basis for making some but not all intrusive methods subject to the necessity for judicial authorisation.

The Inspector-General of Intelligence shares this view. In his submission to the Commission, he insisted that "domestic intelligence gathering operations or techniques that intrude on civilian privacy must be subject to judicial approval and oversight".[49]

---

[46] *Investigating Directorate v Hyundai*, op cit, para 38.
[47] *Park-Ross and Another v Director: Office for Serious Economic Offences*, 1995 (2) SA 148 (C).
[48] Cited in *Investigating Directorate v Hyundai*, op cit, para 38.
[49] Office of the Inspector-General of Intelligence, 'Submission to the Ministerial Review Commission', op cit, pp. 11 and 19.

## 7.6 Ministerial Approval of Intrusive Methods

There is no obligation in legislation for the intelligence services to obtain the Minister's permission to use intrusive methods of investigation. Following the intelligence crisis of 2005/6, however, Minister Kasrils instructed the services to seek his approval for "sensitive projects and targets", these being projects and targets that relate to political intelligence or that have diplomatic implications.[50]

The Task Team proposed that ministerial approval should be required for high-risk operations, which are operations that would have serious consequences for the government or the intelligence organisations if they were compromised.[51]

In many other democratic countries, including Australia, Canada and the United Kingdom, ministerial approval is mandatory for the use of intrusive measures by the intelligence services.[52] In Australia, ministerial authority must be obtained for searches of persons and premises, the use of listening devices and tracking devices, and inspection of postal and delivery service articles.[53] The Canadian Security Intelligence Service Act of 1984 insists on both ministerial and judicial authorisation for a warrant to intercept communication and enter and search premises.[54]

We believe that ministerial approval in South Africa should not be limited to high-risk operations or 'sensitive projects and targets'. It should be required for all intrusive operations. This would properly reflect the seriousness of infringing constitutional rights and the importance of the principle of ministerial accountability.[55]

---

[50] Ministry for Intelligence Services, 'The Role of the Ministry for Intelligence Services. Presentation to the Review Commission on Intelligence', 26 January 2007, pg. 15.
[51] Task Team, 'Final Report', op cit, pg. 78.
[52] Information provided to the Commission by Dr Sandy Africa.
[53] Ibid.
[54] Sections 21(1) and (2) of the Canadian Security Intelligence Service Act of 1984.
[55] In Section 8.7 we discuss and reject the argument that ministerial approval would obviate the need for judicial authorisation for the use of intrusive methods.

## 7.7 Recommendations

### *7.7.1 Legislation*

The Minister for Intelligence Services should introduce legislation that regulates in a uniform manner the use of 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 elements:

- 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 fulfil their functions as defined in law.

- The intelligence services should be prohibited from using intrusive measures against persons and organisations that are involved solely in lawful activity. An alternative formulation would be that the intelligence services may not use intrusive measures in relation to lawful activities unless these activities are reasonably believed to be linked to the commission of a serious offence.

- The intelligence services should be prohibited from interfering with political processes in other countries, whether through the use of intrusive methods or by any other means.

- The use of intrusive measures by the intelligence services should require the approval of the Minister for Intelligence Services. The Minister must be satisfied that the criteria for using these measures have been met.

- The use of intrusive measures should require the prior 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.[56] The application must provide sufficient detail to enable the judge to make an independent assessment of whether the circumstances warrant the employment of intrusive measures.

- As in the case of RICA, the legislation should state that intrusive methods may only be used as a matter of last resort.[57]

- The legislation should require intrusive measures to be carried out with strict regard to decency and respect for a person's rights to dignity and personal freedom, security and privacy.

- The legislation should state that 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.

*7.7.2 Regulations, guidelines and operational directives*

The Minister should issue regulations and policies that guide the implementation of the new legislation on intrusive methods. The policies could be included in a new White Paper on Intelligence (Chapter 3).

As proposed by the Task Team, the Minister should initiate an engagement with the Inspector-General of Intelligence and the JSCI to ensure more

[56] As with section 23 of RICA, the legislation should allow for emergency applications to the judge to be made orally.
[57] See Section 7.4.1 of the Report and section 16(5)(c) of RICA.

effective routine and ad hoc monitoring of compliance with ministerial and departmental prescripts on the conduct of operations.[58]

Flowing from the introduction of new legislation, regulations and ministerial policies, the heads of the intelligence organisations should issue operational directives that provide for internal procedures, controls, authorisation, supervision and compliance.[59]

Prior to the introduction of 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 set a deadline by which this is to be done. The Minister should request the Inspector-General of Intelligence to certify the revised policies and procedures in terms of their alignment with the Constitution and the law.

[58] Task Team, 'Final Report', op cit, pg. 79.
[59] The Task Team's recommendations on operational directives governing intrusive operations are presented in Section 9.2.2.

## CHAPTER 8: INTERCEPTION OF COMMUNICATION AND THE NCC

### 8.1 Introduction

This Chapter focuses on interception of communication and the National Communications Centre (NCC). The NCC is government's facility for intercepting electronic signals that are transmitted via satellite. It monitors the signals of 'targets', being known persons or organisations that have been identified for intelligence monitoring. It also undertakes 'environmental scanning', which entails random monitoring of signals through the Centre's bulk monitoring capability.

Although the preceding Chapter on intrusive measures and the right to privacy applies fully to the interception of communication, we have devoted a separate chapter to this topic for two reasons. First, in our opinion the NCC appears to be engaged in signals monitoring that is unlawful and unconstitutional because it does not comply with the relevant legislation. Similarly, the NIA policy on interception of communication is inconsistent with the Constitution and legislation. The relevant legislation is the Regulation of Interception of Communications and Provision of Communication-Related Information Act No. 70 of 2002 (hereafter "RICA"), which prohibits the interception of private communication without judicial authorisation.

Second, in June 2008 Minister Kasrils tabled the Intelligence Services Amendment Bill,[1] which provides for the establishment of the NCC, and the National Strategic Intelligence Amendment Bill (hereafter "the NCC Bill"),[2] which provides for the functions of the NCC. These legislative amendments are intended to ensure the legality and constitutionality of the NCC's operations. The Minister invited our comment on an earlier version of the

[1] Intelligence Services Amendment Bill [B 37-2008].
[2] National Strategic Intelligence Amendment Bill [B 38-2008].

NCC Bill and we submitted a memorandum to him in February 2008.[3] We also made a submission on the Bill to the Ad Hoc Committee on Intelligence in the National Assembly.[4]

In order to assess the constitutionality of the NCC Bill, we solicited a legal opinion from an advocate in private practice and the NCC thereafter commissioned a further opinion from the advocate.[5] In the course of this Chapter we refer to these opinions, copies of which were given to the Minister.

The Chapter covers the following topics:

- Background information on the NCC (Section 8.2).
- The concerns of the Inspector-General of Intelligence regarding the NCC (Section 8.3).
- The constitutional and legislative framework and the implications for the NCC (Section 8.4).
- The NCC Interim Policy (Section 8.5).
- The NCC Bill (Section 8.6).
- The importance of judicial authorisation (Section 8.7).
- The NIA Directive on Communications Monitoring and Interception (Section 8.8).

[3] Ministerial Review Commission on Intelligence, 'Memorandum on the NCC and Draft NCC Legislation', submitted to the Minister for Intelligence Services, February 2008.
[4] Ministerial Review Commission on Intelligence, 'Submission on the National Strategic Intelligence Amendment Bill [B 38-2008]', submitted to the Ad Hoc Committee on Intelligence in the National Assembly, 10 July 2008, available at www.intelligence.gov.za/commission.
[5] L. Nkosi-Thomas, 'Legal Opinion', commissioned by the Ministerial Review Commission on Intelligence, 4 October 2007; and L. Nkosi-Thomas, 'Addendum to the Legal Opinion of 4 October 2007', commissioned by the NCC, 1 February 2008.

- The SASS policy on interception of communication (Section 8.9).

- Recommendations (Section 8.10).

## 8.2 Background on the NCC

### *8.2.1 The NCC's establishment, controls and activities*

In the NCC's submission to the Commission,[6] the following points were made about the Centre's establishment and the need for governing legislation:

- The NCC collects signals intelligence. The mandate to do this derives from section 2 of the National Strategic Intelligence Act No. 39 of 1994, which mandates NIA to perform a counter-intelligence function.

- The formation of the NCC flowed from a recommendation by the Pikoli Commission in 1996 that government should establish a single, national signals intelligence facility. The objective was to overcome the problem of signals intelligence overlap and duplication among the various intelligence agencies by centralising the state's signals intelligence capacity in a single entity.

- The NCC is currently part of NIA but is expected in due course to be established as a Schedule 1 government department. The NCC's clients are NIA, SASS, the SAPS and the Financial Intelligence Centre.

- Cabinet accepted the Pikoli Commission's recommendation to establish the NCC as a separate entity but declined to introduce legislation governing its activities. In 2002 Cabinet again declined to introduce

[6] National Communications Centre, 'Briefing to Ministerial Review Commission', 30 January 2007.

legislation regulating the NCC. Draft legislation had been prepared and was expected to be tabled in Parliament in 2007. As noted in Section 8.1, the legislation was presented to Parliament in June 2008.

In the NCC's submission to the Commission,[7] the following points were made about control measures:

- The intelligence crisis of 2005/6 highlighted the risk of abusing the NCC's capacity and the inadequacy of existing controls. Minister Kasrils consequently instructed the Task Team on the Review of Intelligence-Related Legislation, Regulation and Policies to prepare a regulatory framework for the authorisation and conduct of signals operations.

- Pending the introduction of legislation on the NCC, the Minister approved the NCC Interim Policy. He also issued a directive stating that the telephone numbers of South Africans may not be loaded as primary numbers.

- A Signals Intelligence Operations Audit Committee headed by the NCC's Deputy Executive Director Operations has been formed to monitor compliance with the Interim Policy and advise the Executive Management on strengthening internal controls.

- The NCC's operational activities are subject to the oversight of the Inspector-General of Intelligence.

- The NCC believes that there is a need for further improvement. In order to minimise the potential for abuse, it is considering the creation of a Clearance Panel for all operational projects.[8]

[7] National Communications Centre, 'Briefing to Ministerial Review Commission', op cit.
[8] The NCC subsequently informed the Commission that it had abandoned the idea of a Clearance Panel in favour of the Audit Committee. Letter from the NCC, September 2007.

### *8.2.2 Perspective of other government departments*

The Minister for Public Service and Administration informed the Commission that she is not convinced that the NCC should be set up as a separate government department. She stated that this could possibly happen but "the Ministry for Intelligence Services should provide more information and motivation in order to consider establishing the NCC as a new national department".[9] In August 2008 we were told that the Minister had approved the establishment of the NCC as a Schedule 1 department.[10] This matter is covered in the NCC Bill that was tabled in Parliament in 2008.

The National Treasury believes that the proliferation of entities reporting to NIA compromises control over the budget and activities of the department. The three entities that report to NIA – namely the NCC, the OIC and COMSEC – should be re-incorporated into NIA. This would put the department on a firm course to better co-ordinate, control and account for intelligence activities. The consolidation of these entities within NIA would also release funds for other critical operations in the department.[11]

## 8.3 The Inspector-General's Concerns about the NCC

In his submission to the Commission, the Inspector-General of Intelligence raised the following concerns about the NCC:

- There is no legislative mandate for the NCC and electronic collection of signals.

- The regulatory framework governing the NCC's special powers is incomplete.

[9] Minister for Public Service and Administration, 'Written Submission to the Ministerial Review Commission on Intelligence', 16 May 2007, pg. 3.
[10] Letter to the Commission from Minister Kasrils, 18 August 2008.
[11] National Treasury, 'Submission by the National Treasury to the Ministerial Review Commission on Intelligence', 11 December 2007.

- Bulk interceptions are not usually subject to judicial control.

- There is a lack of internal compliance mechanisms for operational activities.[12]

The Inspector-General recommended that there be clearly defined parameters. A statutory mandate and proper regulations regarding the NCC's activities would minimise the danger of possible abuse and illegality.

We share the Inspector-General's concerns. In Section 8.5 we comment further on the defects in the NCC Interim Policy. In order to lay the ground for this, the following Section summarises the constitutional and legislative provisions that have a bearing on signals operations.

## 8.4 Constitutional and Legislative Framework and Implications for the NCC

### *8.4.1 Constitutional and legislative provisions*

As discussed in the previous Chapter, section 14 of the Constitution enshrines the right to privacy. Since the interception of communication infringes this right, it is legal only if it takes place in terms of law of general application. Prior to the promulgation of the NCC Bill, the relevant law is RICA.

In accordance with the right to privacy, RICA prohibits the interception of communications:

[12] Office of the Inspector-General of Intelligence, 'Submission to the Ministerial Review Commission: The Concept of the Control of the Civilian Intelligence Services', presented to the Commission on 29 January 2007, pp. 18-23.

> Subject to this Act, no person may intentionally intercept or attempt to intercept, or authorise or procure any other person to intercept or attempt to intercept, at any place in the Republic, any communication in the course of its occurrence or transmission.[13]

As noted in Section 7.4.1, RICA provides that a member of an intelligence service, the police service, the defence force and other specified bodies may apply to a designated judge for an interception direction that permits a member of that body to intercept a person's communication without the knowledge of that person. The judge may issue an interception direction for a period of up to three months if he or she is satisfied that the requirements of the Act have been met.[14]

RICA specifies the grounds on which the judge may issue an interception order and stipulates which of these grounds can be invoked by the different security services and law enforcement bodies.[15] The grounds that can be invoked by the intelligence services are set out in Section 7.4.1 of the Report.

An application for an interception order must indicate, amongst other things, the name of the person, if known, whose communication is to be intercepted; the nature and location of the facilities, if known, from which the communication is to be intercepted; the grounds on which the application is made; and the basis for believing that evidence relating to the grounds on which the application is made will be obtained through the interception.[16]

The application must also indicate whether other investigative procedures have been applied and failed to produce the required evidence or must indicate the reason why other investigative procedures reasonably appear

[13] Section 2 of RICA.
[14] Section 16 of RICA.
[15] Sections 16(3) and (5) of RICA.
[16] Section 16(2) of RICA.

unlikely to succeed or are too dangerous to apply in order to obtain the required evidence.[17]

The Act regards interception of communication as a method of last resort. Before issuing an interception direction, the judge must be satisfied that non-intrusive methods are inadequate or inappropriate (Section 7.4.1).

An application for an interception direction must ordinarily be made in writing. However, the application may be made orally if the applicant is of the opinion that it is not reasonably practicable, having regard to the urgency of the case or the existence of exceptional circumstances, to do so in writing.[18] If the oral application is approved by the judge, the applicant must submit a written application to the judge within 48 hours after the issuing of the direction.[19]

RICA indicates the level of seniority that is required when submitting an application for an interception direction.[20] For example, an intelligence officer who makes an application must do so with the approval of a General Manager or higher official in the intelligence service.[21]

RICA provides that the Minister for Intelligence Services must establish interception centres and an Office for Interception Centres, which are responsible for executing the interception directions issued by the judge. The legislation states further that telecommunication service providers (e.g. MTN) and postal service providers must comply with an interception direction and make available the information required by it.

### *8.4.2 Comment on the NCC in relation to RICA*

RICA prohibits the interception of communication. As an exception to this rule, it allows communication to be intercepted by a security service or law

[17] Section 16(2)(e) of RICA.
[18] Section 23(1) of RICA.
[19] Section 23(4)(b) of RICA.
[20] Section 1(1) of RICA under the definition of “applicant”.
[21] Section 1(1)(c) of RICA under the definition of “applicant”.

enforcement body. Such interception is subject to many safeguards, the most important of which is the necessity to obtain judicial authorisation. The safeguards reflect the intention of the Executive and Parliament to protect the right to privacy, prevent unjustified infringements of this right and ensure independent oversight of lawful interceptions.

During the preparation of the draft NCC Bill, an official in the Ministry for Intelligence Services argued that the NCC lies beyond the ambit of RICA because the signals operations undertaken by the NCC do not fall within RICA's definition of interception of communication.[22] This position is incorrect. RICA defines "intercept" as follows:

> The aural or other acquisition of the contents of any communication through the use of any means, including an interception device, so as to make some or all of the contents of a communication available to a person other than the sender or recipient or intended recipient of that communication, and includes the a) monitoring of any such communication by means of a monitoring device; b) viewing, examination or inspection of the contents of any indirect communication; and c) diversion of any indirect communication from its intended destination to any other destination.[23]

The Act defines "indirect communication" to mean the transfer of information, whether in the form of speech, music, data, text, signals or any other form, that is transmitted in whole or in part by means of a postal service or telecommunication system.[24]

We are in no doubt that the NCC's signals operations are covered by these definitions of "intercept" and "indirect communication".

---

[22] Ministry for Intelligence Services, 'Signals Intelligence in South Africa: Proposed Legal Framework', presentation to the State Law Advisers, 24 July 2007, slide 22.
[23] Section 1(1) of RICA.
[24] Section 1(1) of RICA.

The Ministry official argued further that the NCC's operations lie beyond the ambit of RICA because RICA is concerned with law enforcement whereas the NCC is concerned with intelligence.[25] This position is also incorrect. RICA covers both law enforcement and intelligence.[26] Similarly, the NCC, whose clients include NIA, SASS, the SAPS and the Financial Intelligence Centre, covers both law enforcement and intelligence.[27]

Until such time as the NCC Bill is promulgated, the NCC's signals operations fall squarely within RICA's definition of interception of communication and must therefore comply with the provisions of RICA. The NCC would be acting unconstitutionally and unlawfully if it intercepted communication without judicial authorisation. As discussed in the following Section, this currently appears to be the case.

It is also relevant in this regard, as noted in Section 8.5.2, that the Minister for Intelligence Services has expressly forbidden the loading of South African numbers without judicial authorisation.

## 8.5 The NCC Interim Policy

### *8.5.1 Overview*

The intelligence crisis of 2005/6 highlighted the inadequacy of the NCC's internal controls. Pending the introduction of legislation on the NCC, Minister Kasrils approved a regulatory policy entitled "NCC Interim Operational Procedures and Control Measures for the Authorisation and Conduct of Signals Intelligence Operations".

The policy provides that memoranda of understanding will be entered into with government bodies that use the NCC so as to guarantee that their

[25] Ministry of Intelligence Services, 'Signals Intelligence in South Africa', op cit, slide 22.
[26] Sections 16(3) and (5) of RICA.
[27] National Communications Centre, 'Briefing to Ministerial Review Commission', op cit.

targets are of legitimate intelligence interest; the NCC will focus on the national intelligence priorities set by Cabinet; it will establish an in-house Audit Committee to identify and assess possible misuse of NCC systems; any misuse or misconduct will be reported to the NCC Executive Director and the Minister; and the Office of the Inspector-General will conduct bi-annual audits of signals intelligence operations and submit reports to the Minister and the NCC Executive Director.

The policy distinguishes between applications for the acquisition of political intelligence involving a South African person or organisation and applications for other intelligence projects.[28] The former must be authorised and motivated by the Director-General of the body making the application; they must be addressed to the Executive Director of the NCC; and they must be authorised by the Minister. All applications must contain information about the targeted person or organisation and about the nature of the target's activities that constitute a security threat or potential threat.[29]

The policy states that non-targeted information generated by environmental scanning is retained for two or three days for evaluation and data-mining. Information regarding a South African person or organisation that is incidentally acquired may be retained if it indicates possible involvement in a criminal offence or a threat to the security of South Africa.[30]

### *8.5.2 Comment*

The NCC Interim Policy correctly emphasises the need for proper control, oversight and procedures so that the Centre's capacities are not abused. However, we are extremely concerned that the policy makes no reference to RICA and the legal obligation to obtain judicial authorisation before the NCC

[28] National Communications Centre, 'Interim Operational Procedures and Control Measures for the Authorisation and Conduct of Signals Intelligence Operations', June 2006, sections 6 and 7.
[29] Ibid, section 8.
[30] Ibid, sections 14 and 15.

intercepts the communication of a targeted person or organisation. This concern is shared by the Inspector-General of Intelligence.[31]

We asked an NCC official to explain the omissions from the policy. It appeared from his response that he believed that RICA did not apply to the NCC.[32] He did not provide a sound reason for this belief, which is erroneous. As discussed in Section 8.4.2, the RICA prohibition on intercepting communication without judicial authorisation applies as much to the NCC as to any other body. Our interpretation of RICA in this regard is also held by NIA officials,[33] the Inspector-General of Intelligence,[34] and the SAPS.[35] The SASS policy on interception of communication emphasises compliance with RICA (Section 8.9).

In January 2007 Minister Kasrils informed the NCC that "no South African mobile or fixed line numbers are to be loaded onto the NCC systems as primary targets for NCC operations without first obtaining a Judge's permission".[36] This instruction should have led to a revision of the interim policy, which it did not.

## 8.6 The NCC Bill

### *8.6.1 Overview*

The NCC Bill covers the NCC's functions and purposes. The functions include the collection and analysis of foreign signals intelligence in accordance with the intelligence priorities of the Republic.[37] 'Foreign signals intelligence'

[31] Meeting with the Inspector-General of Intelligence, 10 May 2008.
[32] Correspondence to the Commission from NCC official, 28 February 2008 and 5 March 2008.
[33] Correspondence to the Commission from NIA officials, 21 February 2008.
[34] Meeting with the Inspector-General of Intelligence, 10 May 2008.
[35] Letter to the Commission from the SAPS Divisional Commissioner Crime Intelligence, 7 April 2008.
[36] Letter from Minister Kasrils to the Acting Executive Director of the NCC, 23 January 2007.
[37] Section 2 of the National Strategic Intelligence Amendment Bill [B 38-2008].

means “intelligence derived from the interception of electromagnetic, acoustic and other signals, including the equipment that produces such signals, and includes any communication that emanates from outside the borders of the Republic, or passes through or ends in the Republic”.[38]

The NCC may only perform its functions for the following objectives:

- to identify any threat or potential threat to the security of the Republic or its people;

- to protect and advance international relations and the economic well-being of the Republic;

- to support the prevention or detection of serious crime directed and committed against the Republic and its citizens; and

- to support the prevention or detection of regional and global hazards or disasters that threaten life, property and the environment.[39]

The NCC must perform its functions with due regard for the rights set out in Chapter 2 of the Constitution and subject to ministerial approval. The Minister for Intelligence Services must regulate and authorise in writing the activities of the NCC and, in particular, must authorise each target or communication which is to be monitored or intercepted if the Minister is satisfied that such activities are necessary to achieve the objectives described above.[40]

The Inspector-General of Intelligence must report annually to Parliament on the activities of the NCC and in such report must indicate any contraventions by the NCC of the provisions of RICA.[41]

[38] Section 1 of the National Strategic Intelligence Amendment Bill [B 38-2008].
[39] Section 2 of the National Strategic Intelligence Amendment Bill [B 38-2008].
[40] Section 2 of the National Strategic Intelligence Amendment Bill [B 38-2008].
[41] Section 2 of the National Strategic Intelligence Amendment Bill [B 38-2008].

*8.6.2 The subjects of the constitutional right to privacy*

As noted above, the Bill provides that the NCC may intercept foreign signals that emanate from outside the borders of the country and pass through or end in South Africa.

The communication intercepted by the NCC might consequently have been sent by a South African who is outside the country and/or it might be received by a South African who is inside the country. The Constitution affords citizens the right to privacy and they enjoy this right in relation to the state even when they are beyond the borders of South Africa. Moreover, the right to privacy is not limited to citizens but applies to every person in South Africa. The Constitutional Court has interpreted other constitutional rights in this fashion where the right, according to the Constitution, is held by "everyone".[42]

The Constitution also declares that the Republic is bound by international agreements that were binding on South Africa when the Constitution took effect,[43] and that customary international law is law in the Republic unless it is inconsistent with the Constitution or an Act of Parliament.[44] In this regard, Article 12 of the Universal Declaration of Human Rights states that "no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks".[45] This right is repeated in Article 17 of the International Covenant on Civil and Political Rights,[46] to which South Africa is a signatory.

The international right to privacy is thus protected by our Constitution and protects all people everywhere. The Inspector-General of Intelligence shares this view, maintaining that the NCC should take account of the fact that the

---

[42] See *Lawyers for Human Rights v Minister of Home Affairs* 2004 (4) SA 125 (CC); and *Mohamed v President of the Republic of South Africa* 2001 (3) SA 893 (CC).
[43] Section 231(5) of the Constitution.
[44] Section 232 of the Constitution.
[45] The Declaration can be viewed at www.un.org/Overview/rights.html.
[46] The Covenant can be viewed at www1.umn.edu/humanrts/instree/b3ccpr.htm.

right to privacy exists at the level of international law and thus applies to people outside the country.[47]

### *8.6.3 Commission's submission to the Minister*

Minister Kasrils invited our comment on an earlier version of the Bill.[48] In our response we argued that the Bill did not contain adequate safeguards to protect the right to privacy. It was therefore unlikely to satisfy the Constitutional Court, which has stressed the need for such safeguards in legislation that permits infringements of the right to privacy (Section 7.3).[49] In particular, the draft Bill did not provide for judicial authorisation for the interception of communication.

Our overarching recommendation was that the Bill should be consistent with RICA. This is because the Bill and RICA cover the same activities and have the same objective: to permit and regulate the interception of private communication for the purposes of intelligence, security and law enforcement. In addition, RICA reflects Parliament's views on appropriate safeguards to protect the right to privacy and prevent unjustified infringements of this right.

Some of our proposals were taken into account in the Bill that was tabled in Parliament in June 2008. We present our remaining concerns in the next Section.

### *8.6.4 Comment on the NCC Bill*

We have the following concerns about the NCC Bill:

---

[47] Meeting with the Inspector-General of Intelligence, 10 May 2008.
[48] Ministerial Review Commission on Intelligence, 'Memorandum on the NCC and Draft NCC Legislation', op cit.
[49] See *Mistry v Medical and Dental Council of South Africa* 1998 (4) SA 1127 (CC); and *Investigating Directorate: Serious Economic Offences v Hyundai Motor Distributors (Pty) Ltd: In re Hyundai Motor Distributors (Pty) Ltd v Smit NO (Hyundai)* 2001 (1) SA 545 (CC).

- The Bill does not indicate which organs of state are entitled to make use of the NCC. Given the sensitivity of both intelligence gathering and infringing the right to privacy, the Bill should specify the bodies that may apply to the NCC for assistance with the interception of communications. RICA provides a good example in this regard.[50]

- The Bill does not indicate whether the NCC can, on its own initiative, identify targets for signals monitoring or whether it can only monitor the targets identified by another intelligence service or a law enforcement body.

- Unlike RICA, the Bill does not specify the information that must be provided by an intelligence service or law enforcement body when applying to intercept communication. This legislative safeguard in RICA helps to prevent inappropriate and unjustified infringements of privacy.

- The NCC's relationship to RICA is unclear. The Bill states that the Inspector-General of Intelligence must report annually to Parliament on the NCC's activities and in such report must indicate any contraventions by the NCC of the provisions of RICA.[51] However, the Bill does not state the manner in which the NCC is bound by RICA. If the Inspector-General is to monitor the NCC's compliance with its obligations under RICA, then these obligations ought to be spelt out clearly in the Bill.

- The Bill permits the interception of communication in order to protect and advance international relations and the economic well-being of the Republic, and in order to support the prevention and detection of regional and global hazards and disasters that threaten life, property and the environment.

[50] See the definition of 'applicant' in Section 1 of RICA.
[51] Section 2 of the National Strategic Intelligence Amendment Bill [B 38-2008].

From a constitutional perspective, the broadness of these grounds creates doubt that they can reasonably be invoked to infringe the right to privacy. They would allow for eavesdropping by the state not only in relation to major security threats and criminal offences but also in relation to private activities and conversations that are lawful. They would permit, for example, the secret interception of the communication of bankers, economists and traders if such interception were deemed to advance the economic well-being of the country.

As recommended in Chapter 7, the interception of communication and other intrusive measures should be restricted to situations where there are reasonable grounds to believe that a serious criminal offence has been, is being or is likely to be committed.

- As in the case of RICA, the Bill should state that the interception of communication is a matter of last resort that can only be undertaken when non-intrusive methods are inadequate or inappropriate.

- The Bill should provide for the discarding of incidental information that is collected in the course of an interception. Incidental information includes all information of a personal nature that has no bearing on the security of the country or the purpose of the investigation.

## 8.7 The Importance of Judicial Authorisation

The NCC Bill does not provide for judicial authorisation for the signals interceptions that are undertaken by the NCC. The drafters of the Bill told us that they considered ministerial approval to be an adequate alternative to judicial approval. Cabinet reportedly shared this view.[52] The advocate whose opinion we sought also held this position. It therefore seems advisable to explore the matter further here.

[52] Deon de Lange, 'MPs Wary of Cabinet Snooping Proposal', *Cape Times* 31 July 2008.

In assessing the constitutionality of the draft NCC Bill, the advocate highlighted the value that the Constitutional Court attaches to judicial authorisation for infringements of the right to privacy.[53] Nevertheless, she argued that the requirement of ministerial approval in the draft Bill is akin to the discretion conferred on a judicial officer in other legislation dealing with infringements of this right.[54] If given sufficient information, the Minister for Intelligence Services can make an independent evaluation.[55] Ministerial approval is preferable to judicial approval because signals operations deal with classified matters and it is imperative to maintain confidentiality.[56]

The advocate noted that foreign law can be considered when interpreting rights in our Constitution. She reviewed the law on signals operations in Canada, Australia, New Zealand and the United Kingdom, all of which require ministerial authorisation, and the Foreign Intelligence Surveillance Act of the United States, which requires judicial authorisation. The advocate concluded that ministerial approval is the preferred model in most of these jurisdictions, that the reason for this is national security, and that the model of ministerial approval adopted in the draft NCC Bill is consequently appropriate.[57]

For several reasons we are convinced that these arguments are wrong. First, the legal opinion covers too few countries. It does not acknowledge the obligation to obtain judicial authorisation for wiretapping and electronic eavesdropping in, amongst other countries, Argentina, Austria, Belgium, Estonia, Iceland, Italy, Mexico, Norway and Spain.[58] Nor does the opinion acknowledge that lawful interceptions under the Canadian intelligence legislation require both ministerial and judicial approval.[59]

---

[53] Nkosi-Thomas, 'Legal Opinion', paras 38, 82 and 107.
[54] Ibid, para 102.
[55] Ibid, para 106.
[56] Nkosi-Thomas, 'Addendum to the Legal Opinion', para 28.
[57] Ibid, paras 58-59.
[58] Information obtained from Privacy International at www.privacyinternational.org.
[59] Sections 21(1) and (2) of the Canadian Security Intelligence Service Act of 1984.

Second, in interpreting constitutional rights, foreign laws might be relevant but they are much less significant than judgements of the Constitutional Court. As noted in Section 7.3, the Court has emphasised the importance of judicial authorisation in relation to infringements of the right to privacy.[60] The legal opinion ignores the crucial differences between a minister and a judge in this regard. Whereas ministers are politicians, judges are formally independent, politically impartial and, unlike the Minister for Intelligence Services, have no functional interest in gathering intelligence. Judicial approval thus provides greater assurance than ministerial approval that constitutional rights will not be violated for partisan or functional reasons.

Third, the legal opinion does not take adequate account of the RICA requirement that intelligence officials and police officers must obtain a judge's permission to intercept communication via a monitoring device, an interception centre, a telecommunications service provider or a postal service provider. The legislative architecture would be patently flawed if this requirement were absent when intelligence officials and police officers wanted to intercept communication via signals monitoring undertaken by the NCC.

Finally, there is no basis for assuming that judges are unable to maintain the confidentiality of classified information. The role of the designated judge in the RICA legislation indicates that the Executive and Parliament do not share this assumption.

## 8.8 NIA Directive on Communications Monitoring and Interception

### *8.8.1 Key provisions of the Directive*

The NIA Directive on Communications Monitoring and Interception regulates the monitoring and interception of communication, including signals

[60] *Park-Ross and Another v Director: Office for Serious Economic Offences*, 1995 (2) SA 148 (C); and *Investigating Directorate v Hyundai*, op cit.

intelligence operations and the management of information obtained from such operations.[61] The Directive contains procedures that are intended to ensure compliance with RICA and sets out the information that NIA officials must present to the designated judge when applying for an interception direction.[62]

The Directive observes that the interception of communication intrudes on the constitutional rights to privacy and association. It insists that all interceptions and monitoring operations must therefore be carried out in strict conformity with the Constitution and applicable laws and policies.

In this regard the Directive gives "special emphasis… to the protection of the constitutional rights and privacy of South African citizens".[63] It adds that "the constitutional principle of 'reasonableness' shall, for the purposes of this directive, be implemented by giving different categories of individuals and entities different levels of protection".[64] The Directive proceeds to distinguish between intercepting the communication of South Africans and intercepting the communication of foreigners. According to the Directive, the former but not the latter is covered by RICA and requires judicial authorisation.[65]

The Directive places a great deal of emphasis on compliance. It covers managerial monitoring, control and accountability; responsibilities for ensuring compliance; internal and external audits and oversight, including oversight by the Inspector-General of Intelligence; and administration and record keeping. It states that members have a duty to report irregularities and any instructions that are in contravention of legislation, regulations and policies, and it addresses the issue of sanctions in the event of non-compliance.

[61] National Intelligence Agency, 'NIA Operational Directive (OD.08): Authorisation and Management of Communications Monitoring and Interception', February 2008, section 1.
[62] National Intelligence Agency, 'NIA Operational Directive', op cit, section 1.
[63] Ibid, section 5.
[64] Ibid, section 5.2.
[65] Ibid, sections 5.2 and 5.4.

The Directive describes the criteria and grounds for justifying the interception of communication. These grounds include but are not limited to those contained in RICA.[66]

Section 11 of the Directive creates the impression that judicial authorisation is not required for applications to the NCC for the conduct of signals operations. When we sought clarity from NIA officials, we were informed that this was not intended and that the Directive would be amended to avoid this impression.[67]

*8.8.2 Comment*

The Directive's emphasis on compliance with the Constitution and legislation is commendable. However, the Directive contains a significant mistake in its interpretation of the Constitution and the law. Contrary to the Directive, the right to privacy is not limited to citizens but applies to everyone in South Africa (Section 8.6.2).

NIA is not entitled to give different categories of individuals and entities higher and lower levels of protection in relation to a constitutional right. This differentiation amounts to a limitation of the right and is invalid unless established by law. In prohibiting the interception of communication without judicial authorisation, RICA does not distinguish between the communication of South Africans and the communication of foreign nationals.

In short, NIA and other intelligence organisations are acting unconstitutionally and unlawfully if they intercept any local or foreign communication without judicial authorisation.

[66] National Intelligence Agency, 'NIA Operational Directive', op cit, section 12. We discuss this problem in Section 7.4 of the Report.
[67] Correspondence from NIA to the Commission, 21 February 2008.

## 8.9 SASS Policy on Interception of Communication

The SASS policy on interception of communication is aligned to RICA.[68] It has a number of positive features in this regard: one of its express objectives is to regulate interception of communication in accordance with RICA; one of its appendices is a template for applying for a judicial direction in terms of RICA; and another appendix summarises and reproduces relevant sections of RICA.

Aside from these positive features, we have two reservations about the policy. First, the policy's summary of RICA is unsatisfactory. It excludes a number of the key sections of the legislation, such as the grounds on which the intelligence services may apply to the designated judge for an interception direction. It also summarises some of the sections of RICA so badly as to render them incomprehensible. Needless to say, the policy's summary of RICA has no value if it is inaccurate.

Second, the document states that the Director-General of SASS may approve any deviation from the provisions of the policy if such deviation is in the best interest of the Service.[69] This is unsound. It could be interpreted to mean that the Director-General may approve deviations from RICA, which would be unlawful. Even if this were not the intention, permitting unspecified deviations at the discretion of the Director-General severely undermines the policy and the good governance imperative of adherence to rules. If there is a need for emergency procedures, then they should be specified in the policy.

[68] South African Secret Service, 'Technical Intelligence Policy and Procedural Manual', 13 June 2006.
[69] South African Secret Service, 'Technical Intelligence Policy', op cit, section 5.

## 8.10 Recommendations

### *8.10.1 The NCC Bill*

The National Strategic Intelligence Amendment Bill, which provides for the functions of the NCC, should state that the NCC is bound by RICA. It should also stipulate that the NCC may not intercept the communication of a targeted person unless it has obtained an interception direction issued by the designated judge as provided for in RICA.

The Bill should indicate which intelligence, security and law enforcement bodies are entitled to apply to the NCC for assistance with the interception of communication; it should specify the grounds that can be invoked by each of these bodies; and it should describe the information that must be contained in an application for signals monitoring.

The Bill should not allow for the interception of communication on the grounds of protecting and advancing international relations and the economic well-being of the Republic or on the grounds of supporting the prevention and detection of regional and global hazards and disasters. As proposed in Chapter 7, intrusive measures such as interception of communication should be limited to situations 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 indicate whether the NCC can, on its own initiative, identify targets for signals monitoring or whether it can only monitor the targets identified by another intelligence service or a law enforcement body.

The Bill should provide that interception of communication is a method of last resort that can only take place if non-intrusive methods are inadequate or inappropriate.

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 also cover the NCC's 'environmental scanning', which entails random monitoring of signals. It is not possible to obtain prior judicial authorisation for this kind of monitoring since there are no known targets. Where random monitoring identifies the need to focus on a specific person or organisation, however, then the requirements of ministerial approval and judicial authorisation should apply.

*8.10.2 Intelligence policies and procedures*

The intelligence organisations should take immediate steps to ensure that their policies and procedures on the interception of communication provide for ministerial approval and judicial authorisation and are in alignment with the Constitution and legislation. The Minister should set a deadline by which this is to be done and should request the Inspector-General of Intelligence to certify the revised policies and procedures in terms of their alignment with the Constitution and the law.

## CHAPTER 9: INTERNAL CONTROLS AND POLICIES

### 9.1 Introduction

The intelligence services have numerous internal controls that are intended to prevent misconduct and ensure adherence to the Constitution, legislation and operational policies. The controls include detailed guidelines, criteria and procedures for different kinds of action; specified levels of responsibility and decision-making authority; mechanisms for monitoring compliance with internal policies; periodic reviews of control systems and corrective action where deemed necessary; a duty on members to report illegality and breaches of policy; and disciplinary systems and sanctions for non-compliance and misconduct.

These controls are indicative of the professionalism of the intelligence services, which appreciate that misconduct by their members undermines their credibility and effectiveness and is consequently detrimental to the security of the country.

Over the past decade the intelligence organisations have been engaged in a virtually continuous process of strengthening their control systems. This has intensified since the intelligence crisis of 2005/6. The organisations accept that the crisis exposed many gaps and weaknesses in their systems. To their credit, some of them admitted frankly to the Commission that their controls were not yet adequate.[1] Efforts to address the problems, particularly in relation to tightening monitoring and compliance mechanisms, were underway in NIA throughout the period of our review.[2]

---

[1] National Intelligence Agency, 'Base Document for Presentation on Matters Relating to the Terms of Reference of the Ministerial Review Commission', submission to the Commission, 24 January 2007, pg. 33; and National Communications Centre, 'Briefing to Ministerial Review Commission', 30 January 2007, para 7.1.

[2] National Intelligence Agency, 'Ministerial Review Commission: Request Relating to the Compliance Programme of NIA', 13 March 2007.

The Office of the Inspector-General of Intelligence plays a valuable role in improving the control systems of the intelligence organisations. It does this through a variety of activities that include compliance monitoring, investigations, inspections, certification and rendering advice (Chapter 5).

Throughout the Report we examine aspects of the operational policies and controls of the intelligence services. In this Chapter we discuss the findings and recommendations on operational policies that were made by the Legislative Review Task Team in 2006. We also discuss the concern raised by some officials that the intelligence community is over-regulated. The financial controls of the intelligence services are examined in Chapter 10.

The Chapter covers the following topics:

- The Task Team's findings and recommendations on operational policies (Section 9.2).

- The Commission's comments on the findings and recommendations of the Task Team (Section 9.3).

- The question of whether the intelligence services are subject to too much regulation and oversight (Section 9.4).

- Recommendations (Section 9.5).

## 9.2 The Findings and Recommendations of the Task Team

In 2005 Minister Kasrils established the Task Team on the Review of Intelligence-Related Legislation, Regulation and Policies (hereafter the "Task Team").[3] Following the onset of the intelligence crisis of 2005/6, he instructed the Task Team to pay special attention to the operational policies of NIA and

[3] The Task Team is described in Section 1.6.

SASS and the proposed operational policies of the NCC. In this Section we summarise the Task Team's findings and recommendations on these policies.

### *9.2.1 Findings of the Task Team*

The Task Team began its discussion on operational policies by noting that the state gives the intelligence services two very powerful and dangerous rights, namely the right to invade the privacy of citizens and the right to function secretly.[4] It then identified five critical factors for assessing the policies of NIA, SASS and the NCC and, in particular, for gauging the efficacy of these policies in ensuring compliance with the Constitution and legislation:[5]

- The most important factor is the process by which the intelligence services receive or determine their intelligence priorities and then identify the targets for intelligence collection in the light of these priorities. This process relates to the setting of the National Intelligence Priorities by Cabinet annually on the basis of the National Intelligence Estimate conducted by NICOC.[6] The essential point is that the intelligence services should not be self-tasking. They should use their powerful rights to secrecy and intrusion in relation to threats that the government has decided constitute threats to national security.

- The second critical factor is the recognition that the primary function of the intelligence services is to forewarn government of developments and events that might impact on national security or interests and to do so in a sufficiently timely manner for government to take preventive action. Where forewarning is not possible, intelligence must at the very least provide government with insights that help it to acquire a deep understanding of the issues at stake and design and implement measures to deal with these issues.

[4] Task Team on the Review of Intelligence-Related Legislation, Regulation and Policies, 'Final Report of the Task Team on the Review of Intelligence-Related Legislation, Regulation and Policies', April 2006, pg. 47.
[5] Task Team, 'Final Report', op cit, pp. 52-57.
[6] We comment on the National Intelligence Priorities in Section 12.3.1.

- The third critical factor is the control system that governs the use of intrusive methods of intelligence collection. Three sets of controls are relevant:

  - First, there is the decision-making and authorisation process that determines whether intrusive methods can be used. This process should involve a clear assessment of the nature of the threat; the identification of targets and the type of intrusive methods that are needed to accomplish the operational goals; and an evaluation of the risk that the operation might be compromised. The consequences of compromise include embarrassment to the government, a threat to diplomatic relations, threats to government programmes and projects, and the compromise of intelligence capacities, methods and interests.

  - Second, there is the level of authorisation for carrying out an intrusive operation. The higher the risk of compromise of an operation, the higher the level of authorisation should be.

  - Third, there is the management and supervision of intrusive operations. Here, too, the higher the risk of compromise, the higher the required level of management and supervision.

- The fourth critical factor relates to the issue of incidental information, which is information that is obtained in the course of an intrusive operation but is unrelated to the threat against which the operation is directed. Such information should not be retained unless it relates clearly to another threat.

- Fifth, there must be sound processes of monitoring and enforcing compliance with operational policies. The key issues here are the necessity to keep accurate and detailed records of all decisions, authorisations, developments and products relating to intrusive operations;

the different levels of monitoring, including internal mechanisms, the Inspector-General of Intelligence (hereafter the "Inspector-General"), the JSCI and the Minister; and enforcement, which entails dealing effectively with failures to comply with operational policies.

The Task Team assessed the operational policies of NIA, SASS and the NCC against the factors outlined above. Its general finding was that the policies broadly complied with these factors but the following gaps and concerns were identified:[7]

- The process by which the National Intelligence Priorities approved by Cabinet are drawn down in the operational planning, priority-setting and targeting mechanisms of the intelligence services is not clear and precise enough in all cases.

- The levels of authorisation for intrusive operations are not consistently based on the level of risk and do not prescribe the involvement of the Minister or higher authority in authorising or concurring with high-risk operations. In the case of foreign operations conducted by SASS, there is no formal procedure for determining the level of authorisation and obtaining the concurrence of the Minister.

- There is insufficient attention to prescribing the level of management and supervision of operations, particularly where the operations are high-risk.

- There are no clear prescripts for dealing with incidental information that is gathered in the course of an intrusive operation.

- The mechanisms that monitor the compliance of intelligence operations with the regulatory framework are broadly adequate on paper but need to be tightened with additional mechanisms and procedures.

[7] Task Team, 'Final Report', op cit, pp. 57-58.

The Task Team added that the integrity of the system of authorising operations depends on the integrity and professionalism of the officials who make the decisions. Significant institutional transformation since 1994 had raised the level of professionalism but had not completely overcome the "culture of non-accountability of intelligence and security services, and a no-holds-barred approach to intelligence operations".[8]

The Task Team concluded that it was necessary to introduce a programme of culture change that instilled an understanding of constitutionality, legality, accountability and integrity in the civilian intelligence services. However, this programme must recognise that "it is sometimes necessary to 'bend the rules' in order to ensure that the threat is adequately dealt with".[9]

*9.2.2 Recommendations of the Task Team*

The Task Team recommended that the Minister issue regulations that achieve the following:[10]

- Regulate the system of determining the National Intelligence Priorities, oblige the intelligence services to prepare annually an operational plan based on these priorities and monitor the delivery of the services according to the priorities.

- Require the intelligence services to consult the Minister where there is a need to conduct intrusive operations that carry a high risk, if compromised, of embarrassing the government politically, jeopardising diplomatic relations or posing a threat to government programmes and projects on the domestic or international terrains.

- Mandate the heads of the services to issue directives for the conduct of intelligence operations. The directives should:

[8] Task Team, 'Final Report', op cit, pg. 59.
[9] Ibid.
[10] Ibid, pp. 78-79.

- Determine specific internal processes for priority-setting and targeting in light of the National Intelligence Priorities.

- Specify the criteria to be applied in authorising the use of intrusive techniques.

- Outline the levels of authority required to approve intrusive operations, dependent on the risk of compromise.

- Determine the level and system of supervision of high-risk intelligence operations.

- Specify the procedures to be followed in authorising specific methods of intrusive collection of intelligence.

- Determine the requirements and procedures for dealing with incidental information collected during intrusive operations.

- Determine the details required for record-keeping of all processes relating to the authorisation and management of intrusive operations.

- Oblige the intelligence services to establish internal mechanisms for monitoring compliance with these directives and dealing with failures of compliance.

▪ Mandate the Minister to institute a community-wide system of monitoring compliance with the regulations.

The Task Team proposed further 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.

The Task Team recommended that the Minister, together with the heads of the services and the intelligence academy, develop a programme of education in the civilian intelligence community to promote constitutionality, legality, accountability, integrity and professionalism in the conduct of intelligence operations.[11]

## 9.3 Comment on the Findings and Recommendations of the Task Team

For the most part, we believe that the findings and recommendations of the Task Team are sound and should be supported by the Minister and the JSCI. However, we have the following disagreements, qualifications and additions:

- There should be an additional critical factor in assessing the operational policies of the intelligence services, which is that the policies must interpret correctly and be properly aligned with the relevant constitutional and legislative provisions. Where the policies mistakenly ignore or misinterpret these provisions, then intelligence operations might comply with the internal rules but inadvertently be unconstitutional and/or illegal (Section 11.7).

- We support the introduction of a civic education programme but disagree strongly with the Task Team's view that it is acceptable for intelligence officers to bend the rules in order to deal with serious threats. This position is unconstitutional. It also contradicts the Minister's insistence on compliance with laws and rules (Section 11.2). In addition, it undermines the internal controls, negates the policy emphasis on compliance and will prevent the development of an institutional culture of respect for the law (Section 11.6).

[11] We discuss this education programme in Section 11.4.

- We agree with the Task Team's proposals aimed at tightening controls over intrusive operations. However, we believe that ministerial approval should be required for all intrusive operations and not only for high-risk operations; that judicial authorisation should be required for the use of intrusive methods since they infringe constitutional rights; and that the use of intrusive measures should be governed by legislation and not only by regulations and departmental policies (Chapter 7).

- The Task Team maintains that the primary criterion for determining the level of authorisation, management and supervision of an operation should be the risk that the operation might be compromised. We believe that the risk that an operation might violate constitutional rights and interfere with the democratic political process is also a vitally important consideration.

- As a further internal control measure, we recommend the re-introduction of clearance panels for the authorisation of intrusive operations. These panels of senior intelligence officers, which functioned in previous years but have since been abandoned, entail a peer review of applications to engage in intrusive operations. This allows for collective judgement and makes it very difficult to launch an operation for improper purposes. Internal audit committees are less effective in this regard since they generally conduct compliance tests after an operation has taken place.[12]

- We agree that there is a need for policy on dealing with incidental information collected during intrusive operations and make a recommendation on this matter in Section 7.7.

- The Task Team did not address the topic of financial policies and controls but we believe there is an urgent need for reform in this area (Chapter 10).

[12] Information provided to the Commission in informal discussions with intelligence officers.

## 9.4 A Problem of Too Much Regulation and Oversight?

### *9.4.1 The perspectives of the intelligence organisations*

Some intelligence officials hold the view that there is excessive oversight of the intelligence organisations and that the organisations are over-regulated or in danger of becoming over-regulated.[13] In its report to the Minister for Intelligence Services, the Task Team warned that "over-regulation and over-accountability of the intelligence services have the potential to render the intelligence services unable to carry out their noble duty to protect constitutional democracy".[14]

NIA maintains that the oversight and review mechanisms governing the intelligence services are necessary and appropriate.[15] However, it would be helpful if steps were taken to ensure that the oversight becomes more structured and routine. In addition, NIA warns that "over-regulation and over-accountability have the potential of preventing or limiting the effective pursuit of vital national interests and rendering the Agency incapable of carrying out its duty to protect constitutional democracy and combating terrorism and organised crime".[16]

In the assessment of SASS, the intelligence services are subject to more oversight than any other government department in South Africa, any enterprise in the private sector and any other intelligence department in the world. The excessive oversight is a reaction to the situation that prevailed during the apartheid era, when intelligence was a law unto itself and prone to illegal conduct and irregular behaviour. This situation no longer pertains and the intelligence services are now run along professional lines.[17]

---

[13] Task Team, 'Final Report', op cit, pg. 48.
[14] Ibid, pg. 59.
[15] National Intelligence Agency, 'Base Document', op cit, pg. 36.
[16] Ibid.
[17] South African Secret Service, 'Presentation to the Ministerial Review Commission', 31 January 2007, pg. 15.

The main recommendation that SASS made to the Commission was for a major reform of intelligence oversight:

> A Basic Recommendation: a reform of approach to intelligence oversight based on the premise that intelligence is an institution of professional people and that the regulatory strategy should be built on a greater degree of self regulation, a clearer set of performance indicators and zero tolerance of illegal conduct and abuse of power.[18]

*9.4.2 Comment*

The arguments of the intelligence services can be divided into two strands. The first is that the services are obliged to spend too much time and effort attending to the various review and reporting requirements of the control and oversight bodies, namely the Minister, the JSCI, the Auditor-General and the Inspector-General. The services are in continuous audit, review and report writing mode at the expense of pursuing their intelligence functions.

More specifically, SASS insists that there is too much overlap and duplication between the oversight of the Auditor-General and that of the Inspector-General; there is insufficient rationalisation and integration of the work of these bodies; and the oversight institutions do not co-ordinate their activities, with the result that they undertake reviews and expect reports from the services throughout the year. There is thus a plea for more synchronised and efficient oversight, monitoring and review.[19] There should be one annual audit plan that covers the activities of the entire oversight community.[20]

We disagree with the claim that the intelligence organisations labour under a greater oversight burden than any other body in the world. All government departments in South Africa (and other democratic countries) are subject to

[18] South African Secret Service, 'Presentation', op cit, pg. 15.
[19] Ibid.
[20] Ibid, pg. 37.

ministerial control, parliamentary oversight and independent financial scrutiny. The additional oversight mechanism in the case of the intelligence organisations is the Inspector-General. Institutions of this kind exist in other countries, including Australia, Bosnia and Herzegovina, Canada, New Zealand and the United States.

Nevertheless, we are sympathetic to the call for greater rationalisation and co-ordination of intelligence oversight and review activities, and we would therefore support a search for solutions that do not compromise the quality of control and oversight.

The second strand of the argument regarding excessive oversight and over-regulation is that the intelligence services are now professional organisations and are no longer a law unto themselves. Illegal activities are aberrations rather than pervasive. In addition, the oversight mechanisms are unduly constraining, impairing the ability of the services to carry out their duties. Accordingly, regulatory arrangements should be based more on self-regulation than on external oversight.

We are not sympathetic to this leg of the argument. It fails to take adequate account of the distinct threats that intelligence services pose to democracy (Section 2.2). These threats are summed up perfectly by the Task Team itself:

> The state gives its intelligence services two very powerful and dangerous rights – the right to operate in secrecy and the right to invade the privacy of citizens. In South Africa's past (and in many other jurisdictions – past and present) these rights were heavily abused to protect the state from the legitimate struggle for freedom and democracy. With the birth of a democratic South Africa, our new legislature was at pains to ensure that a democratic

intelligence dispensation could never again abuse these two rights.[21]

As we point out elsewhere in this Report, the intelligence organisations also have the means to violate other constitutional rights, interfere in lawful political and social activities, favour some political parties and politicians at the expense of others, and subvert the democratic process (Chapters 2, 6 and 7). Given these dangers, intelligence services cannot meaningfully be compared with other government departments and private sector enterprises.

It must be stressed that the dangers are not peculiar to South Africa and that the oversight mechanisms do not imply that NIA, SASS and the NCC are steeped in misconduct. The dangers are inherent in intelligence organisations, which are consequently subject to special controls and oversight throughout the democratic world.[22] The bottom line is well captured by NIA: "Because of their power and the inherent risk of abuse of power, the security services should be subject to extensive controls and rigorous oversight by the elected and duly appointed civil authority".[23]

## 9.5 Recommendations

There should be an additional critical factor in assessing the operational policies of the intelligence services, which is that the policies must interpret correctly and be properly aligned with the relevant constitutional and legislative provisions.

[21] Task Team, 'Final Report, op cit, pg. 47.
[22] See, for example, Hans Born, Loch K. Johnson and Ian Leigh (eds), *Who's Watching the Spies? Establishing Intelligence Service Accountability*, 2005, Washington D.C.: Potomac Books; and Hans Born and Mariana Caparini (eds), *Democratic Control of Intelligence Services: Containing Rogue Elephants*, 2007, Aldershot: Ashgate.
[23] National Intelligence Agency, 'Base Document', op cit, pp. 11-12.

We support the recommendations of the Task Team regarding the need for ministerial regulations and operational directives that tighten controls over intrusive operations.

As discussed in Chapter 7, intrusive operations should be governed by legislation and should be subject to ministerial approval and judicial authorisation.

The determination of the level of authorisation, management and supervision of an intelligence operation should take account of the risk that the operation might violate constitutional rights and interfere with the democratic political process.

The intelligence services should establish internal clearance panels comprising senior officials in order to assess applications to initiate intrusive operations.

Efforts should be made to achieve greater rationalisation and co-ordination of intelligence oversight and review activities, provided that the solutions do not compromise the quality of control and oversight.

## CHAPTER 10: FINANCIAL CONTROLS AND OVERSIGHT

### 10.1 Introduction

The financial controls and oversight of the intelligence services are important for two reasons. First, the risk of abuse of funds for personal enrichment, which is always present when large amounts of money are held by an organisation, is particularly high where the money can be used for secret projects and information is only shared on a strict need-to-know basis. Payments made to informants and expenditure incurred in setting up front companies, for example, are obviously at greater risk of abuse than normal financial transactions.

Second, it is possible for intelligence officers to cause political mischief without spending any money, such as by spreading false information about a political party or politician, but major acts of mischief and sustained interference in politics 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.

In this Chapter we first summarise and comment on the laws and control and oversight mechanisms that regulate financial matters in the intelligence services, taking account of the submission we received from the National Treasury. We then present and comment on the Auditor-General's submission to the Commission.[1]

The Chapter covers the following topics:

- The main legislation governing the funds and financial administration, management and oversight of the civilian intelligence organisations (Section 10.2).

[1] In preparing this Section we were also assisted by research undertaken by Dr Sandy Africa.

- The failure to publish and present to Parliament the annual budgets and financial reports of the intelligence services (Section 10.3).

- The financial controls of the intelligence services (Section 10.4).

- The Auditor-General's submission to the Commission (Section 10.5).

- The failure to publish the audit reports on the intelligence services (Section 10.6).

- The absence of a complete financial audit of the intelligence services (Section 10.7).

- Recommendations (Section 10.8).

## 10.2 Legislation

### *10.2.1 Summary of main legislation*

The main legislation governing the funds and financial administration, management and oversight of the civilian intelligence agencies is as follows:

- The Secret Services Act No. 56 of 1978, which provides for the establishment of the Secret Services Account. It also provides for the establishment of a Secret Services Evaluation Committee whose members are appointed by the President. This Committee does not exist at present.[2]

- The Security Services Special Account Act No. 81 of 1969, which provides for the establishment of the Security Services Special Account. The funds

[2] Letter to the Commission from NIA, 24 October 2007.

appropriated by Parliament for the civilian intelligence organisations are transferred into this account via the Secret Services Account. The account is under the control of the directors-general of NIA and SASS, who must cause proper records to be kept of all moneys received and expended.[3] The account is audited by the Auditor-General.[4]

- The Public Finance Management Act No. 1 of 1999, which aims to ensure the accountability, transparency and sound management of the revenue, expenditure, assets and liabilities of government departments and other specified entities. The Act prescribes the way in which public funds must be managed by departments and specifies the responsibilities of the heads of department regarding financial management, controls, budgets and reports.

- The Public Audit Act No. 25 of 2004, which provides for the functions of the Auditor-General and the auditing of institutions in the public sector.

- The Intelligence Services Act No. 65 of 2002, which states that the directors-general of NIA and SASS are the heads and the accounting officers of their respective organisations.[5] The Act also confers certain powers on the Minister for Intelligence Services, who may do or cause to be done all things which are necessary for the efficient superintendence, control and functioning of the intelligence services and SANAI.[6] The Minister may acquire or dispose of immovable property.[7] After consultation with the JSCI, he or she may make regulations regarding the control over and administration of funds appropriated to the services and SANAI in order to bring about the systematic and orderly management thereof and promote efficiency and economy in the utilisation thereof.[8]

[3] Section 3 of the Security Services Special Account Act of 1969.
[4] Section 4 of the Security Services Special Account Act.
[5] Section 3(3)(b) of the Intelligence Services Act of 2002.
[6] Section 12(1) of the Intelligence Services Act.
[7] Section 12(2) of the Intelligence Services Act.
[8] Section 37(1)(m) of the Intelligence Services Act.

- The Intelligence Services Oversight Act No. 40 of 1994, which covers the financial oversight functions of the JSCI. The JSCI must obtain the annual audit reports prepared by the Auditor-General; consider the financial statements of the intelligence organisations, the audit reports issued on those statements and any reports issued by the Auditor-General on the affairs of the intelligence organisations; and report thereon to Parliament.[9] The JSCI must also obtain from the responsible ministers the budgets of each of the intelligence organisations.[10]

*10.2.2 Comment on the legislation*

The overall legislative framework governing the funds, financial controls and financial oversight of the intelligence services is comprehensive and sound. In particular, the Public Finance Management Act of 1999 and the Public Audit Act of 2004 are modern pieces of legislation that reflect state-of-the-art principles of financial governance. In terms of the two Acts, the heads of the intelligence services have a high level of accountability and a set of rigorous regulatory obligations that are no different from those of other heads of department.

The Security Services Special Account Act of 1969 and the Secret Services Act of 1978, on the other hand, are anachronistic relics of the murky business of covert security funding in the apartheid era. We recommend that these Acts be repealed. This view is shared by the National Treasury, which believes that the Acts are redundant. The National Treasury proposes that, as with other government departments, the funds allocated to the intelligence services by Parliament should go directly to them.[11]

[9] Section 3(a)(i) of the Intelligence Services Oversight Act.
[10] Section 3(a)(iv) of the Intelligence Services Oversight Act.
[11] National Treasury, 'Submission by the National Treasury to the Ministerial Review Commission on Intelligence', 11 December 2007; and meeting with the Commission, 20 March 2008.

### 10.3 Failure to Publish Intelligence Budgets and Financial Reports

In its submission to the Commission, the National Treasury expressed concern that the intelligence services do not have their own budget vote in respect of the funds appropriated to them annually by Parliament.[12] Instead, these funds appear as a single line transfer payment in the budget vote of the National Treasury. To put the matter graphically: whereas the estimate of national expenditure for the Department of Correctional Services runs to 20 pages of figures and explanations, the budget vote for NIA and SASS is limited to a single line.

The budgets and annual financial reports of the intelligence services are reviewed by the JSCI, which reports to Parliament, but the documents themselves are confidential and are not presented to Parliament. As a result, according to the National Treasury, the intelligence services are not directly accountable to Parliament for their budgets and spending.

This arrangement deviates from the Constitution, which states that national, provincial and municipal budgets and budgetary processes must promote transparency and accountability.[13] The arrangement is also inconsistent with the public finance management principle that transparency leads over time to better delivery and better decision-making on allocation of funds.

One of the fundamental rules of a democratic dispensation is that government can only spend money with the approval of Parliament. Yet our Parliament does not have any direct insight into the budgets and activities of the intelligence services and therefore cannot engage in an informed debate on these matters. These limitations apply equally to the public, whose taxes are used to fund the intelligence services.

[12] National Treasury, 'Submission by the National Treasury', op cit.
[13] Section 215(1) of the Constitution.

Intelligence organisations throughout the world are resistant to revealing their budgets on the grounds that foreign intelligence agencies would thereby gain an advantage over them. We believe that this argument is overstated. A foreign agency would derive no benefit from knowing how much money another country spends on its intelligence bodies. Nor indeed would any advantage or prejudice arise from disclosing the spending breakdown on personnel, operating costs and capital expenditure. It is only at a higher level of detail – regarding targets, methods, sources and operational outputs and constraints – that security could be undermined through disclosure.

We have read a number of the budgets and strategic plans presented to the JSCI by NIA and SASS and do not believe that disclosure of these documents would in any way prejudice intelligence operations or the security of the country.

We support the National Treasury recommendation that the intelligence services should have their own vote in respect of monies approved annually by Parliament. The services should present annual budgets and financial reports to Parliament. When doing so, they would not be expected to disclose information that would compromise their operations, methods or sources.

### 10.4 Financial Controls

There are three levels of financial control in the intelligence services:

- The Minister for Intelligence Services has issued directives that govern expenditure on intelligence operations. These directives, discussed below, appear in a document entitled “Ministerial Delegation of Powers and Direction of Payment”.

- In accordance with legislative requirements and Treasury regulations, the heads of the intelligence services have issued directives regulating

financial administration and expenditure on operational activities. The directives aim to ensure that the correct procedures and control systems exist and are adhered to.

- The intelligence services have internal audit committees that are responsible for monitoring compliance with the directives and relevant legislation through regulatory and performance audits of expenditure.

There is also the external audit conducted annually by the Auditor-General in terms of the Public Audit Act of 2004. The Auditor-General's reports are presented to the Minister for Intelligence Services and the JSCI. The audits are a form of external oversight rather than internal control but the Auditor-General's staff work closely with the internal audit personnel of the intelligence services to improve the control systems (Section 10.5).

In order to assess the adequacy of the financial controls of the intelligence organisations and compliance with these controls, we requested the Auditor-General to prepare a submission and address a number of questions about financial controls over covert operations.[14] We also had a meeting with the Auditor-General's staff who are responsible for conducting the audits of NIA and SASS.

### 10.5 Submission of the Auditor-General

We present below the key points that were made in the Auditor-General's submission to the Commission:[15]

- The Auditor-General undertakes two kinds of audit, namely regularity audits and performance audits. In relation to the intelligence services, the

[14] Section 1 of the National Strategic Intelligence Act No. 39 of 1994 defines "covert collection" as "the acquisition of information which cannot be obtained by overt means and for which complete and continuous secrecy is a requirement".
[15] Auditor-General, 'Review of the Civilian Intelligence Services', submission to the Commission, 22 January 2008.

Auditor-General has only undertaken regularity audits. This includes testing system controls and performing value-for-money procedures that relate to supply chain management, subsistence and travel, and human resource management. Performance audits, on the other hand, focus on information relating to the performance of the audited body against specified objectives.

- The Auditor-General reviews the financial policies of NIA and SASS on an annual basis and brings control weaknesses to the attention of senior management. The Auditor-General also audits the funds that are transferred to NIA and SASS via the Secret Services Act of 1978.

- NIA and SASS comply with the requirement of the Public Finance Management Act of 1999 to prepare financial statements and submit these statements to the Auditor-General. SASS is maintaining full and proper records. At NIA, non-adherence was found in respect of the asset register and guarantees.

- In general, SASS has adequate policies and controls to manage its financial activities. During the 2006-7 financial year NIA reviewed and improved its financial policies. The review covered NIA's spending entities, namely NICOC, the NCC, COMSEC and the OIC, and included the policies relating to the funding of covert operations.

- The controls that are specified in the intelligence services' policies on funding covert operations seem to be adequate. The Auditor-General has tested these controls and found that they are adhered to in general.

- The Auditor-General had no concerns about discretionary spending by the heads of the services during the 2005-6 and 2006-7 audits.

- Specific concerns regarding financial, administrative and other compliance and control matters are raised in the annual audit reports for the services.

In addition to the above, the Auditor-General's submission to the Commission explained that annual audits have three components: planning, execution and reporting. The following points were made about these components in relation to the audits of the intelligence services:

- Planning. The Auditor-General has helped NIA and SASS to improve their system, manual and management controls. At SASS the controls are functioning effectively and the information system is such that reliance thereon is currently being tested; no reliance is yet placed on the work of the internal audit section as the internal auditors requested time to address control weaknesses that were identified previously. At NIA the control environment is still stabilising; consequently, no reliance is placed on the controls but reliance could possibly be placed on certain areas of work performed by the internal audit section.

- Execution. It is not always possible for the Auditor-General to obtain the evidence that is required to draw reasonable conclusions. More specifically, in the case of covert operations it is not possible to obtain evidence from an independent source or through direct observation. The Auditor-General's staff cannot interview the paid informants of the intelligence services and they cannot verify the existence of assets, such as surveillance equipment, that are being used in covert operations. Nor does the Auditor-General have the expertise to verify that the amounts paid to informants are justified in terms of the quality of information they give. It is expected that the Inspector-General of Intelligence (hereafter the "Inspector-General") will be able to provide expert confirmation.

- In light of these limitations, the Auditor-General can reach a conclusion on whether the controls over covert operations are being adhered to but cannot test the effectiveness of the controls. In general, a lower level of audit assurance is obtained in relation to covert operations.

- The following qualification is thus included in the audit reports for the intelligence services: “Owing to the nature of certain transactions and the circumstances under which they are incurred and recorded as well as the circumstances under which assets and services are procured and utilised, the level of audit assurance will often be lower than is normally the case with ordinary audits. These limitations must be taken into account when reading this report”.

- The Auditor-General has consulted the Inspector-General and the Minister for Intelligence Services about raising the level of audit assurance. The Auditor-General and the Inspector-General are piloting a project in the 2007-8 financial year whereby the Inspector-General’s review of covert operations will potentially be utilised by the Auditor-General. The Auditor-General will evaluate the work performed by the Inspector-General and, if deemed reliable in terms of the relevant rules, will be used to support the audit opinion.

- Reporting. At both NIA and SASS, audit steering committee meetings are held regularly to discuss the planning, execution and findings of the audit. In general, these meetings are effective and efficient. An audit steering committee comprises the staff of the Auditor-General and the staff of the organisation being audited.

- NIA and SASS share an audit committee, the members of which are appointed by the Minister for Intelligence Services. The committee meets four times a year. The meetings are always attended by the NIA and SASS accounting officers or their delegates, the chief financial officers, the internal audit staff and the Auditor-General’s staff. In the view of the Auditor-General, the audit committee functions effectively. It is responsible for reviewing internal control structures, including financial control, accounting and reporting systems; internal audit functions; liaison with the external auditors; and monitoring compliance with legal requirements and the organisations’ codes of conduct.

- In terms of the Public Audit Act of 2004, all audit reports are submitted to the Minister for Intelligence Services for review before the reports are finalised. At the request of the Minister, information that is detrimental to national security may be excluded from the audit but the report must then state that information has been excluded. Over the past four years the Minister has not requested the Auditor-General to remove any information on this ground.

- The JSCI is responsible for oversight of the civilian intelligence services. This includes oversight of the administration, financial management and expenditure incurred by the services as well as reporting thereon to Parliament. To enhance its support to the JSCI, the Auditor-General is in the process of signing a memorandum of understanding with the Committee.

- At the invitation of the JSCI, the Auditor-General has attended budget presentations by the intelligence services to the Committee; briefed the Committee on the audit report findings; served as an expert witness when the services have met with the JSCI to discuss the audit reports; and conducted a special investigation into certain expenditure.

In the rest of this Chapter we raise two major concerns about the matters covered in the Auditor-General's submission.

### 10.6 Failure to Publish the Audit Reports on the Intelligence Services

The Constitution states that the Auditor-General must audit and report on the accounts, financial statements and financial management of all national and provincial state departments and administrations.[16] The Constitution provides further that "the Auditor-General must submit audit reports to any legislature

[16] Section 188(1) of the Constitution.

that has a direct interest in the audit and to any other authority prescribed by national legislation. All reports must be made public".[17]

Despite this provision, the audit reports on the intelligence services are presented only to the JSCI and are classified as 'confidential' or 'secret'. As a result, the reports are not in the public domain. This is clearly unconstitutional.

In the view of the Auditor-General, the audit reports on NIA and SASS should be made public and should be presented to Parliament after the reports have been discussed by the JSCI.[18] The Auditor-General is convinced that there is nothing in the reports that would prejudice the services or compromise the security of the country.

It is relevant in this regard that the Public Audit Act of 2004 contains several provisions on protection of sensitive information. It states that the Auditor-General must take precautionary steps to guard against the disclosure of secret or classified information obtained in the course of an audit.[19] The Auditor-General may not disclose facts that "would harm the national interest".[20] When reporting on a confidential security account, the Auditor-General "must have due regard for the special nature of the account and, on the written advice from the relevant Minister, on the basis of national interest, may exclude confidential, secret or classified details of findings from the audit report, provided that the audit report states that these details were excluded".[21]

We have read a number of the audit reports on NIA and SASS and share the Auditor-General's view that the reports should be made public. There is no reasonable and justifiable basis for deviating from a constitutional obligation that serves to inform the public of the adequacy of financial controls in government departments and to assure the public that effective financial

[17] Section 188(3) of the Constitution.
[18] Meeting with Auditor-General's staff, 3 December 2007.
[19] Section 18(1) of the Public Audit Act.
[20] Section 18(2) of the Public Audit Act.
[21] Section 22(1) of the Public Audit Act.

oversight is being exercised by the Auditor-General. There is no need for concern that sensitive information will be disclosed since the Minister for Intelligence Services is permitted to request that such information be withheld.

### 10.7 The Absence of a Complete Audit

We are extremely concerned that the Auditor-General is not conducting a complete and thorough audit of the intelligence services' expenditure and assets relating to covert operations. This concern is shared by the Inspector-General.[22] Precisely because covert operations are secret, the potential for abuse of funds is high and there is a corresponding need for rigorous oversight.

The Auditor-General's staff who are responsible for the audits of NIA and SASS told us that they have 'top secret' security clearances and that there is no legal barrier to their scrutinising expenditure on covert operations. However, there is resistance to such scrutiny from sectors of the intelligence community, which believe that there are compelling security reasons to avoid exposing the details of covert operations to people who have no intelligence training. There is also an element of self-restraint on the part of the Auditor-General's staff, who have some anxiety about peering too deeply into the perilous world of covert intelligence activities.

We are sympathetic to these reservations and therefore support strongly the need for the Auditor-General to involve the Inspector-General in the annual audits.

The Inspector-General informed us that in 2007 the Minister for Intelligence Services had facilitated consultations between the Office of the Inspector-General of Intelligence (OIGI) and the Office of the Auditor-General in order to

[22] Letter from the Inspector-General of Intelligence to the Commission, 4 April 2008.

rectify the practice of limited access leading to qualified audits. The initial understanding was that the OIGI staff would carry out specific procedures on behalf of the Auditor-General in relation to source remuneration, covert assets and contracts. This understanding has not yet been formalised, however, and the relationship between the Inspector-General and the Auditor-General is still in its infancy.[23]

### 10.8 Recommendations

The Security Services Special Account Act No. 81 of 1969 and the Secret Services Act No. 56 of 1978 are relics of the apartheid era and should be repealed. As with other government departments, the funds allocated to the intelligence services by Parliament should go directly to them.

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. The budgets and financial reports should exclude information that would endanger security or compromise intelligence operations, methods or sources.

As required by the Constitution, the audit reports on the intelligence services should be presented to Parliament. In accordance with the Public Audit Act No. 25 of 2004, sensitive information can be withheld from the reports if deemed necessary by the Auditor-General or the Minister for Intelligence Services.

The audit reports on the intelligence services for the past five years should be disclosed to Parliament. This process should be co-ordinated by the Minister in consultation with the JSCI.

[23] Letter from the Inspector-General of Intelligence to the Commission, 4 April 2008.

As a matter of urgency, the Auditor-General and the Inspector-General of Intelligence should finalise arrangements whereby the Inspector-General provides the assistance that is necessary to ensure a satisfactory audit of expenditure on covert operations. The Minister for Intelligence Services should facilitate further meetings between the Auditor-General and the Inspector-General for this purpose.

## CHAPTER 11: INSTITUTIONAL CULTURE

### 11.1 Introduction

The institutional culture of the intelligence services is every bit as crucial as their internal rules because it is one of the major 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 attitude of the senior managers of the intelligence organisations is especially important. If they break the rules or tolerate the breaking of rules – either because they are negligent or because they believe that rule-breaking is justified – then the formal controls will count for little and the risk of misconduct will be high.

Our overall assessment is that the institutional culture of the intelligence community has several positive features but they are undermined by four negative trends. The positive features are the following:

- Executive policy on the political norms governing the intelligence services is perfectly aligned to the Constitution and democratic principles.

- There is a constitutional injunction, which is reiterated in executive and departmental policies, that the intelligence services must be politically non-partisan.

- The operational policies of the services emphasise compliance with the Constitution and the law.

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

As discussed in this Chapter, the negative trends relate to the politicisation of NIA; unsatisfactory labour relations and grievance mechanisms; the belief among some senior officials that it is legitimate to break the rules when dealing with serious security threats; and the absence of adequate legal expertise in the intelligence community.

We have not conducted the kind of forensic investigation that would indicate the prevalence of misconduct in the intelligence services. An investigation of this nature lay outside our mandate. Nevertheless, there are grounds for concern in light of the intelligence crisis of 2005/6 (Section 1.2), the Inspector-General's perspective on the institutional culture of the services (Section 11.5.1), the comments of the officials quoted in Section 11.6.1, and the high level of secrecy that inhibits rigorous accountability (Chapter 12).

This state of affairs underscores the vital role of the Office of the Inspector-General of Intelligence (OIGI).[1] The OIGI has the mandate, powers and expertise to penetrate the veil of secrecy, identify weaknesses in control systems, detect malpractice and recommend punitive or corrective action to the heads of the services, the Minister and the JSCI. Ultimately, the most effective strategy for preventing misconduct is an approach of zero tolerance of misconduct when it occurs.[2] This approach should be followed by the Minister, the JSCI, the OIGI and the heads of the intelligence services.

[1] We discuss the Inspector-General of Intelligence in Chapter 5.
[2] In its submission to the Commission, SASS recommended that there be "zero tolerance of illegal conduct and abuse of power". SASS, 'Presentation to the Ministerial Review Commission', 31 January 2007, pg. 15.

This Chapter covers the following topics:

- Executive policy on the political norms governing intelligence (Section 11.2).
- Political non-partisanship and non-interference (Section 11.3).
- The civic education programme for the intelligence services (Section 11.4).
- The Inspector-General's perspective (Section 11.5).
- Bending the rules (Section 11.6).
- The absence of adequate legal expertise in the intelligence community (Section 11.7).
- Recommendations (Section 11.8).

## 11.2 Executive Policy on the Political Norms Governing Intelligence

One the major themes of the White Paper on Intelligence of 1994 is the transformation of the intelligence community from a repressive and unaccountable apparatus to one that complies with the rule of law and other democratic norms. These norms include political non-partisanship and non-interference; respect for human rights; executive control of the intelligence organisations; and subordination and accountability to Parliament and the other constitutional bodies mandated to oversee these organisations (Chapter 3).

In response to the intelligence crisis of 2005/6, Minister Kasrils produced and disseminated widely within the civilian intelligence community a statement entitled 'Five Principles of Intelligence Service Professionalism'. This document is displayed prominently in the offices of the intelligence organisations and a summary appears on the Ministry website.[3] We reproduce the statement below because it encapsulates what we believe to be the correct political approach to intelligence in a constitutional democracy.

**Five Principles of Intelligence Service Professionalism**

Message from the Minister for Intelligence Services
Mr Ronnie Kasrils (MP)
September 2005

1. **We must accept the fundamental principle of legality.** We do not stand above the law. We are not exempt from the law. We are unequivocally and emphatically bound by the law and the Bill of Rights. All our operations must be conducted within the parameters of the Constitution and relevant legislation. The founders of our democracy took this issue so seriously that they enshrined in our Constitution the requirement that members of the security services should disobey a manifestly illegal order.

2. **We must accept the fundamental principle that we are subordinate and accountable to the elected and duly appointed civilian authority.** The establishment and maintenance of democracy is not possible if we do not accept this principle.

3. **We must accept the fundamental principle of political non-partisanship.** We may not further, in a partisan manner, any interest of a political party and we may not prejudice a political party interest that is legitimate in terms of the Constitution. We must refrain from involvement in party politics. How you vote is your preference outside the workplace.

[3] The Ministry website can be viewed at www.intelligence.gov.za.

Conversely, government and opposition groups should not misuse the Intelligence Services for partisan political ends.

4. **We must accept that our Services owe no loyalty to any political party or faction, or statutory or non-statutory security service of the past era.** We owe our loyalty to the Constitution, to the citizens of our country, to the state, to the intelligence structure in which we are employed, and to each other. Any kind of partisan conflict within our ranks is unprofessional and unacceptable and cannot be tolerated.

5. **We must strive to maintain high standards of technical proficiency in the performance of our functions, enhance our skills and knowledge, safeguard the property and other assets of the state, and undertake our activities in an efficient and effective manner.**

These principles constitute the normative foundation of the new civic education programme for the intelligence services (Section 11.4).

## 11.3 Political Non-Partisanship and Non-Interference

In this Section we first present the constitutional, legislative and policy provisions on political non-partisanship and non-interference, and then discuss the problem of a politicised domestic intelligence agency.

### *11.3.1 Constitutional, legislative and policy provisions*

The Constitution, legislation and intelligence policies reflect an acute awareness of the dangers that flow from intelligence services behaving in a politically partisan fashion. Section 199(7) of the Constitution contains a firm injunction in this regard:

> Neither the security services nor any of their members may, in the performance of their functions, a) prejudice a political party interest

> that is legitimate in terms of the Constitution; or b) further, in a partisan manner, any interest of a political party.

The Intelligence Services Act No. 65 of 2002 states that the heads of the intelligence services must take steps to ensure adherence to this constitutional provision.[4]

The Intelligence Services Regulations of 2003 provide that a member of the intelligence services is guilty of misconduct if he or she "abuses his or her position inside or outside the scope of his or her official duties to promote or prejudice personal interests or those of any party, group, political organisation or other individual".[5]

The White Paper on Intelligence of 1994 insists on "adherence to the principle of political neutrality".[6] As noted previously, the White Paper elaborates as follows:

> Measures designed to deliberately interfere with the normal political processes in other countries and with the internal workings of parties and organisations engaged in lawful activity within South Africa must be expressly forbidden. Intelligence agencies or those within them guilty of such breaches must be disciplined in the severest terms.[7]
>
> No intelligence or security service/organisation shall be allowed to carry out any operations or activities that are intended to undermine, promote or influence any South African political party or organisation at the expense of another by means of any acts (eg

[4] Section 4(b) of the Intelligence Services Act.
[5] Quoted in National Intelligence Agency, 'Base Document for Presentation on Matters Relating to the Terms of Reference of the Ministerial Review Commission', 24 January 2007, pg. 30.
[6] White Paper on Intelligence, 1994, pg. 5.
[7] Ibid, pg. 8.

> "active measures" or "covert action") or by means of disinformation.[8]

A number of NIA's operational policies reiterate the ban on political interference and partisanship. For example, the Agency's Service Standards Directive, which deals with work ethics, includes the following points:

> No member shall use his or her official authority or influence, or permit the use of a programme/activity administered by the Agency, to interfere with or affect the result of an election or nomination of a candidate or to achieve any other political purpose. Additionally, no member shall engage in any act or attempt to interfere with anyone who seeks to pay, lend, or contribute private funds or private property to a person or political organisation for political purposes. Any member who violates either of these provisions within the working environment shall be subject to disciplinary action.[9]

*11.3.2 The on-going politicisation of NIA*

As a result of the Cold War and the struggle against and in defence of apartheid, the statutory and non-statutory intelligence services were highly politicised at the time of integration in 1994. Some historical allegiances and animosities are likely to linger until a new generation of intelligence managers is in place. Transformation is a long-term challenge that requires constant vigilance and attention from the heads of the services and the Minister.

The problem has been compounded by NIA's political intelligence focus. This requires NIA to monitor and investigate lawful political activities and developments within and between political parties and other organisations. The political intelligence focus thus draws NIA directly into the arena of party

[8] White Paper on Intelligence, pg. 12.
[9] Quoted in National Intelligence Agency, 'Base Document', op cit, pp. 31-32.

politics, contributes to the politicisation of the Agency and heightens the risk of interventions that favour one party or faction to the detriment of others.[10]

As noted in Section 6.8, NIA itself is deeply concerned about the dangers associated with its political intelligence focus and the other political aspects of its mandate. It believes that these functions "may be interpreted and/or abused as party political 'apparatchik' with the purpose of dealing with political opponents in an undemocratic manner. Such abuse will compromise [NIA's] credibility".[11] In addition, "the politicisation of the intelligence process and product has a high risk of stunting the command and control, oversight and accountability of the Agency and impedes its abilities to truly serve the national interest".[12]

There are two courses of action that might help to address the problem of inappropriate political conduct by the intelligence organisations and their members. First, as discussed in Chapter 6, NIA's political intelligence function as presently conceived should be abandoned.

Second, it should be made a criminal offence for intelligence officers to act in a politically partisan manner or interfere in lawful political activities and, similarly, it should be an offence for any other person to request or instruct intelligence officers to act in this manner. The White Paper states that intelligence personnel who are guilty of such acts should be disciplined in the most severe terms. To give effect to this statement, the intelligence legislation should proscribe the prohibited activities as criminal offences.

[10] We discuss this problem in Chapter 6.
[11] National Intelligence Agency, 'Base Document', op cit, pg. 34.
[12] Ibid, pg. 13.

## 11.4 Civic Education Programme for the Intelligence Services

### *11.4.1 The Civic Education Charter*

As a further response to the intelligence crisis of 2005/6, Minister Kasrils decided to establish a Civic Education Programme (CEP) for the civilian intelligence services. He set up a CEP Steering Committee comprising the heads of the Ministry, NIA, SASS, NICOC and SANAI, and a Technical Committee comprising other staff. The committees were mandated to prepare a civic education charter, curricula and programme of action.[13]

The CEP is "aimed at deepening the culture of respect for the Constitution and the rule of law within the intelligence services as key professional values of an intelligence officer in a non-racial, non-sexist and democratic South Africa".[14] The guiding principles of the programme are those contained in the statement by Minister Kasrils on intelligence service professionalism (Section 11.2).

According to the Civic Education Charter, the motivation for the programme derives principally from the Constitution, which stipulates that the security services must act, and must teach and require their members to act, in accordance with the Constitution and the law.[15] The further motivation is that "the promotion of a core set of values for professional intelligence services in a constitutional democracy will promote cohesion, trust and camaraderie within the services".[16]

The Charter allocates roles and responsibilities as follows:

[13] One of the Commission's members, Laurie Nathan, is a member of the CEP Steering Committee and Technical Committee.
[14] Ministry of Intelligence Services, 'Civic Education Charter of the Civilian Intelligence Services', 31 January 2007, pg. 1.
[15] Section 199(5) of the Constitution.
[16] Ministry of Intelligence Services, 'Civic Education Charter', op cit, pg. 1.

- The Minister is the overall sponsor of the CEP and must ensure that the heads of the intelligence organisations account for its implementation.

- The Steering Committee comprising the heads of the intelligence organisations must advise the Minister on implementation, provide the necessary resources and promote an organisational culture that fosters a professional work ethic based on an agreed set of values.

- The heads are also responsible for implementing the CEP in their respective structures. They must ensure that all their members undergo formal civic education training at the appropriate stages of development, that the ethos of the CEP is infused into all aspects of their members' service, that all their managers support the guiding principles and that an appropriate monitoring system is put in place.

- The Technical Committee must undertake the necessary research, prepare a curriculum and develop a plan for implementing it.

- SANAI must participate in the research and design of the curriculum and incorporate it into all basic, intermediate and advanced courses at the Academy.

The Charter states that the public has an interest in an intelligence community that is well grounded in an appreciation of the Constitution and the rule of law. The Minister and the Steering Committee will therefore endeavour to provide platforms for the public to make input into the curriculum by periodically holding public discussions and debates on relevant topics.

The JSCI will receive regular reports on the CEP from the Minister and may make recommendations to the Minister.

The Charter lists the activities of the CEP as follows: the design and implementation of the curriculum; hosting debates on intelligence and the

Constitution within the intelligence community; engaging with foreign services about their experience of intelligence in a democracy; undertaking research on the conduct of intelligence in a democracy; and hosting public debates. The curriculum was to have been completed by April 2007.[17]

The curriculum must cover the following topics:

- security and intelligence in a democracy;
- the importance of values and ethics for intelligence officers;
- the benefits of the CEP to the intelligence services and members;
- the rule of law, the Bill of Rights, the supremacy of the Constitution and the implications for the services;
- the legislation governing the services;
- the main features of a democracy, including subordination and accountability to the political authority;
- the power of the services and the potential for abuse of power;
- non-partisanship and non-interference in legitimate political activities;
- the proper balance between secrecy and openness;
- the proper balance between intrusive methods of investigation and respect for civil liberties;
- the elements of a professional work ethic and the personal responsibility of the intelligence officer;
- a culture of openness, debate and critical thinking; and
- eliminating racism and sexism and building cohesion, trust and camaraderie.

*11.4.2 CEP activities*[18]

In 2007 all formative courses for new recruits at SANAI included the core themes of the CEP, and issues pertaining to legality and ethical conduct were being integrated into all functional training at the Academy.

[17] Ministry of Intelligence Services, 'Civic Education Charter', op cit, pg. 5.
[18] The information in this Section is drawn mainly from SANAI, 'Progress Report Civic Education Curriculum', undated, prepared for the Commission; and correspondence to the Commission from SANAI, 22 April 2008.

Internal debates on contentious ethical topics have been organised in the civilian intelligence community and a lecture series with external speakers has been planned for 2008. The debates and lectures are intended to stimulate critical thinking and expose intelligence officers to different perspectives on the topics that form part of the curriculum.

SANAI is preparing two three-day workshops that will be run in all the civilian intelligence organisations. The workshops will cover the role of intelligence in a democracy; the legal parameters in which intelligence operates; awareness of the power of the intelligence services and the potential for abuse of power; the ethics and civic responsibility underpinning intelligence activities; and the dilemmas of intelligence work in the 21st century. SANAI will train facilitators from each of the intelligence organisations, and the heads of the organisations must ensure that all their members attend the workshops.

There is not yet much activity in the intelligence organisations other than SANAI. When we asked these organisations for progress reports on civic education, NIA told us that we should direct our inquiry to the Ministry;[19] SASS said that all new members are advised of their civic responsibilities and that the Service would prioritise the implementation of the Charter once the curriculum had been approved and facilitators had been trained by SANAI;[20] and NICOC replied that it would implement the roll-out plan for the curriculum as soon as this was ratified by the Steering Committee.[21]

It appears that the Steering Committee and the Technical Committee are not meeting regularly and that the bulk of the CEP work is being undertaken by SANAI. The two committees were set up by the Minister to ensure the full participation and buy-in of all the civilian intelligence entities and it is essential that the committees fulfil their designated responsibilities.

[19] Letter to the Commission from the Director-General of NIA, 14 April 2008.
[20] Letter to the Commission from the Director-General of SASS, 10 December 2007.
[21] Letter to the Commission from the Co-ordinator of Intelligence, 3 December 2007.

## 11.5 Inspector-General's Perspective

### *11.5.1 Submission of the Inspector-General*

In the assessment of the Inspector-General of Intelligence, since 1994 systems of accountability in the intelligence community have improved, transparency has increased and institutional reform has taken place on the basis of the post-apartheid intelligence legislation. However, "certain transgressions and less than satisfactory transformation… have continued to shadow the intelligence community".[22]

With respect to the organisational culture of the intelligence services, the Inspector-General has highlighted a number of issues that have an adverse effect on the rights of members and the morale of staff as a whole and might consequently impair the efficacy of control systems.[23]

The problematic issues include the following:

- There have been incidents of abuse of authority resulting in unfairness, perceived victimisation and unfair labour practice.

- The labour rights that are provided for in section 23 of the Constitution are limited in the case of members of the intelligence services. This is understandable but the limitations have not occurred in terms of law of general application as required by the Constitution.

- There is no independent dispute resolution mechanism in the intelligence organisations. If a member's dispute with management is not resolved, the only remedy is to approach a court of law. The independent appeals board

[22] Office of the Inspector-General of Intelligence, 'Submission to the Ministerial Review Commission. The Concept of the Control of the Civilian Intelligence Services', presented to the Commission on 29 January 2007, pg. 21.
[23] Ibid, pp. 23-25.

provided for in the ministerial regulations of 2003 has not yet been established.

- The policies and procedures that govern conditions of service and human resource processes are not adhered to consistently. The lack of due process has a negative impact on staff morale.

- There is a need to promote a culture of respect for the rule of law. Manifestly illegal instructions might be obeyed by rank-and-file members because of fear, threats and concerns about losing their jobs. The members do not have adequate recourse and remedies in these situations.

- There are pockets of lingering mistrust arising from the integration of the statutory and non-statutory intelligence services in the mid-1990s. This leads to the formal chain of command being bypassed and to the exclusion of individuals from discussion on matters for which they are responsible and accountable.

*11.5.2 Comment*

In its submission to the Commission, the Staff Council in the Intelligence Services, which is an employee representative body, complained that the civilian intelligence organisations are excluded from the labour legislation and that the members of these organisations do not enjoy the labour rights enshrined in section 23 of the Constitution.[24] Section 23 provides, among other things, for the rights to fair labour practices, to form and join a trade union and to engage in collective bargaining.

[24] Staff Council in the Intelligence Services, submission to the Commission, August 2007.

In the opinion of the State Law Adviser, the limitation of section 23 rights in the intelligence organisations is unconstitutional.[25] This opinion is informed by the Constitutional Court's ruling on the limitation of trade union rights in the SANDF; the Court held that the SANDF could place reasonable limitations on the trade union activities of military personnel but could not deny completely their right to join a trade union.[26]

A detailed examination of employer-employee relations and human resource issues lies outside our mandate. However, our terms of reference focus on the imperative of ensuring full compliance and alignment with the Constitution. We therefore recommend that the Minister, in consultation with the members of the intelligence organisations, finds an arrangement that addresses the labour rights of members to the satisfaction of all the parties.

In Section 5.5 we argued that the Inspector-General should not be used to resolve human resource grievances and disputes, as happens from time to time. The Minister should request the Intelligence Services Council on Conditions of Service to prepare proposals on improving the mechanisms for addressing grievances and disputes.

In the following Section we explore further the problems of illegal instructions and the absence of complete respect for the rule of law.

### 11.6 Bending the Rules

Some senior intelligence officers believe that it is legitimate to 'bend the rules' in order to deal with serious security threats. This was the position taken by the Task Team on the Review of Intelligence-Related Legislation, Regulation

[25] Letter from the Office of the Chief State Law Adviser to the Chairperson of the Staff Council in the Intelligence Services, 11 January 2004.
[26] *South African National Defence Union v Minister of Defence* 1999 (4) SA 469 (CC).

and Policies (hereafter the "Task Team") in its final report to the Minister for Intelligence Services.[27]

The Task Team's position is unconstitutional, flouts the rule of law and undermines efforts to develop an institutional culture of respect for the law. We address the argument at some length because of its intrinsic dangers and because it goes to the heart of the Commission's terms of reference.

*11.6.1 The position of the Task Team*

In its final report to the Minister, the Task Team made proposals to strengthen the operational policies of the intelligence services (Chapter 9). It then made the valid point that the integrity of the system of authorising operations depends on the integrity and professionalism of the officials who have decision-making responsibility. The requisite standards of professionalism had not been attained, however. In the wake of the intelligence crisis of 2005/6, the Task Team expressed concern that the institutional culture of the services was not yet sufficiently respectful of democracy and the law:

> The majority of the members of our services come from the background of the struggle against or in defence of apartheid and the Cold War era. The experiences and training of this era inculcated a culture of non-accountability of intelligence and security services, and a no-holds-barred approach to intelligence operations.
>
> While it is true that eleven years of a democratic intelligence dispensation have seen significant transformatory inroads into this culture, it is obviously not completely gone. Perhaps it can only be

[27] Task Team on the Review of Intelligence-Related Legislation, Regulation and Policies, 'Final Report of the Task Team on the Review of Intelligence-Related Legislation, Regulation and Policies', April 2006, pp. 58-59.

> completely gone when a totally new generation of intelligence officers has worked their way into the system.[28]

Given these problems, the Task Team supported the introduction of a civic education programme for the intelligence services but it warned that the programme should recognise that the services may sometimes have to bend the rules in order to deal with terrorist and other security threats.

> Any effective programme to ensure compliance with prescripts in the conduct of intelligence operations must include an element of culture-change – of instilling an understanding of constitutionality, legality, accountability and of integrity and professionalism.
>
> But a word of caution is necessary. Prescripts are a necessary part of ensuring the democratic transformation of our intelligence services. So is the inculcation of a new culture of constitutionality and accountability. But intelligence remains intelligence. The state gives powers and mandate[s] to the intelligence services to employ secret means in order to protect the very Constitution that governs the conduct of intelligence itself.
>
> Over-regulation and over-accountability of the intelligence services have the potential to render the intelligence services unable to carry out their noble duty to protect constitutional democracy.
>
> Also, in the hard reality of intelligence operations – when the threats and the targets are clear – it is sometimes impossible to do things by the book. When operating against terrorist threats or organised crime or other clear threats and targets, it is sometimes necessary to 'bend the rules' in order to ensure that the threat is adequately dealt with. This is an operational reality in order to ensure that the real 'nasties' do not get away with their 'nastiness'.

[28] Task Team, 'Final Report', op cit, pg. 59.

> Therefore, while a programme of cultural transformation cannot obviously make this point, it must at least recognise this reality. Ultimately, the 'bending of the rules' depends extensively on the integrity of those who may have to take such decisions and on methods to ensure that this is not abused. The danger lies in a programme of cultural transformation that inculcates the right of any intelligence officer to disobey a manifestly illegal order. This right must be balanced against the need for discipline and command in the conduct of operations, especially when tackling the 'big threats'.[29]

The Task Team's use of the term 'bending the rules' is misleading since there is no middle ground between obeying and breaking rules. The term is clearly intended to be a euphemism for breaking the rules. The passages quoted above would make no sense if 'bending the rules' were in any way compatible with obeying the rules.

*11.6.2 The Constitution*

The Constitution prohibits the breaking of rules. The following provisions are categorical in this regard:

- Every citizen is protected by law.[30]

- Our democratic state is founded on the supremacy of the Constitution and the rule of law.[31]

- The Constitution is the supreme law of the Republic. Law or conduct inconsistent with it is invalid, and the obligations imposed on it must be fulfilled.[32]

[29] Task Team, 'Final Report', op cit, pg. 59.
[30] Preamble to the Constitution.
[31] Section 1(c) of the Constitution.

- The Bill of Rights applies to all law, and binds the legislature, the executive, the judiciary and all organs of state.[33]

The Constitution does not exempt the security services from these provisions. On the contrary, it stresses that the security services must obey the law:

- National security must be pursued in compliance with the law.[34]

- National security is subject to the authority of Parliament and the national executive.[35]

- The security services must act, and must teach and require their members to act, in accordance with the Constitution and the law.[36]

- No member of any security service may obey a manifestly illegal order.[37]

Given these provisions, the Task Team's position on bending the rules is unconstitutional.

*11.6.3 The rule of law*

It is impermissible and untenable for a government department in a democratic country to adopt a position that is incontrovertibly illegal and it is even less tolerable for a department to adopt a policy position that permits illegality.

The rule of law is a fundamental tenet of governance that distinguishes a democratic state from an undemocratic state. It means that the country is

[32] Section 2 of the Constitution.
[33] Section 8(1) of the Constitution.
[34] Section 198(c) of the Constitution.
[35] Section 198(d) of the Constitution.
[36] Section 199(5) of the Constitution.
[37] Section 199(6) of the Constitution.

governed by law and not by fiat, that all persons and organisations, regardless of their status, position, power and function, are bound by duly enacted laws and that no person or organisation is above the law or beyond the reach of the law. By definition, there are no legitimate exceptions to the rule of law.

The rule of law is not a philosophical abstraction, divorced from the real world of blood and guts and nastiness. It is a product of bloody struggles against tyranny throughout the ages. The fact that it constrains the state's freedom of action is not accidental. The rule of law is deliberately intended to shackle rulers in order to prevent them from posing a threat to the freedom and security of citizens. In South Africa the motivation for the constitutional emphasis on the rule of law is heightened by our experience of living in a society where the security services acted outside the realm of law.

In a democracy, all laws have to be approved by public representatives who are elected by citizens. A policy that allowed intelligence officers or any other category of state employee to break the rules would subvert the will of the electorate, negate the authority of Parliament and permit unelected officials to override decisions made by our elected representatives. For all these reasons, the policy would be antithetical to democracy.

The Task Team suggests that there is a danger in a programme of cultural transformation that "inculcates the right of any intelligence officer to disobey a manifestly illegal order. This right must be balanced against the need for discipline and command in the conduct of operations, especially when tackling the 'big threats'".[38] In our view, this perspective reflects several misunderstandings.

First, the Constitution states that members of the security services have a duty, not a right, to disobey a manifestly illegal order.[39] Far from being a

[38] Task Team, 'Final Report', op cit, pg. 59.
[39] Section 199(6) of the Constitution.

danger, this duty helps to protect society and individuals against criminality and repression by the security services. It emerged from the experience of Nazi Germany and the unacceptable defence of accused persons at the Nuremberg trials that they were 'only following orders'.

Second, the duty to disobey illegal orders and the need for discipline and command do not require 'balancing' as they might if they were on opposite sides of an equation. They are on the same side of the equation, which is the side of the rule of law. The authority to exercise command, the power to issue an order, the duty to obey a lawful order and the obligation to disobey an unlawful instruction are all aspects of the rule of law and derive from the Constitution and legislation.

*11.6.4 The dangers of bending the rules*

The Task Team does not suggest that the rules can be bent lightly or routinely. Its position is intended to apply to exceptional situations where the security threat is severe and bending the rules is necessary "in order to ensure that the real 'nasties' do not get away with their 'nastiness'".[40] In taking this position, however, the Task Team fails to appreciate the grave danger that the exceptions will become the norm and preclude the emergence of an institutional culture of respect for the law.

The Task Team states that "the bending of the rules depends extensively on the integrity of those who may have to take such decisions and on methods to ensure that this is not abused".[41] This is not reassuring. The Task Team does not specify the methods that will prevent abuse and there is no guarantee that every official will behave with integrity. The intelligence crisis of 2005/6 demonstrated in a dramatic fashion that some officials do lack integrity and that the political dangers of bending the rules are severe.

[40] Task Team, 'Final Report', op cit, pg. 59.
[41] Ibid.

One of the statutory mechanisms for detecting and preventing abuse in the intelligence community is the Office of the Inspector-General of Intelligence (OIGI). A policy that allowed the rules to be broken, even if only in exceptional circumstances, would fatally compromise this Office and its mandate and staff. The OIGI would either have to be kept ignorant of rule-breaking or have to condone it, and the Inspector-General's reports would then unwittingly or knowingly deceive the Minister and the JSCI. This would be a constitutional and political catastrophe.

Finally, if members of the intelligence services not only broke the rules but were allowed to break the rules, then it would not be possible to build and maintain within these services a culture of respect for the law. It would be impossible to inculcate "a new culture of constitutionality and accountability", which the Task Team itself believes to be necessary.

*11.6.5 Reorienting the debate*

Members of the intelligence services have a keen sense of the security threats that confront the state and society. They might believe that their legal powers and other features of the law are too weak to stop people with the desire and means to inflict substantial harm on the country. They might therefore favour the breaking of rules in extreme cases. We have argued that this position is illegitimate. As the Minister for Intelligence Services has put it, the intelligence community "must accept the fundamental principle of legality. We do not stand above the law. We are not exempt from the law. We are unequivocally and emphatically bound by the law and the Bill of Rights".[42]

If the intelligence organisations feel that their powers are inadequate or that the law is too constraining, then they have to convince the Executive of the necessity to amend the law. The Executive, in turn, would have to persuade

[42] Minister Ronnie Kasrils, 'Five Principles of Intelligence Service Professionalism', September 2005.

Parliament of this necessity and the resultant amendments would have to be consistent with the Constitution.

Strict adherence to the rules is in the interests of the intelligence services themselves. Aside from the damage done to the reputation and morale of the services when senior officials are caught breaking the law, intelligence officers will not function effectively if they are uncertain about the parameters of permissible conduct. Some might act without restraint and others with excessive caution, neither of which approach will yield optimal results. In the aftermath of the intelligence crisis, members of NIA were reluctant to take any action for fear of getting into trouble.[43] This situation would not arise if both the rules and the imperative of obeying the rules were clearly understood.

### 11.7 The Absence of Adequate Legal Expertise

Elsewhere in this Report we express our concern about departmental policies and memoranda that mistakenly ignore or misinterpret provisions of the Constitution and legislation. For example, there are erroneous views that the right to privacy does not apply to foreign nationals in South Africa (Section 8.8), and that the prohibition on intercepting communication without judicial authorisation does not apply to the NCC's signals operations (Section 8.5).

These errors, which appear in policies that emphasise the importance of complying with the law, have the very serious effect of rendering certain intelligence activities unlawful and/or unconstitutional. Full compliance with the law is obviously unlikely if operational directives do not interpret the law correctly.

One of the underlying problems is that the legal advisers in the intelligence community fail to take proper account of Constitutional Court judgements when they draft or vet internal policies. It is not sufficient to look only at the

[43] Meeting with the NICOC Co-ordinator, 10 May 2007.

Bill of Rights. The legal advisers must also consider the interpretive framework and corpus of law that has emerged from the Constitutional Court's interpretation of these rights and its findings on legislation that limits rights.

On the basis of our review of departmental policies and our exchanges with a number of legal advisers in the civilian intelligence community, our conclusion is that the community does not have adequate legal and constitutional expertise.

In addition to this general conclusion, on the basis of our review we are concerned about the absence of familiarity with those aspects of international law that have a bearing on intelligence operations. In his submission to the Commission, the Inspector-General identified international law as an area that required attention. He recommended that efforts be made to ensure that domestic intelligence legislation is aligned to international law and that intelligence officers act in accordance with international law and international agreements that bind South Africa.[44]

As noted previously, 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, including customary international law and international agreements binding on South Africa.[45] It is therefore necessary for the relevant aspects of international law to be included in the civic education curricula.

### 11.8 Recommendations

The heads of the intelligence organisations must have a zero-tolerance approach to misconduct and illegality by their members, and the Minister for

[44] Office of the Inspector-General of Intelligence, 'Submission to the Ministerial Review Commission', op cit, pg. 21.
[45] Section 199(5) of the Constitution.

Intelligence Services, the Inspector-General of Intelligence and the JSCI must ensure adherence to this policy.

The Minister should ensure that the civic education Steering Committee and Technical Committee meet regularly and submit reports to him or her.

The heads of the intelligence organisations should set up the required monitoring systems to assess their institutional culture and the impact of the civic education programme, and should submit bi-annual reports to the Minister on the results of the monitoring.

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.

In consultation with the members of the civilian intelligence organisations, the Minister should find an arrangement that addresses the labour rights of members to the satisfaction of all the parties.

The Minister should request the Intelligence Services Council on Conditions of Service to prepare proposals on improving the mechanisms for addressing grievances and disputes in the intelligence organisations. The Minister should also ensure that the independent appeals board provided for in the 2003 ministerial regulations is set up immediately.

The Minister and the heads of the services should take steps to enhance the quality of legal advice in the intelligence community. They should send their legal staff on training and refresher courses; submit draft operational policies to the Inspector-General and external experts for comment; and consider the option of making high-level appointments of legal experts.

The Minister should request the Inspector-General or SANAI to do a survey of international law that has a bearing on the operations of the intelligence organisations, indicate the implications for these operations and propose any amendments to domestic laws and policies that are necessary.

The Technical Committee of the Civic Education Programme should include the relevant aspects of international law in the civic education curricula.

# CHAPTER 12: TRANSPARENCY, SECRECY AND PROVISION OF INFORMATION

## 12.1 Introduction

This Chapter deals with the vexed issue of secrecy and openness in relation to the intelligence community, a topic that is characterised by strong competing pressures. On the one hand, certain aspects of the intelligence services and their activities must be kept secret in order to avoid compromising the security of the country, the integrity of operations and the lives of people. On the other hand, secrecy is antithetical to democratic governance, it prevents full accountability and it provides fertile ground for abuse of power, illegality and a culture of impunity.

Given these competing pressures, many governmental and non-governmental publications on intelligence assert that 'a reasonable balance must be struck between secrecy and transparency'. This formulation is too abstract and non-committal to be of any value. In the South African context, moreover, it fails to recognise that there is a constitutional presumption in favour of transparency and access to information. Secrecy must consequently 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.

We believe that the intelligence organisations have not yet shed sufficiently the apartheid-era security obsession with secrecy. The emphasis of these organisations is on secrecy with some exceptions when it should be on openness with some exceptions. In this Chapter we make concrete recommendations on enhancing the transparency of the intelligence

community in ways that would not undermine the intelligence services or the security of the country.[1]

The Chapter covers the following topics:

- The constitutional and governance principles on transparency and access to information and the implications of these principles for the intelligence services (Section 12.2).

- Specific areas of information about intelligence and the intelligence services that are currently secret but that should be in the public domain (Section 12.3).

- The responsibilities of the intelligence services in terms of the Promotion of Access to Information Act No. 2 of 2000 (hereafter "PAIA") (Section 12.4).

- The Protection of Information Bill, which the Minister for Intelligence Services tabled in March 2008 (Section 12.5).[2]

- Recommendations (Section 12.6).

The Protection of Information Bill will replace the prevailing Protection of Information Act No. 84 of 1982 and the national information security policy known as the Minimum Information Security Standards, approved by Cabinet in 1998. We do not discuss the 1982 legislation, which is a remnant of the apartheid era, because it will be repealed in due course.

[1] In preparing this Chapter we benefited from the submissions we received from the Open Democracy Advice Centre, the South African History Archive Project, the South African Human Rights Commission and the South African National Editors' Forum. These submissions can be viewed at www.intelligence.gov.za/commission.
[2] Protection of Information Bill [B 28-2008].

## 12.2 Constitutional and Governance Principles

### *12.2.1 Constitutional and legal principles*

The point of departure for any discussion on transparency, secrecy and the intelligence services in South Africa must be the Constitution, which is the supreme law and the foundation of our democratic order.

Section 32(1) of the Constitution contains the following emphatic assertion on access to information: everyone has the right of access to a) any information held by the state; and b) any information that is held by another person and that is required for the exercise or protection of any rights. Section 32(2) provides that national legislation must be enacted to give effect to this right. The relevant legislation is PAIA.

PAIA seeks to foster a culture of transparency and accountability in public and private bodies by giving effect to the right of access to information.[3] The Act applies to the exclusion of any provision of other legislation that prohibits or restricts the disclosure of a record of a public or private body and that is materially inconsistent with an object or provision of the Act.[4] Furthermore, any limitation of the right of access to information must be consistent with section 36(1) of the Constitution, which deals with limitations of rights.

In addition to providing for the right of access to information, the Constitution emphasises the principles of transparency, openness and accountability as fundamental tenets of governance.[5] It declares that the founding values of the Constitution include “universal adult suffrage, a national common voters roll, regular elections and a multi-party system of democratic government, to ensure accountability, responsiveness and openness”.[6]

---

[3] Preamble to PAIA.
[4] Section 5 of PAIA.
[5] See, for example, the Preamble and sections 1(d), 36(1), 39(1), 41(1)(c), 59 and 199(8) of the Constitution.
[6] Section 1(d) of the Constitution.

The Constitution does not treat the security services as an exception in this regard. On the contrary, it states expressly that "to give effect to the principles of transparency and accountability, multi-party committees must have oversight of all security services in a manner determined by national legislation or the rules and orders of Parliament".[7]

Constitutional Court judge Mr Justice Sachs has observed that the most notable feature of the constitutional provisions on transparency is the "inseparability of the concepts of democracy and openness".[8] The right of access to information lies at the heart of transparent governance and provides a basis for democratic accountability and an open and free society.

The right of access to information also serves to advance human rights. Parliament enacted PAIA in order to "actively promote a society in which the people of South Africa have effective access to information to enable them to more fully exercise and protect all of their rights".[9] Conversely, restrictions on access to information can undermine human rights. According to PAIA, the previous system of government in South Africa "resulted in a secretive and unresponsive culture in public and private bodies which often led to an abuse of power and human rights violations".[10]

*12.2.2 Implications for the intelligence services*

It is legitimate to protect certain information from disclosure. Such information might relate, for example, to sensitive diplomatic activities, aspects of military, police and intelligence operations, and the private medical and financial records of individuals. Nevertheless, the protection of information must be mindful of the dangers inherent in secrecy, it must be exceptional and not routine, it must be balanced against the public interest in disclosure, it must

[7] Section 199(8) of the Constitution.
[8] *Independent Newspapers (Pty) Ltd v Minister for Intelligence Services and Freedom of Expression Institute*, CCT 38/07 [2008] ZACC 6, para 154.
[9] Preamble to PAIA.
[10] Ibid.

take place according to criteria and rules approved by Parliament, and it must be consistent with the constitutional provisions outlined above.

The secrecy surrounding the intelligence organisations is not consistent with the Constitution. So much critical information about these bodies is confidential that they appear to be exempt from the constitutional imperatives of transparency and access to information. Unlike other government departments, the annual reports, budgets and financial reports of the intelligence services are not tabled in Parliament; the Auditor-General's reports on the services are not presented to Parliament; Cabinet's intelligence priorities are not in the public domain; and ministerial regulations on intelligence are partly or totally secret (Section 12.3). NIA has reinterpreted its mandate three times since 1994 without the results being disclosed to Parliament and the public (Chapter 6).

The high level of secrecy is contrary to the spirit of the Constitution and, as discussed in the following Section, in some instances it is contrary to the letter of the Constitution. The Constitution is binding on all organs of state and the dangers associated with secrecy – lack of accountability, abuse of power, infringements of rights and a culture of impunity – apply to the intelligence organisations no less than to other sectors of the state.

A fundamental reorientation is therefore required. Secrecy should not dominate and engulf the intelligence community but should be confined mainly to those areas where disclosure of information would cause significant harm to the lives of individuals, the intelligence organisations, the state or the country as a whole. The emphasis on secrecy with some exceptions should be replaced by an emphasis on openness with some exceptions.

The justification for secrecy should not rest on the concept of 'national security'. This concept can be interpreted narrowly to mean the security of the state or broadly to encompass human security and the wide range of political, economic, social and environmental dimensions of security. The broad

definition is adopted by the White Paper on Intelligence of 1994 (Chapter 3). If secrecy can be justified on these expansive and inexact grounds, then there is a great danger of excessive and spurious classification of information.

In general, 'national security' provides a compelling basis for openness rather than secrecy. The Constitution proclaims 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".[11] A high level of secrecy is incompatible with this injunction. It seems clear that national security is not something different from fundamental rights and freedoms and is therefore not something that has to be balanced against these rights and freedoms. A constitutional approach to national security embraces rights and freedoms.

We conclude that secrecy should not be based on the concept of 'national security'. Instead, it should be motivated with reference to specified and significant harm that might arise from the disclosure of particular information. Depending on the circumstances, that harm might have to be weighed against a strong public interest in disclosure.[12]

It must be stressed in this regard that the government cannot seek to avoid all possible harm that might arise from the disclosure of sensitive information. Some risk of harm has to be tolerated in a democracy because the dangers posed by secrecy can imperil the democratic order itself.

We are convinced that less secrecy and greater provision of information about the intelligence services would be of benefit to the services themselves.

---

[11] Section 198(a) of the Constitution.

[12] In *Independent Newspapers v Minister for Intelligence Services*, op cit, Independent Newspapers sought an order to compel public disclosure of restricted portions of the record of judicial proceedings involving NIA. It based its application on the right to open justice. The Minister objected to the disclosure on grounds of national security. The majority of the Court ordered the release of some of the material since there was no valid national security basis for non-disclosure but held that other information, covering relations with foreign intelligence services, the chain of command within NIA and the identity of NIA operatives, must remain restricted. A minority judgement held that it was in the public interest to release all the material, excluding the names of certain operatives.

A system of over-classifying information lacks credibility, it is difficult to maintain and enforce, and it is administratively costly and inefficient. Too much time and effort are devoted to classifying and protecting innocuous information, potentially at the expense of safeguarding genuinely sensitive information.

In addition, excessive secrecy gives rise to suspicion and fear of the intelligence organisations and this reduces public support for them. In a democracy, unlike a police state, intelligence agencies must rely on public co-operation rather than coercion to be successful. The provision of greater information about the intelligence services would raise their profile in a positive way, reduce the apprehension and fears induced by secrecy, improve co-operation with the services and thereby enhance their effectiveness.

This is especially important in the case of NIA since it is the domestic intelligence service. NIA wants to become "a people's intelligence organisation that visibly illustrates that it contributes to protect the Constitution and that it serves and defends the South African community".[13] The Agency believes that the concept of a people's intelligence organisation raises the need for it to build relationships within the community, win the trust and acceptance of the South African people and gain their assistance in gathering intelligence.[14] Needless to say, this vision is not attainable if NIA remains hidden behind a cloak of secrecy.

The following Section seeks to make more concrete the constitutional and governance principles discussed above. It identifies areas in which a greater amount of information about the intelligence services and their work should be disclosed.

[13] National Intelligence Agency, 'NIA's Mandate and Operational Philosophy', Operational Directive OD.01, 2003, para 4.5.
[14] Ibid, paras 4.5.1-4.5.3.

## 12.3 Greater Provision of Information on Intelligence

In this Section we discuss the need for greater disclosure of information in relation to the following areas:

- The National Intelligence Priorities.
- Ministerial regulations.
- Executive policies.
- Annual reports of the intelligence services.
- Intelligence assessments.
- The budgets and financial reports of the intelligence services.
- The Auditor-General's reports on the intelligence services.
- The websites of the intelligence community.

In each of these areas a substantial amount of information that is currently secret could be disclosed, without compromising intelligence operations or security, in order to enhance public understanding, debate, accountability and democratic governance.

### *12.3.1 National Intelligence Priorities*

On an annual basis the Cabinet issues a set of National Intelligence Priorities based on the National Intelligence Estimate prepared by the NICOC. The Cabinet's priorities provide executive direction for the intelligence organisations' focus, priorities and allocation of resources in the forthcoming year.

In a democracy the government's security priorities should not be secret. On the contrary, national security priorities and policies require public support and the Executive should therefore explain and motivate its perspective and decisions.

Parliamentary and public consultation and debate on the National Intelligence Priorities would deepen accountability and democratic decision-making on a

component of national policy that effects profoundly the security of citizens. Security would not be undermined since the priorities do not include the names of individuals and organisations. Instead, the document refers to categories such as 'organised crime' and 'nuclear proliferation'.

*12.3.2 Ministerial regulations*

As discussed in Section 4.7, two sets of ministerial regulations on intelligence have been issued since 1994: the Intelligence Services Regulations of 2003, the bulk of which is secret; and the Regulations on Liaison with Foreign Intelligence Services of 2007, which is totally secret. This secrecy is permissible in terms of the intelligence legislation.[15] However, it is contrary to the Constitution, which states that "proclamations, regulations and other instruments of subordinate legislation must be accessible to the public".[16]

The secrecy of the intelligence regulations is anomalous and undesirable. Regulations are subordinate legislation and must be promulgated in the *Government Gazette* in order to have any legal effect.[17] In a democratic society whose constitutional principles include transparency and access to information, the main rules governing the intelligence services ought to be available to the public. It is inappropriate that innocuous regulations on conditions of service are, as noted by the Constitutional Court, so secret that even a court would not ordinarily have access to them.[18]

A distinction should be drawn between rules that must be confidential for operational reasons and ministerial regulations that must be in the public

[15] The intelligence legislation allows the Minister for Intelligence Services to issue regulations that are not published in the *Government Gazette* but are communicated to the people affected thereby in a manner determined by the Minister. See section 6(4) of the National Strategic Intelligence Act No. 39 of 1994; section 37(5) of the Intelligence Services Act No. 65 of 2002; and section 8(2) of the Intelligence Services Oversight Act No. 40 of 1994.
[16] Section 101(3) of the Constitution.
[17] Correspondence to the Commission from the Office of the Chief State Law Adviser, 3 December 2007.
[18] *Masetlha v President of the Republic of South Africa and Another* 2008 (1) SA 566 (CC), para 229.

domain because they are integral to democratic governance. The regulations should be promulgated in the *Government Gazette*.

The Ministry for Intelligence Services is currently developing a document entitled “Draft Regulations on the Coordination of Intelligence as an Activity: Determination of Intelligence Priorities and Prescripts Relating to the Conduct of Intelligence Services”. This document covers executive direction on target setting; authorisation and management of intrusive operations and investigative techniques; and general principles governing the conduct of intelligence operations. Once finalised, this document should be published by the Minister.

*12.3.3 Executive policies*

In Chapter 4 we note with concern the absence of ministerial policy on many politically significant topics relating, for example, to the mandates, powers and functions of the intelligence services. Policies on these topics tend to be covered in confidential directives issued by the heads of the intelligence services.

There is a strong need for executive policies on intelligence to be in the public domain. This is especially important with respect to intelligence activities that infringe constitutional rights and might lead to interference with lawful political and social processes. In Section 3.8 we identify a number of issues that should be addressed in a new White Paper on Intelligence.

*12.3.4 Annual reports of the intelligence services*

Unlike other government departments, the annual reports of the intelligence services are not published routinely and tabled in Parliament. There is no good reason for this. Security considerations are not at issue since NIA has

published some of its annual reports on its website.[19] This is true also of intelligence services in other democratic countries.[20]

In a democracy the publication of annual reports by government departments and other organs of state is a necessary form of ensuring accountability to Parliament and citizens. The National Treasury adds the further motivation that government departments should be judged by their outputs, and the publication of annual intelligence reports would help taxpayers determine whether they are getting value for money.[21]

*12.3.5 Intelligence assessments*

Intelligence assessments that focus on particular individuals and organisations would in many instances be unsuitable for publication because of the risk of compromising security operations and crime investigations. However, intelligence assessments that deal with categories of security and threats to security can frequently be published without any risk of harm.

By way of example, the Canadian Security Intelligence Service (CSIS) produces a range of material, including background papers on topics like economic security, weapons proliferation and counter-terrorism; a publication called *Commentary* that focuses on issues related to the security of Canada; and a series of research reports based on CSIS reviews of open source information.[22]

The annual reports of the Dutch General Intelligence and Security Service (AIVD) go so far as to include commentaries on radical and terrorist

[19] These reports are not up-to-date, however. At the time of writing (May 2008), the most recent annual report on the NIA website was for the 2003/4 financial year.
[20] The Annual Report of the Dutch intelligence service is a good example of a comprehensive and useful report. See www.fas.org/irp/world/netherlands/aivd2004-eng.pdf.
[21] National Treasury, 'Submission by the National Treasury to the Ministerial Review Commission on Intelligence', 11 December 2007.
[22] See the website of the Canadian Security Intelligence Service at www.csis-scrs.gc.ca.

organisations that are mentioned by name, including organisations that are based in the Netherlands.[23]

The publication of intelligence assessments by NIA and SASS would constitute a useful form of accountability to citizens, who would be able to consider and debate the perspectives of the services. It would also stimulate interest and exchange among academics. Over time, informed public discussion might lead to refinements in the perspectives of the services.

*12.3.6 The budgets and financial reports of the intelligence services*

In Section 10.3 we recorded the National Treasury's concern that the annual budgets and financial reports of the intelligence services are confidential and are not presented to Parliament. Although the documents are reviewed by the JSCI, the services are not directly accountable to Parliament for their budgets and spending. This is contrary to the constitutional provision that national budgets and budgetary processes must promote transparency and accountability.[24]

We have had an opportunity to read some of the budgets and strategic plans submitted to the JSCI by the intelligence services and do not believe that publication of these documents would compromise intelligence operations or the security of the country and its people. We agree with the National Treasury recommendation that the budgets and financial reports of the services be presented openly to Parliament.

*12.3.7 The Auditor-General's reports on the intelligence services*

In Section 10.6 we pointed out that although the Constitution requires the audit reports of the Auditor-General to be submitted to the relevant legislature

[23] See www.fas.org/irp/world/netherlands/aivd2004-eng.pdf.
[24] Section 215(1) of the Constitution.

and be made public,[25] the audit reports on the intelligence services are presented only to the JSCI and are classified as 'confidential' or 'secret'.

We share the Auditor-General's view that the reports should be made public and should be presented to Parliament after they have been discussed by the JSCI.[26] Since the Public Audit Act No. 25 of 2004 allows for sensitive information to be withheld from the reports, there is no justifiable basis for deviating from the Constitution.

*12.3.8 The websites of the intelligence community*

The website of the Ministry for Intelligence Services contains a fair amount of information, including the intelligence legislation, an organogram of the intelligence community, ministerial statements, court judgements that have a bearing on the intelligence services, speeches by the President and the Minister, and parliamentary questions and answers regarding intelligence.[27]

NIA and SASS have websites that contain information about their work and orientation.[28] An impressive document on the SASS website is entitled "South African Secret Service Ten Year Review", and the NIA website contains detailed (though not up-to-date) annual reports. Another positive aspect of the NIA website is the section on the PAIA legislation. NIA offers advice on requesting information in terms of PAIA and provides forms for making such requests.

NICOC and the Office of the Inspector-General of Intelligence (OIGI) do not have websites. This is disappointing and inappropriate given the important functions of these bodies. Since the OIGI plays an ombuds role and investigates complaints against the intelligence services, members of the public should be aware of its responsibilities, activities and results. A website

[25] Section 188(3) of the Constitution.
[26] Meeting with the Auditor-General's staff, 3 December 2007.
[27] The Ministry website can be viewed at www.intelligence.gov.za.
[28] The website of NIA can be viewed at www.nia.gov.za. The website of SASS can be viewed at www.sass.gov.za.

that contained this information would raise public confidence in the Inspector-General and the intelligence services.

## 12.4 The Promotion of Access to Information Act

This Section provides an overview of PAIA and recommends that the intelligence services comply with the legislative requirement for public bodies to produce manuals with specified information.

### *12.4.1 Overview of PAIA*

PAIA is intended to give effect to the constitutional right of access to information held by the state and to information that is held by another person and that is required for the exercise or protection of any rights.[29] The Act provides for exceptions on certain grounds, including privacy, commercial confidentiality and "defence, security and international relations of the Republic".[30] It establishes mechanisms and procedures to enable people to obtain records of public and private bodies as expeditiously as possible.

Section 83 of PAIA states that the South African Human Rights Commission (SAHRC) must monitor compliance with the Act, make recommendations and facilitate the realisation of the right of access to information. The SAHRC is an independent body created by the Constitution in order to promote, protect and monitor human rights in South Africa.[31] As described below, the SAHRC believes there is inadequate compliance with PAIA by the intelligence services.[32]

---

[29] Section 9(a) of PAIA.
[30] Chapter 4 of PAIA.
[31] Section 184 of the Constitution.
[32] South African Human Rights Commission, 'Ministerial Review Commission on Intelligence: Submission by the South African Human Rights Commission', 30 July 2007 (www.intelligence.gov.za/commission).

*12.4.2 PAIA manuals*

Section 14 of PAIA states that every public body must compile and make available to the public a manual that contains specified information (hereafter the "PAIA manual").

Section 14 sets out the details as follows:

> "(1) Within six months after the commencement of this section or the coming into existence of a public body, the information officer of the public body concerned must compile in at least three official languages a manual containing—
> *(a)* a description of its structure and functions;
> *(b)* the postal and street address, phone and fax number and, if available, electronic mail address of the information officer of the body and of every deputy information officer of the body appointed in terms of section 17(1);
> *(c)* a description of the guide [on how to use the Act] referred to in section 10, if available, and how to obtain access to it;
> *(d)* sufficient detail to facilitate a request for access to a record of the body, a description of the subjects on which the body holds records and the categories of records held on each subject;
> *(e)* the latest notice, in terms of section 15(2), if any, regarding the categories of records of the body which are available without a person having to request access in terms of this Act;
> *(f)* a description of the services available to members of the public from the body and how to gain access to those services;
> *(g)* a description of any arrangement or provision for a person… by consultation, making representations or otherwise, to participate in or influence (i) the formulation of policy; or (ii) the exercise of powers or performance of duties by the body;
> *(h)* a description of all remedies available in respect of an act or a failure to act by the body; and
> *(i)* such other information as may be prescribed.
>
> (2) A public body must, if necessary, update and publish its manual referred to in subsection (1) at intervals of not more than one year.

(3) Each manual must be made available as prescribed.

Section 14 thus creates a practical tool that enables members of the public to acquire information from and about government departments and other public bodies and to learn how to go about influencing their policies.

*12.4.3 The exemption of the intelligence services*

Section 14(5) of the Act allows for exemptions from the duty of public bodies to produce a PAIA manual: "For security, administrative or financial reasons, the Minister [of Justice] may, on request or of his or her own accord by notice in the *Gazette*, exempt any public body or category of public bodies from any provision of this section for such period as the Minister thinks fit."

The intelligence services applied for and received such an exemption, which remains in force. The SAHRC believes that the exemption is unnecessary and that the services should be subject to greater scrutiny and openness. Much of the information covered by section 14 is not confidential and would not prejudice the intelligence organisations if it were provided.

We agree with the SAHRC and believe that this issue is a good example of the need to replace the intelligence community's emphasis on secrecy with an emphasis on openness.

## 12.5 Protection of Information Bill

In March 2008 Minister Kasrils published the Protection of Information Bill, which is intended to bring the principles, criteria and procedures governing the protection of state information into alignment with the Constitution.[33] The Bill provides for sensitive information to be classified as 'confidential', 'secret'

[33] Protection of Information Bill [B 28-2008].

or ‘top secret’. The heads of organs of state are responsible for classifying sensitive information held by their respective organisations. The Minister for Intelligence Services has general functions and powers, and NIA must advise, support and monitor organs of state in implementing the legislation.

The Minister invited our comment on an earlier version of the Bill.[34] We also prepared a submission for consideration by the parliamentary committee that reviewed the draft legislation.[35] We present below our main conclusions.

*12.5.1 Main conclusions regarding the Bill*

The Bill recognises the importance of transparency and the free flow of information and has many provisions that aim to prevent inappropriate and excessive restrictions on access to state information. The Bill asserts correctly that access to information is the basis of a transparent, open and democratic society, it is a basic human right, it promotes human dignity, freedom and the achievement of equality and it can also promote safety and security.[36]

The Bill states that the classification of information is an exceptional measure and should be used sparingly.[37] It goes so far as to make it a criminal offence to classify information for the purpose of concealing breaches of law, furthering an unlawful act, hiding inefficiency or administrative error, preventing embarrassment to a person or organisation, or any other purpose ulterior to the Act.[38]

Despite these positive provisions, the Bill has a number of sections that are likely to encourage secrecy. In particular, the Bill’s approach to ‘secrecy in the

[34] Ministerial Review Commission on Intelligence, ‘Memorandum on the Protection of Information Bill’, submitted to the Minister for Intelligence Services, 31 March 2008.
[35] Ministerial Review Commission on Intelligence, ‘Revised Submission on the Protection of Information Bill’, submitted to the Ad Hoc Committee on Intelligence in the National Assembly, 20 July 2008, available at www.intelligence.gov.za/commission.
[36] Section 7 of the Protection of Information Bill.
[37] Section 22(1)(c) of the Protection of Information Bill.
[38] Section 49 of the Protection of Information Bill.

national interest' is reminiscent of apartheid-era laws and is in conflict with the constitutional right of access to information.

The Bill states that "sensitive information is information which must be protected from disclosure in order to prevent the national interest of the Republic from being harmed".[39] It then defines the 'national interest of the Republic' to include "all matters relating to the advancement of the public good" and "all matters relating to the protection and preservation of all things owned or maintained for the public by the State".[40]

So broad a definition of the 'national interest' is bound to lead to a chronic over-classification of information. This would be inconsistent with the Constitution and our democratic dispensation. An underlying premise of the Bill is that "secrecy exists to protect the national interest".[41] This is constitutionally unsound. Since the 'national interest' includes the pursuit of democracy,[42] it is not secrecy but rather transparency and access to information that best protect the national interest.

A second major problem with the Bill is that the guidelines governing the disclosure and non-disclosure of information are extremely complicated and will be very difficult to apply in practice. The officials who classify information must take account of numerous criteria and principles, some of which are in conflict with each other and most of which depend on subjective judgement. We believe that the principles and criteria should be simplified substantially in order to facilitate consistent and sound decision-making by government officials.

Our third major concern is that some of the criteria for classifying information do not indicate a sufficient degree of harm and certainty to justify non-disclosure. For example, state information may be classified as 'confidential' if

[39] Section 14 of the Protection of Information Bill.
[40] Section 15(1) of the Protection of Information Bill.
[41] Section 22(1)(a) of the Protection of Information Bill.
[42] Section 15(2)(b) of the Protection of Information Bill.

"the information is sensitive information, the disclosure of which may be harmful to the security or national interest of the Republic or could prejudice the Republic in its international relations".[43] The notions of 'prejudicing the Republic in its international relations' and 'harming the national interest of the Republic' are overly broad catch-alls. In a democratic society, moreover, some prejudice and harm arising from the disclosure of information has to be tolerated in the greater interests of freedom, accountability and transparent governance.

We recommend that the criteria for classifying information be made more precise, indicating clearly the degree of harm and certainty required for classifying information as 'confidential', 'secret' or 'top secret'.

The fourth major problem is that the Bill gives NIA sole responsibility for advising, supporting and monitoring organs of state in the implementation of the Act. NIA can play a valuable role in this regard because it specialises in protecting sensitive information. Precisely for this reason, however, it is not oriented towards promoting the constitutional right of access to information. We therefore recommend that the Bill also provide for the involvement of the South African Human Rights Commission in the implementation of the Act.

### 12.6 Recommendations

The National Intelligence Priorities approved annually by Cabinet should be subject to parliamentary consultation and debate. The consultation should first be conducted with the JSCI, allowing for a frank but confidential discussion between the Executive and parliamentarians. The document should thereafter be presented to Parliament for open debate involving all members. Information that is extremely sensitive could be withheld from the public document.

[43] Section 20(1)(a) of the Protection of Information Bill.

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

Once the Minister has finalised the "Draft Regulations on the Coordination of Intelligence as an Activity: Determination of Intelligence Priorities and Prescripts Relating to the Conduct of Intelligence Services", he or she should table the document for parliamentary and public comment. Following the consultation, the regulations should be published in the *Government Gazette*.

Executive policy on intelligence and the operations of the intelligence services should be in the public domain.

The intelligence services should publish their annual reports on their websites and the Minister for Intelligence Services should table these reports in Parliament. The intelligence services should also publish periodic assessments of security and threats to security on their websites.

We support the National Treasury proposal that the annual budgets and financial reports of the intelligence services should be presented to Parliament as public documents. The documents should exclude information that, if disclosed, would endanger security or compromise intelligence operations, methods or sources.

We endorse the Auditor-General's recommendation that the audit reports on the intelligence services be presented to Parliament as public documents, subject to the withholding of sensitive information as permitted by law. In addition, the audit reports on the intelligence services for the past five years should be disclosed to Parliament.

NICOC and the Office of the Inspector-General of Intelligence should set up websites that include detailed information about their respective functions and activities.

All the intelligence organisations should have on their websites a section that assists members of the public who want to request information under the PAIA legislation.

The intelligence services should produce the information manuals required by section 14 of PAIA. If there is specific information whose disclosure would cause significant harm, then the intelligence services should apply for an exemption to exclude that information.

**BIBLIOGRAPHY**


Barnett, H., 2006, *Constitutional and Administrative Law*, 6th edition, Oxford: Routledge-Cavendish.

Berkowitz, B. and A. Goodman, 2000, *Best Truth: Intelligence in the Information Age*, New Haven and London: Yale University Press.

*Bernstein and Others v Bester and Others NNO*, 1996 (2) SA 751 (CC).

Born, H. and M. Caparini (eds), 2007, *Democratic Control of Intelligence Services: Containing Rogue Elephants*, Aldershot: Ashgate.

Born, H., P. Fluri and S. Lunn (eds), 2003, *Oversight and Guidance: The Relevance of Parliamentary Oversight of the Security Sector and Its Reform*, Geneva Centre for the Democratic Control of Armed Forces and Nato Parliamentary Assembly.

Born, H., L.K. Johnson and I. Leigh (eds), 2005, *Who's Watching the Spies? Establishing Intelligence Service Accountability*, Washington DC: Potomac Books.

Born, H. and I. Leigh, 2005, *Making Intelligence Accountable: Legal Standards and Best Practice for Oversight of Intelligence Agencies*, Oslo: Parliament of Norway.

Brodeur, J.P., P. Gill and D. Tollborg, 2003, *Democracy, Law and Security: Internal Security Services in Contemporary Europe*, Aldershot: Ashgate.

Bruneau, T.C. and S.C. Boraz (eds), 2007, *Reforming Intelligence: Obstacles to Democratic Control and Effectiveness*, Austin: University of Texas.

Burgess, J.P., 2008, 'Security as Ethics', *Policy Brief* 6/2008, International Peace Research Institute, Oslo.

Buzan, B., 1991, *People, States and Fear: An Agenda for International Security Studies in the Post-Cold War Era*, 2nd edition, New York and London: Harvester Wheatsheaf.

Caparini, M., 2007, 'Controlling and Overseeing Intelligence Services in Democratic States', in H. Born and M. Caparini (eds), *Democratic Control of Intelligence Services: Containing Rogue Elephants*, Aldershot: Ashgate, pp. 3-24.

Cawthra, G. and R. Luckham (eds), 2003, *Governing Insecurity: Democratic Control of Military and Security Establishments in Transitional Societies*, London and New York: Zed.

Davies, P., 2004, 'Intelligence Culture and Intelligence Failure in Britain and the United States', *Cambridge Review of International Affairs*, vol. 17, no. 3, pp. 496-520.

Dombroski, K., 2006, 'Reforming Intelligence: South Africa after Apartheid', *Journal of Democracy*, vol. 17, no. 3, 43-57.

Farson, A.S., D. Stafford and W. Wark (eds), 1991, *Security and Intelligence in a Changing World*, London: Frank Cass.

Gill, P., 2007, 'Democratic and Parliamentary Accountability of Intelligence Services after 9/11', in H. Born and M. Caparini (eds), *Democratic Control of Intelligence Services: Containing Rogue Elephants*, Aldershot: Ashgate, pp. 195-214.

Gill, P., 1994, *Policing Politics: Security Intelligence and the Liberal Democratic State*, London: Frank Cass.

Godson, R. (ed), 1989, *Intelligence Requirements for the 1990s: Collection, Analysis, Counterintelligence and Covert Action*, Lexington: Lexington Books.

Godson, R. (ed), 1979-1985, *Intelligence Requirements for the 1980s*, 7 volumes, Washington DC: National Strategy Information Centre.

Hannah, G., K. O'Brien and A. Rathmell, 2005, 'Intelligence and Security Legislation for Security Sector Reform', *Technical Report* TR-288-SSDAT, Rand Europe.

Hutton (Lord), 2004, *Report of the Inquiry into the Circumstances Surrounding the Death of Dr. David Kelly*, United Kingdom, 28 January (www.the-hutton-inquiry.org.uk).

Hutton, L., 2007, 'Looking Beneath the Cloak: An Analysis of Intelligence Governance in South Africa', *ISS Paper* no. 154, Institute for Security Studies, November.

*Independent Newspapers (Pty) Ltd v Minister for Intelligence Services* CCT 38/07 [2008] ZACC 6.

Institute for Security Studies, 2007, 'Submission on Intelligence Governance and Oversight in South Africa to the Ministerial Review Commission on Intelligence', 11 May (www.intelligence.gov.za/commission).

*Investigating Directorate: Serious Economic Offences and Others v Hyundai Motor Distributors (Pty) Ltd and Others: In Re Hyundai Motor Distributors (Pty) Ltd and Others v Smit NO and Others*, 2001 (1) SA 545 (CC).

Johannesburg Principles on National Security, Freedom of Expression and Access to Information, 1996, Article 19, (www.article19.org/pdfs/standards/joburgprinciples.pdf).

Joint Standing Committee on Intelligence, 2006, 'Special Report of the Joint Standing Committee on Intelligence – On the Reports of the Inspector-General of Intelligence', report to the National Assembly, 15 August.

Joint Standing Committee on Intelligence, 'Annual Report of the Joint Standing Committee on Intelligence for 2004/5', Parliament of the Republic of South Africa.

Joint Standing Committee on Intelligence, 'Annual Report of the Joint Standing Committee on Intelligence for the Reporting Period Ended 31 March 2004', Parliament of the Republic of South Africa.

Joint Standing Committee on Intelligence, 'Annual Report, 1 April 2002 – 31 March 2003', Parliament of the Republic of South Africa.

Kasrils, R., 2008, 'To Spy or Not to Spy? Intelligence and Democracy in South Africa', Institute for Security Studies Public Dialogue Series (www.intelligence.gov.za).

Kasrils, R., 2008, 'To Spy or Not to Spy?', address by the Minister for Intelligence Services on the occasion of the intelligence services budget debate, National Assembly, 23 May (www.intelligence.gov.za).

Kasrils, R., 2007, 'Emulating the Skills of the African Spies of Yesteryear', address by the Minister for Intelligence Services on the occasion of the intelligence services budget debate, National Assembly, 25 May (www.intelligence.gov.za).

Kasrils, R., 2006, 'Debate on the Report of the Joint Standing Committee on Intelligence (JSCI) in Response to the Investigation by the Inspector

General', address in the National Assembly, 21 September (www.intelligence.gov.za).

Kasrils, R., 2006, 'South African Intelligence Services Meeting the Challenges for the 21st Century: The Importance of Oversight', address by the Minister for Intelligence Services on the occasion of the intelligence services budget debate, National Assembly, 1 June (www.intelligence.gov.za).

Kasrils, R., 2005, 'South African Intelligence Services Meeting the Challenges of the 21st Century: Spies, Soothsayers, Sangomas', address by the Minister for Intelligence Services on the occasion of the intelligence services budget debate, National Assembly, 17 May (www.intelligence.gov.za).

*Lawyers for Human Rights v Minister of Home Affairs* 2004 (4) SA 125 (CC).

Leigh, I., 2007, 'The UK's Intelligence and Security Committee', in H. Born and M. Caparini (eds), *Democratic Control of Intelligence Services: Containing Rogue Elephants*, Aldershot: Ashgate, pp. 177-194.

Leigh, I., 2005, 'More Closely Watching the Spies: Three Decades of Experiences', in H. Born, L.K. Johnson and I. Leigh (eds), *Who's Watching the Spies? Establishing Intelligence Service Accountability*, Washington D.C.: Potomac Books, pp. 3-11.

Leigh, I. and L. Lustgarten, 1994, *In from the Cold: National Security and Parliamentary Democracy*, Oxford: Clarendon Press.

*Masetlha v President of the Republic of South Africa and Another*, 2008 (1) SA 566 (CC).

Mbeki, T., 2005, 'Address of the President of South Africa, Thabo Mbeki, at the Intelligence Services Day 10th Anniversary Awards Ceremony and Inauguration of the Wall and Garden of Remembrance', Musanda, 24 November (www.dfa.gov.za/docs/speeches/2005/mbek1125.htm).

Ministerial Review Commission on Intelligence, 2008, 'Revised Submission on the Protection of Information Bill', submitted to the Ad Hoc Committee on Intelligence in the National Assembly, 20 July (www.intelligence.gov.za/commission).

Ministerial Review Commission on Intelligence, 2008, 'Submission on the National Strategic Intelligence Amendment Bill [B 38-2008]', submitted to the Ad Hoc Committee on Intelligence in the National Assembly, 10 July (www.intelligence.gov.za/commission).

*Mistry v Interim Medical and Dental Council of South Africa* 1998 (4) SA 1127 (CC).

*Mohamed v President of the Republic of South Africa* 2001 (3) SA 893 (CC).

O'Brien, K., 2005, 'Controlling the Hydra: A Historical Analysis of South African Intelligence Accountability', in H. Born, L.K. Johnson and I. Leigh (eds), *Who's Watching the Spies? Establishing Intelligence Service Accountability*, Washington D.C.: Potomac Books, pp. 199-222.

OECD DAC, 2005, *Security System Reform and Governance*, DAC Guidelines and Reference Series, Paris: OECD (www.oecd.org/dataoecd/8/39/31785288.pdf).

Office of the Inspector-General of Intelligence, 2006, 'Executive Summary of the Final Report on the Findings of an Investigation into the Legality of the Surveillance Operations Carried out by the NIA on Mr S Macozoma. Extended Terms of Reference Report on the Authenticity of the Allegedly Intercepted E-Mails', media briefing, 23 March (www.intelligence.gov.za/OversightControl/IG%20Exec%20Summary%2023%20Mar%2006.doc).

Owen, T., 2004, 'Human Security – Conflict, Critique and Consensus: Colloquium Remarks and a Proposal for a Threshold-Based Definition', *Security Dialogue*, vol. 35, no. 3, pp. 373-387.

*Park-Ross and Another v Director: Office for Serious Economic Offences*, 1995 (2) SA 148 (C).

*Powell NO v Van der Merwe NO* 2005 (5) SA 62 (SCA).

Sanders, J., 2006, *Apartheid's Friends: The Rise and Fall of South Africa's Secret Service*, London: John Murray.

Schnabel, A. and H. Ehrhart (eds), 2006, *Security Sector Reform and Post-Conflict Peacebuilding*, United Nations University Press.

South African History Archive, 2007, 'Call for Submission to the Ministerial Review Commission on Intelligence', 4 May (www.intelligence.gov.za/commission).

South African Human Rights Commission, 2007, 'Ministerial Review Commission on Intelligence: Submission by South African Human Rights Commission', 30 July (www.intelligence.gov.za/commission).

*South African National Defence Union v Minister of Defence* 1999 (4) SA 469 (CC).

Weller, G.R., 1996/7, 'Comparing Western Inspectors General of Intelligence and Security, *International Journal of Intelligence and Counterintelligence*, vol. 9, no. 4, pp. 383-406.

White Paper on Intelligence, 1994, Republic of South Africa (www.intelligence.gov.za/Legislation/white_paper_on_intelligence.htm)

White Paper on National Defence for the Republic of South Africa, 1996.

Wilson, P., 2005, 'The Contribution of Intelligence Services to Security Sector Reform', *Conflict, Security and Development*, vol. 5, no. 1, pp. 87-107.

Wolfers, A. 1952, '"National Security" as an Ambiguous Symbol', *Political Science Quarterly*, vol. 67, no. 4, pp. 481-502.

MINISTRY
INTELLIGENCE SERVICES
REPUBLIC OF SOUTH AFRICA

PO Box 51278, Waterfront, 8002, CAPE TOWN, 18th floor, 120 Plein Street, Parliament, CAPE TOWN Tel: (021) 401 1800 Fax: (021) 461 4644
PO Box 1037, Menlyn, 0077, PRETORIA, Ruth First Building, Bogare, Cnr Atterbury Road & Lois Avenue, MENLYN Tel: (012) 367 0700 Fax: (012) 367 0749
www.intelligence.gov.za

# MINISTERIAL REVIEW COMMISSION ON INTELLIGENCE

## Establishment of Commission

The Ministerial Review Commission on Intelligence is hereby established by the Minister for Intelligence Services.

## Composition of the Commission

Mr J Matthews
Dr F Ginwala
Mr L Nathan

## Terms of Reference

*Aim of the review*

The aim of the review is 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 shall cover the following structures:

a. National intelligence Agency (NIA);
b. South African Secret Service (SASS);
c. National Intelligence Coordinating Committee (NICOC);
d. National Communications Centre (NCC);
e. Electronic Communications Security (Pty) Ltd (COMSEC); and
f. Office for Interception Centres (OIC).

*Independence of the Commission*

The Commission shall be independent. No person or body may do anything to undermine its independence or seek to influence the Commissioners in an improper manner.

*Focus of the review*

The focus of the review shall include the following topics in so far as they relate to the aim of the Commission:

- Executive control of the intelligence services;
- Control mechanisms relating to intelligence services' operations;
- Control over intrusive methods of investigation;
- The spheres of activity currently referred to as political and economic intelligence;
- Political non-partisanship of the intelligence services;
- The balance between secrecy and transparency; and
- Controls over the funding of covert operations.

*Methods of inquiry*

In order to achieve its aim, the Commission may undertake the following methods of inquiry:

- Review the legislation, regulations and policies governing the intelligence services;
- Review the reports of the Legislative Task Team;
- Review the directives on intrusive methods of collection and directives on the conduct of surveillance;
- Consider any other reports submitted to the Commission by the Minister;
- Invite written or oral submissions/presentations from interested parties;
- Invite submissions from the intelligence services;
- Hold public consultations at which members of the public and interested parties can make submissions to the Commission;
- Undertake comparative study of good practice in the governance of intelligence services in other countries; and
- Any other methods that it deems appropriate.

*Report to the Minister*

On completion of its review, the Commission shall submit a public report to the Minister. The emphasis of the report will be on practical recommendations for strengthening control and regulation of the operations of the civilian intelligence services.

The first phase of the report will be completed by 30 June 2007 and the final report will be submitted by the end of 2007.

**APPENDIX B**

## SUBMISSIONS RECEIVED BY THE COMMISSION

### Governmental Bodies

Auditor-General
Ministry of Public Service and Administration
National Treasury
Public Protector

### Intelligence Bodies

Electronic Communications Security (Pty)
Ministry for Intelligence Services
National Communications Centre
National Intelligence Agency
National Intelligence Co-ordinating Committee
Office of the Inspector-General of Intelligence
Office for Interception Centres
South African National Academy of Intelligence
South African Secret Service
Staff Council in the Intelligence Services

### Non-Governmental Bodies

Institute for Security Studies
South African History Archive
South African Traders Association
Open Democracy Advice Centre
South African National Editors' Forum

### Individuals

R.T. Antara
Dr N. Barnard
S. Banhegyi
Dr R. Broekman
D.J. Coetzee
M.B. Davies
D. Latham
H.J.P. Lebona
M.J.M. Louw
Dr T. Madinane

S.L. Mathe
V.M. Ntsubane
A. Roberts
J.N. Sikhakhane-Rankin
D.B. Sole
Dr S. Zondi

**APPENDIX C**

## LIST OF RECOMMENDATIONS

This Appendix contains the recommendations made in the Report.

Chapter 3: The White Paper on Intelligence

A new White Paper on Intelligence is required. The White Paper on Intelligence of 1994 is strong in terms of philosophy and principles. but weak in terms of policy, strategy and institutional arrangements. There is a need for more elaborate policy perspectives on a range of issues.

The following topics should be covered in the new White Paper:

- The mandates, functions and powers of the intelligence organisations, including oversight of, and controls over, their powers to infringe constitutional rights.

- Executive control and accountability, and the relationship between the intelligence services and the President, Cabinet and the Minister for Intelligence Services (hereafter "the Minister").

- Civilian oversight, including oversight by the Joint Standing Committee on Intelligence (JSCI) and the Inspector-General of Intelligence (hereafter "the Inspector-General").

- The relationship between the different intelligence organisations in South Africa, the co-ordination of intelligence and the functions of the National Intelligence Co-ordinating Committee (NICOC).

- Relations with foreign intelligence services and sharing intelligence about South African citizens with foreign governments.

- Secrecy and transparency, covering both the provision of information and the protection of information.

- The institutional culture of the intelligence services and ensuring respect for the Constitution and the rule of law.

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

Chapter 4: Ministerial Control and Responsibility

*Supply of intelligence to the Minister*

The Minister must be a designated recipient of national strategic intelligence and of intelligence relating to threats to the security of the Republic and its people. Accordingly, the National Strategic Intelligence Act No. 39 of 1994 should be amended to include the following provisions:

- The National Intelligence Agency (NIA) must inform the Minister of any domestic threat or potential threat to the security of the Republic or its people.

- The South African Secret Service (SASS) must inform the Minister of any foreign threat or potential threat to the security of the Republic or its people.

- NICOC must provide the Minister with national strategic intelligence and with intelligence regarding threats and potential threats to national security.

The powers of the Minister in relation to intelligence reports, and limitations on the exercise of those powers, should be covered in a ministerial directive drawn up in consultation with and approved by the JSCI.

*Supply of departmental intelligence*

In relation to the supply of departmental intelligence, the National Strategic Intelligence Act should be amended to reflect the following positions:

- NIA, SASS and NICOC may only supply departmental intelligence, or enter into a standing arrangement to supply departmental intelligence, with the approval of the Minister and subject to any conditions that he or she might set.

- A request for NIA, SASS or NICOC to provide departmental intelligence or enter into a standing arrangement to provide departmental intelligence must be made by the responsible minister in the case of a national department and by the Premier in the case of a provincial administration or department. The request must be made to the Minister.

The Minister should issue guidelines that regulate and expedite the supply of departmental intelligence.

*Supply of intelligence to the President*

The supply of intelligence and intelligence reports to the President by NIA, SASS and NICOC, and access to the President by the heads of these bodies,

should be regulated by the National Strategic Intelligence Act, ministerial regulations or a presidential directive.

The rules should state that intelligence and intelligence reports that are given to the President by NIA, SASS or NICOC must also be given to the Minister.

*Authority for tasking the intelligence services*

The National Strategic Intelligence Act should be amended to include the following provisions on authorisation for tasking the intelligence services:

- NIA, SASS and NICOC may only be tasked to gather and supply intelligence by the President, Cabinet, a Cabinet security cluster, the Minister and the Co-ordinator of NICOC. Any such tasking must be directed to the head of the intelligence body.

- NIA may request SASS to gather and provide it with any foreign intelligence that is required to fulfil the functions of NIA, and SASS may request NIA to gather and supply it with any domestic intelligence that is required to fulfil the functions of SASS.

- As recommended above, a request for NIA, SASS or NICOC to provide departmental intelligence to a government department must be made by the responsible minister in the case of a national department and by the Premier in the case of a provincial administration or department, and the request must be made to the Minister.

- If a parliamentary committee (other than the JSCI) or a parastatal organisation requires an intelligence briefing on a topic related to its business, the head of the committee or organisation must make the request via the Minister.

*Dismissal, suspension and transfer of a Director-General*

The Minister should introduce legislative provisions and regulations that cover disciplinary measures against, and the dismissal, suspension, demotion and transfer of, the heads of the intelligence services, NICOC and the South African National Academy of Intelligence (SANAI).

In preparing the legislative provisions and regulations, the Minister should consider the following issues:

- Whether the authority to conduct a disciplinary inquiry and take disciplinary action against the head of an intelligence structure should lie with the President or with the Minister subject to the President's approval.

- Whether the grounds for dismissing a Director-General of a government department outside the intelligence community should apply equally to the head of an intelligence structure.

- Whether a breakdown in trust between the Minister and the head of an intelligence structure should constitute grounds for dismissing the head.

- Whether demotion and transfer are viable options in the case of the head of an intelligence structure.

The terms of employment of the heads of the intelligence services are regulated by both the Intelligence Services Act No. 65 of 2002 and the Public Service Act No. 103 of 1994 but the interplay between the provisions of these two statutes is complex and unclear. In consultation with the Minister for Public Service and Administration, the Minister should fix the gaps and ambiguities through legislative amendments.

*Ministerial regulations and directives*

The Minister should issue regulations on the following topics:

- The conduct of intrusive operations, counter-intelligence operations and counter-measures.

- The supply of intelligence to the Minister.

- The supply of departmental intelligence to government departments.

- The production and dissemination of intelligence for consideration by Cabinet and the Executive.

- Authority for tasking NIA, SASS and NICOC to gather and produce intelligence.

- Disciplinary measures against, and the dismissal, suspension, demotion and transfer of, the heads of the intelligence services, NICOC and SANAI.

- The Inspector-General's investigations, inspections and certification of the reports issued by the heads of the intelligence services.

The existing regulations and those issued by the Minister in the future should be published in full in the *Government Gazette*. Rules that must be kept confidential for operational reasons should be issued as ministerial directives.

Ministerial approval should be required for the provision of information and intelligence on citizens and other people living in South Africa to foreign intelligence services, and the focus of any such information and intelligence should be confined to the planning or commission of a crime.

Chapter 5: The Inspector-General of Intelligence

The Intelligence Services Oversight Act of 1994 should be amended so that the mandate of the Inspector-General is confined to the ombuds role, which entails monitoring compliance by the intelligence structures with the Constitution and applicable legislation and policies; investigating complaints of non-compliance, abuse of power, misconduct and illegality by these structures; and certifying the reports submitted by the heads of the structures. The mandate should not cover significant intelligence failures, the effectiveness and efficiency of intelligence and counter-intelligence operations, and human resource complaints.

If the investigation of significant intelligence failures were removed from the Inspector-General's mandate, then the President, the relevant ministers, the JSCI or Parliament could determine the most appropriate means of investigating such failures on a case-by-case basis.

The Inspector-General's ombuds role should be extended to cover SANAI. The Inspector-General should be empowered in law or by ministerial directive 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 budget of the Office of the Inspector-General of Intelligence (OIGI) should be increased so that the Inspector-General is able to employ sufficient staff to fulfil his or her legislative mandate in a satisfactory manner.

The OIGI should be given independent organisational status, allowing it to receive and manage its budget independently of NIA and affording the Inspector-General full control over the resources and activities of the Office. 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 No. 1 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.

With respect to the Inspector-General's investigations and inspections:

- The Inspector-General should not have the power to subpoena witnesses.

- The Inspector-General should be obliged to report criminal conduct by a member of an intelligence service to the SAPS.

- The right to legal representation should apply where the Inspector-General uncovers criminality and there is the possibility of criminal charges being laid against a member of an intelligence service.

- The Inspector-General should not be authorised to indemnify witnesses against criminal 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. Amongst other things, it should have a website that provides contact details and describes its functions, activities and findings.

## Chapter 6: The Mandate of NIA

*The domestic intelligence mandate*

We support NIA's view that the concept of 'security threats' should be defined more clearly and that the Agency should have a narrower mandate. More specifically, we agree with NIA's recommendation that its mandate should focus on terrorism, sabotage, subversion, espionage, proliferation of weapons of mass destruction, organised crime and corruption. In addition, we propose that the mandate should cover large-scale violence and drug trafficking.

The term 'unconstitutional activity' as a security threat should either be defined properly or dropped. It is currently used to mean something different from 'illegal activity' but there is no indication of the kind of activities that are covered by the term.

We support the retention of 'border intelligence' as part of NIA's mandate.

We do not endorse NIA's recommendation that it should retain its focus on economic intelligence in support of government's economic policies and initiatives.

The National Strategic Intelligence Act should be amended to reflect the preceding recommendations. NIA's intelligence mandate should not be based on imprecise terms like threats to 'national stability', the 'constitutional order' and the 'well-being of the people'. Instead, the mandate should be defined more concretely and specifically with reference to terrorism, sabotage, subversion, espionage, proliferation of weapons of mass destruction, drug trafficking, organised crime, large-scale violence, corruption and specified financial and economic crimes (hereafter the "designated security threats").

The term ‘subversion’ should be redefined to cover activities that are intended to destroy or undermine the constitutional system of government through the use of violence or by other criminal means.

The legislation should state that security threats exclude lawful advocacy, protest, dissent or other activity unless undertaken in conjunction with one of the designated security threats.

In relation to the designated security 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 about the threats;
- to provide strategic intelligence to NICOC; and
- to contribute to law enforcement and preventive action by providing intelligence to the SAPS, the Department of Home Affairs and other government departments.

Whereas the emphasis of the police is on law enforcement and criminal investigation for the purpose of prosecution, the emphasis of the domestic intelligence agency should be on analysis, prediction, prevention, forewarning and advising the Executive.

It will be necessary to determine priorities within some of the designated threat categories, such as organised crime and corruption. As is currently the practice, on an annual basis Cabinet should identify National Intelligence Priorities based on the National Intelligence Estimate conducted by NICOC, and NIA should determine its operational priorities accordingly.

We agree with NIA that it should abandon its political intelligence focus as currently conceived. The Agency will still have to undertake non-intrusive monitoring of the political and socio-economic environment. In order to avoid any relapse into ‘political intelligence’, the aims of the monitoring should be spelt out clearly: to predict and detect the designated threats that fall within NIA’s mandate; to understand the dynamics and causes of these threats; to forewarn and advise the Executive about the threats; and to provide intelligence to NICOC, the SAPS and other relevant departments.

The intelligence legislation should prohibit the use of intrusive methods where there are no reasonable grounds to believe that the target has committed or is about to commit an unlawful act.

*The counter-intelligence mandate*

NIA should continue to perform the counter-intelligence functions of security screening, protection of intelligence and classified information, and any other defensive function that is provided for in law.

The National Strategic Intelligence Act should define more precisely, and should regulate, the functions of impeding and neutralising the effectiveness of foreign or hostile intelligence operations and countering threats.

The legislation should prohibit the intelligence services from interfering with, and using countermeasures in relation to, lawful political and social activities in South Africa and other countries.

The legislation should also prohibit the intelligence services from disseminating false or misleading information to the public.

In addition to tighter legislative provisions, there is a need for ministerial regulations. The National Strategic Intelligence Act provides that the Minister may, after consultation with the JSCI, make regulations regarding the co-ordination of counter-intelligence by NIA. The regulations should cover guidelines, principles and authorisation for the use of countermeasures.

*The departmental intelligence mandate*

In Chapter 4 we made recommendations on departmental intelligence. In summary, the Minister should issue policy and procedural guidelines that regulate and expedite the provision of departmental intelligence; the provision of departmental intelligence should be subject to the Minister's approval and any conditions that he or she might set; and a request for departmental intelligence must be made by the responsible minister in the case of a national department and by the Premier in the case of a provincial administration or department.

The focus of departmental intelligence should be narrowed in accordance with our preceding recommendations on narrowing NIA's intelligence mandate. Departmental intelligence should be confined to intelligence regarding security arrangements and the designated security threats and should be provided to a department where this is necessary, and only to the extent that it is necessary, for the department to take action in accordance with its mandate.

Chapter 7: Intrusive Operations

*Legislation*

The Minister should introduce legislation that regulates in a uniform manner the use of 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 elements:

- 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 fulfil their functions as defined in law.

- The intelligence services should be prohibited from using intrusive measures against persons and organisations that are involved solely in lawful activity. An alternative formulation would be that the intelligence services may not use intrusive measures in relation to lawful activities unless these activities are reasonably believed to be linked to the commission of a serious offence.

- The intelligence services should be prohibited from interfering with political processes in other countries, whether through the use of intrusive methods or by any other means.

- The use of intrusive measures by the intelligence services should require the approval of the Minister. The Minister must be satisfied that the criteria for using these measures have been met.

- The use of intrusive measures should require the prior 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 make an independent assessment of whether the circumstances warrant the employment of intrusive measures.

- As with the Regulation of Interception of Communications and Provision of Communication-Related Information Act No. 70 of 2002 (hereafter "RICA"), the legislation should state that intrusive methods may only be used as a matter of last resort.

- The legislation should require intrusive measures to be carried out with strict regard to decency and respect for a person's rights to dignity and personal freedom, security and privacy.

- The legislation should state that 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.

*Regulations, guidelines and operational directives*

The Minister should issue regulations and policies that guide the implementation of the new legislation on intrusive methods. The policies could be included in a new White Paper on Intelligence.

As proposed by the Legislative Review Task Team, 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.

Flowing from the introduction of new legislation, regulations and ministerial policies, the heads of the intelligence organisations should issue operational directives that provide for internal procedures, controls, authorisation, supervision and compliance.

Prior to the introduction of 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 set a deadline by which this is to be done. 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

*The NCC Bill*

The National Strategic Intelligence Amendment Bill, which provides for the functions of the NCC, should state that the NCC is bound by RICA. It should also stipulate that the NCC may not intercept the communication of a targeted person unless it has obtained an interception direction issued by the designated judge as provided for in RICA.

The Bill should indicate which intelligence, security and law enforcement bodies are entitled to apply to the NCC for assistance with the interception of communication; it should specify the grounds that can be invoked by each of these bodies; and it should describe the information that must be contained in an application for signals monitoring.

The Bill should not allow for the interception of communication on the grounds of protecting and advancing international relations and the economic well-being of the Republic, or on the grounds of supporting the prevention and detection of regional and global hazards and disasters. As proposed in Chapter 7, intrusive measures such as interception of communication should be limited to situations 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 indicate whether the NCC can, on its own initiative, identify targets for signals monitoring or whether it can only monitor the targets identified by another intelligence service or a law enforcement body.

The Bill should provide that interception of communication is a method of last resort that can only take place if non-intrusive methods are inadequate or inappropriate.

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. Where random monitoring identifies the need to focus on a specific person or organisation, the requirements of ministerial approval and judicial authorisation should apply.

*Intelligence policies and procedures*

The intelligence organisations should take immediate steps to ensure that their policies and procedures on the interception of communication provide for ministerial approval and judicial authorisation and are in alignment with the Constitution and legislation. The Minister should set a deadline by which this is to be done and should request the Inspector-General to certify the revised policies and procedures in terms of their alignment with the Constitution and the law.

## Chapter 9: Internal Controls and Policies

The operational policies of the intelligence services must interpret correctly and be properly aligned with the relevant constitutional and legislative provisions.

We support the recommendations of the Legislative Review Task Team regarding the need for ministerial regulations and operational directives that tighten controls over intrusive operations.

The determination of the level of authorisation, management and supervision of an intelligence operation should take account of the risk that the operation might violate constitutional rights and interfere with the political process.

The intelligence services should establish clearance panels comprising senior officials in order to assess applications to initiate intrusive operations.

Efforts should be made to achieve greater rationalisation and co-ordination of intelligence oversight and review activities, provided that the solutions do not compromise the quality of control and oversight.

## Chapter 10: Financial Controls and Oversight

The Security Services Special Account Act No. 81 of 1969 and the Secret Services Act No. 56 of 1978 should be repealed. As with other government departments, the funds allocated to the intelligence services by Parliament should go directly to them.

We support the National Treasury proposal that the intelligence services should have their own vote in respect of monies approved annually by Parliament and that the annual budgets and financial reports of the services should be presented to Parliament as public documents. The documents should exclude information that, if disclosed, would endanger security or compromise intelligence operations, methods or sources.

As required by the Constitution, the audit reports on the intelligence services should be presented to Parliament. In accordance with the Public Audit Act No. 25 of 2004, sensitive information can be withheld from the reports if deemed necessary by the Auditor-General or the Minister.

The audit reports on the intelligence services for the past five years should be disclosed to Parliament. This process should be co-ordinated by the Minister in consultation with the JSCI.

As a matter of urgency, the Auditor-General and the Inspector-General should finalise arrangements whereby the Inspector-General provides the assistance that is necessary to ensure a satisfactory audit of expenditure on covert operations. The Minister should facilitate meetings between the Auditor-General and the Inspector-General for this purpose.

## Chapter 11: Institutional Culture

The heads of the intelligence organisations must have a zero-tolerance approach to misconduct and illegality by their members, and the Minister, the Inspector-General and the JSCI must ensure adherence to this policy.

The Minister should ensure that the civic education Steering Committee and Technical Committee meet regularly and submit reports to him or her.

The heads of the intelligence organisations should set up the required monitoring systems to assess their institutional culture and the impact of the civic education programme, and should submit bi-annual reports to the Minister on the results of the monitoring.

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.

In consultation with the members of the civilian intelligence organisations, the Minister should find an arrangement that addresses the labour rights of members to the satisfaction of all the parties.

The Minister should request the Intelligence Services Council on Conditions of Service to prepare proposals on improving the mechanisms for addressing grievances and disputes in the intelligence organisations. The Minister should also ensure that the independent appeals board provided for in the 2003 ministerial regulations is set up immediately.

The Minister and the heads of the services should take steps to enhance the quality of legal advice in the intelligence community. They should send their legal staff on training and refresher courses; submit draft operational policies to the Inspector-General and external experts for comment; and consider the option of making high-level appointments of legal experts.

The Minister should request the Inspector-General or SANAI to do a survey of international law that has a bearing on the operations of the intelligence organisations, indicate the implications for these operations and propose any amendments to domestic laws and policies that are necessary.

The Technical Committee of the Civic Education Programme should include the relevant aspects of international law in the civic education curricula.

## Chapter 12: Transparency, Secrecy and Provision of Information

The National Intelligence Priorities approved annually by Cabinet should be subject to parliamentary consultation and debate. The consultation should first be conducted with the JSCI, after which the document should be presented to Parliament for open debate involving all members. Information that is extremely sensitive could be withheld from the public document.

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

Once the Minister has finalised the “Draft Regulations on the Coordination of Intelligence as an Activity: Determination of Intelligence Priorities and Prescripts Relating to the Conduct of Intelligence Services”, he or she should table the document for parliamentary and public comment. Following the consultation, the regulations should be published in the *Government Gazette*.

Executive policy on intelligence and the operations of the intelligence services should be in the public domain.

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

As recommended in Chapter 10, the annual budgets and financial reports of the intelligence services should be presented to Parliament as public documents.

As recommended in Chapter 10, the audit reports on the intelligence services should be presented to Parliament as public documents. In addition, the audit reports on the intelligence services for the past five years should be disclosed to Parliament.

NICOC and the OIGI set up establish websites that include detailed information about their respective functions and activities.

All the intelligence organisations should have on their websites a section that assists members of the public who want to request information under the Promotion of Access to Information Act No. 2 of 2000 (hereafter “PAIA”).

The intelligence services should produce the information manuals required by section 14 of PAIA. If there is specific information whose disclosure would cause significant harm, then the intelligence services should apply for an exemption to exclude that information.