Submission from the Institute for Security Studies and the Open Society Justice Initiative to the Ad Hoc Committee considering the Protection of Information Bill [B6-2010]

25 June 2010

Contact details Lauren Hutton
Researcher
Security Sector Governance Programme
t - (012) 346 9500
f - (012) 460 0998
e – lhutton@issafrica.org

Recommendations

1. The Bill should be withdrawn from Parliament and significantly re-drafted.

2. Definitions of **intelligence, counter-intelligence** and **domestic intelligence** should be standardised in agreement with existing intelligence policy and legislation.

3. A process to review the 1994 White Paper on Intelligence would be useful to ensure that the definitions of the terms **intelligence, counter-intelligence, domestic intelligence** and **foreign intelligence** have broad-based agreement. This would require wider dialogue on the role of intelligence in democratic South Africa in the 21st century.

4. **Chapter 2, item (j)** under 'General principles of state information' should be removed.

5. **National security** and **national interest** should not be used as the criteria for the justification for protection.

6. Chapter 6 (15) Classification criteria should be made clearer. The terms **harmful** and **endanger** should be defined.

7. Clauses relating to the protection of **commercial information** should be removed and no powers be granted to allow for the classification of commercial information.

8. Reasons for classification should be clearly noted. **Sections 15** and **17** need to be aligned into one section that lists classification criteria.

9. An independent authority should be assigned tasks associated with the implementation and monitoring of the use of classification.

10. **Hostile activity offences** should be limited through the inclusion of a public interest clause.

11. **Section 40** should be removed.

CONTENTS

1. Introduction

Legislation to regulate the classification and declassification of information has been expected in South Africa since the end of the apartheid regime. The current legislation – The Protection of Information Act – dates back to 1982 and the height of the centralised security state. The 1982 Act does not find resonance in a democratic society with constitutional imperatives of openness, transparency and accountability. In this regard, the new Protection of Information Bill is welcomed as a step towards improving access to information by creating restrictions on the types of information that can be classified and controlled and limits on the periods for which information can be classified.

When this Bill was originally proposed in 2008, there was much public concern about provisions that could infringe upon media freedom and the constitutional right to information. The Bill was withdrawn towards the end of 2008 and a redrafted version has now been presented for debate. On first glance, there are some improvements to the Bill; overall it is more concise and coherent. However, many of the fundamental issues, brought to the fore by the media and civil society groups, remain unchanged.

This submission seeks to highlight some aspects of the Protection of Information Bill [B6-2010] (hereafter the Bill) that are could be interpreted as contrary to the constitutional rights of access to information and freedom of expression and democratic governance imperatives as well as being contrary the aim of creating a succinct regime for the protection of information.

2. Definitions

In the section of the Bill providing definitions of the terms contained therein, there are a number of inconsistencies with intelligence policy and other intelligence legislation, most particularly the White Paper on Intelligence and the National Strategic Intelligence Act.

The Bill defines **intelligence** as 'any information, obtained by a national intelligence structure, for the purpose of crime prevention, investigation and combating or for the purpose of informing any government decision or policy-making process carried out in order to protect national security or to further the national interest.'

The 1994 White Paper on Intelligence – the guiding policy framework for the governance of intelligence functions in South Africa – defines **intelligence** as (Section 3.2.1) '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.'

The definition proposed in the new Bill is broader than that presented in the White Paper on Intelligence. Firstly, the definition in the Bill equates *intelligence*

to *any information*. Information or data, in and of itself, is not intelligence. Intelligence has to be treated as a special kind of information because of the special powers associated with the collection thereof. By equating intelligence to any information informing the decision and policy making process, broadens the scope of intelligence to include media reports, civil society and research papers and information generated by political parties, trade unions and information from many other sources.

Intelligence involves information but the factor, which distinguishes intelligence from any information, is the ability to utilise covert means of collection and the need to secure such information as its release could negate its effectiveness. The ability to use secrecy to collect and then protect information is central to differentiating intelligence from other forms of information. Other differentiating points would be that intelligence is associated with the security of the state and is tasked by, collected and processed for government decision-making purposes. As explained in the 2003 Intelligence Budget Vote speech by then Minister of Intelligence Services Lindiwe Sisulu,

> Intelligence is a secret state activity to understand any threat to national security and thereafter to advise policy makers on steps to counteract such threat. It is an activity performed by officers of the state for state purposes. Secret collection and the use of information that is not publicly available are the constitutive elements that would distinguish this from other intellectual activity[i].

The definition of intelligence as provided in the White Paper is already broad and allows for the inclusion into the realm of secrecy any information associated with policy- and decision-making on stability, security and development. This enables the state intelligence services to define a broad area of engagement and justifies the use of what should be a specialised tool in a wide range of challenges facing the nation. Working from such extensive definitions of the scope of intelligence in South Africa, the focus has moved from concerns with external and foreign actors[1] as threats, to a primary focus on threats to internal stability and development. Given the security dynamics facing South Africa, the strategic risks and vulnerabilities have their roots in socio-economic tensions and the role of intelligence in combating internal risks of this nature needs to be further interrogated. The concern with the 'new' definition presented in the Protection of Information Bill is that the already broad scope of intelligence is further enlarged to include not only processed information but rather any information. The scope in which secrecy as a defining characteristic of intelligence can be used is therefore expanded to a degree that is inconsistent with constitutional imperatives, democratic norms and good governance standards.

The second definition presenting inconsistencies is **counter-intelligence** which is defined in the Bill as 'measures and activities conducted, instituted or taken to

[1] Internationally, intelligence has traditionally been associated with external threats, foreign relations and the military capacities and intentions of foreign states. However, in former colonies, the state security structures have had a remarkably different historical evolution that has imbued intelligence in most parts of Africa with an internal focus. The apartheid legacy in South Africa has also contributed to a continued concern with internal instability.

impede and to neutralise the effectiveness of foreign or hostile intelligence operations, to protect intelligence and any classified information, to conduct security screening investigations and to counter sedition, treason and terrorist and –related activities.'

The National Strategic Intelligence Act 39 of 1994 defines **counter-intelligence** as 'measures and activities conducted, instituted or taken to impede and to neutralise the effectiveness of foreign or hostile 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.'

The difference lies in the phrasing and word selection of the last part of the definition. The primary concern is the substitution of the words *subversion* and *sabotage* (in the National Strategic Intelligence Act) for *sedition* (in the Bill). Sedition differs significantly from subversion. The act of sedition can be defined as 'the speaking or publishing of words which excite public disorder or defiance of lawful authority.[ii]' Sedition as an offence has its roots in the monarchies of Europe in the 1600 and 1700s that were fearful of critique and dissent and used legal means to restrict criticism and freedom of speech.

Subversion as a threat to the state refers to attempts to overthrow structures of authority for example through a *coup d'état*. The main concern with the change in language in the new Bill is that the counter-intelligence mandate is already broad and does not specify nor restrict the range of measures and activities that can be conducted under the banner of counter-intelligence. Indeed, the 2008 Report of the Ministerial Review Commission on Intelligence, registered the following concern about the 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 investigations. 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 definition contained in the Bill enlarges an already broad and dangerously vague mandate, and potentially allows the intelligence structures to redefine their scope of operations to include taking measures to counter criticism of government policies and officials or to counter individuals seeking to organise and mobilise to express discontent with government policy. Furthermore, the National Strategic Intelligence Act specifies that hostile acts warranting inclusion under a counter-intelligence mandate are acts 'aimed at or against personnel, strategic installations or resources of the Republic.' The definition of counter-intelligence as formulated in the Bill places no such limitation and thus creates

potential for the political manipulation of counter-intelligence resources for partisan purposes. Notably within the Constitution the freedom of expression is already contextualised to exclude incitement of imminent violence and incitement to cause harm. Further restriction as a counter-intelligence interest, is thus unnecessary and poses greater risks to freedom of expression and public accountability than potential gains for national security.

The third definition in the Bill that differs significantly from definitions already contained in other legislation is that of **domestic intelligence**. The Bill defines **domestic intelligence** 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, the safety and well-being of its people, *on 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*.' The italicised phrase is not contained in the definition of domestic intelligence in the National Strategic Intelligence Act. This is of concern as the domestic intelligence mandate is already viewed by civil society groups as being overly broad and open to manipulation – as expressed in the Institute for Security Studies submission to the Ministerial Review Commission on Intelligence in 2007[iii]. Indeed, the Review Commission found that:

- The domestic intelligence mandate is too broad and open to interpretation
- NIA has historically interpreted this mandate in so expansive a fashion as to encompass the thematic focus of virtually every government department
- The broad mandate and political intelligence function may have politicised NIA and given rise to an inappropriate focus on political activities
- The Act should be amended so that NIA's intelligence mandate is not based on imprecise terms like threats to 'national stability'

The definition presented in the Bill suffers from the same weaknesses as noted above and is further compromised by the reference to 'all matters relating to the advancement of the public good.' This has further expanded to terrain of intelligence focus and activities, which is impractical and does not allow for focus and prioritisation in countering serious criminal threats and the potential for violence. Additionally, including this additional language is tantamount to expanding the mandate of the domestic intelligence body without public consultation or parliamentary debate on the role and function of intelligence in democratic South Africa. This is in stark contrast to the constitutional imperatives for open and participatory governance.

Finally, the manner in which **foreign intelligence** is defined, although echoing the words of the National Strategic Intelligence Act, remains flawed in one significant regard: the 1994 White Paper distinctly associates intelligence with decision- and policy-making information, while the proposed statutory language does the opposite. The definition of **foreign intelligence** presents scope for the collection of information of foreign threats and opportunities 'irrespective of

whether or not it can be used in the formulation of the foreign policy of the Republic.' If foreign intelligence has no foreign policy purpose, then what or whose purpose does it serve?

3. General principles of state information

The statement of general principles as enunciated in Chapter 2 imbues the Bill with a strong commitment to transparency, openness and access to information. For example, item (b) notes that 'information that is accessible to all is the basis of a transparent, open and democratic society' and item (c) notes that 'access to information is a basic human right and promotes human dignity, freedom and the achievement of equality.'

However, the utility of the principles is compromised with item (j), which places the caveat of national security as the overriding principle. Item (j) states 'paragraphs (a) to (i) are subject to the security of the Republic, in that the national security of the Republic may not be compromised.' Principles (a) to (i) are no less true in the context of national security and should not be viewed as being in contradiction to national security. Indeed as argued in the Ministerial Review Commission submission on the Protection of Information Bill in 2008, national security provides a compelling basis for transparency because from a constitutional perspective, national security is not something different from fundamental rights and freedoms.

The term 'national security' as used throughout the Bill creates difficulties. Firstly, the definition of national security is expansive, vague and imprecise. The Bill defines **national security** as:

> 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, and includes protection of the people and occupants of the Republic from hostile acts of foreign intervention, terrorist and related activities, espionage and violence, whether directed from or committed within the Republic or not, and includes the carrying out of the Republic's responsibilities to any foreign country in relation to any of the matters referred to in this definition.

From this definition it is very difficult to ascertain what is and is not an issue of national security. To use this as the basis for determining when rights as enshrined in the Bill of Rights may be limited is contrary to the constitutional imperative that rights may only be limited 'to the extent that the limitation is reasonable and justifiable in an open and democratic society.'

Similarly, the definition of **national interest** in Chapter 5, Part A (11) of the Bill provides little clarity on what is in the national interest. The phrase 'all matters relating to the advancement of the public good' virtually equates national interest to all areas of government activity. If such broad definitions of national security and national interest are utilised in the legislation, there needs to be greater clarity of what within these realms constitutes legitimate areas of activity for the state security sector, intelligence functions related thereto and

areas in which secrecy can be legitimately employed. Otherwise, the role of intelligence, the functions of the state security sector and the legitimate use of secrecy become functional aspects of all government departments.

Given the problems with the definitions of national interest and national security as mentioned above, these terms are not useful as guides to justify the restriction of access information. But even in the application of these cumbersome terms, the Bill suffers from a lack of consistency. For example, Chapter 6 (15) Classification levels:

- State information can be classified as "Confidential" if disclosure thereof may be harmful to the 'security or national interest of the Republic'
- State information can be classified as "Secret" if disclosure thereof may endanger the 'security or national interest of the Republic'
- State information may be classified as "Top Secret" if disclosure 'may cause serious or irreparable harm to the national interest of the Republic'

Instead of utilising the term *national security,* which was defined in the earlier sections, the drafters used the term *security,* which is undefined and thus has even less utility as a guide for determining if information should be protected. Furthermore, it will be difficult to distinguish what information is *harmful* and what would *endanger* the security of the Republic, making 'Confidential' and 'Secret' information too similar to differentiate.

A further example of the difficulties in applying the terms 'national security' and 'national interest' occurs in Section 17(1)(j) which states that 'scientific and research information not clearly related to the national security and national interest may not be classified.' Given that 'national security' encompasses the freedom from fear and want and 'national interest includes all matters related to the public good, there is little indemnity in the amount of information that can be classified. Item (j) does not create any protection from excessive classification and could be used to classify any range of scientific and research material from health and education matters to regional economic development, social sciences and infrastructure and development.

Similarly in relation to **commercial information** (Chapter 5(12))**,** justifying secrecy in order to prevent 'reputation injury' seems to stand in stark contrast to the principles of public accountability, openness and transparency. In detailing classification levels, commercial information that if disclosed could 'cause financial loss to an entity or may prejudice an entity in its relations with its clients, competitors, contractors and suppliers' can be classified 'Confidential' and protected. This seems very broad; fear of 'financial loss' and 'prejudice' can be broadly employed to prevent public accountability, especially in relation to the utilisation of state funds. The Bill needs to specify in greater detail what kind of commercial information needs to be protected and why.

We consulted with several international experts when compiling this submission and could not find any examples of states that classify commercial information in

a similar manner to that proposed in the Bill. Thomas M. Susman, Director of the Governmental Affairs Office of the American Bar Association, provided the following input:

> In making an argument against providing for classification of commercial information, the government should be reminded of the great expense of maintaining classified records: special designation for government officials, special handling, special storage, etc. I've followed this (commercial information) field for decades and have not seen any jurisdiction that finds it necessary to impose a classification scheme for protection.

In light of the above sentiment, the commercial information clauses should be removed or at least significantly altered. Classified information is, as defined in the Bill, information that requires protection and it is our contention that commercial information should not be placed in that category.

Broad definitions and the use of terms such as national interest and prejudice as the guiding principles on the classification of information do not assist the organs of state in the processing of information and will not enable improved flows of information nor will they reduce the amount of information that is classified. As these are amongst the reasons given by the Ministry of State Security for the introduction of this Bill, these aspects should be given greater clarity in the text of the proposed legislation.

There is also an inconsistency between the reasons for classification as enunciated in Section 15 and the directions for classification in Section 17. According to Section 17 (1)(d):

> Information is classified only when there is –
>
> (i) a clear, justifiable and legitimate need to do so
>
> (ii) a demonstrable need to protect the information in the national interest

The protection of commercial information that may prejudice the financial interests of an individual or corporation may not be in the public good. Which Section takes precedent in such instances? Section 17 (1)(c) notes that 'the classification of information is an exceptional measure and should be conducted strictly in accordance with sections 11 and 15.' The failure of the Bill to clearly articulate the reasons for classification will create an environment of uncertainty in application and could lead to greater restrictions on access to information than possibly intended.

4. Criteria for continued classification of information

The criteria presented in Chapter 7 of the Bill are clearer and more concise than the criteria for classification presented in Chapter 6. These are strong guidelines on the type of information that should be protected and could possibly be used in the preceding chapters instead of vague terms like national interest. The only aspect of concern is item (f) which again speaks to the need to classify information that may cause financial loss or prejudice the interests of non-state

institutions. This does not speak to the notion of the protection of information to prevent significant and demonstrable harm to the national interest of the Republic – which is placed as a central tenet of the Bill. There seems to be an inconsistency between applying the special power of secrecy in limitation of constitutional rights on the one hand to protect persons from life threatening or physical harm and on the other to prevent non-state institutions from financial loss. It is understandable to utilise classification to protect sources, plans and methods but to use secrecy to protect the financial interests of non-state actors begins to tread controversial ground that calls into question commitments to transparent and accountable governance.

5. The role of the National Intelligence Agency

Chapter 10 outlines the implementation and monitoring responsibilities as assigned to the Agency in the Bill. Cognisant of the counter-intelligence mandate assigned to NIA in the National Strategic Intelligence Act, if the purpose of the Bill is to decrease classification and excessive secrecy, then the Agency may not be the best actor to be entrusted with the implementation and monitoring thereof. Intelligence agencies by their very nature are more prone to secrecy than transparency. Also given the questionable reputation of NIA and the public association of the domestic agency with internal political competition, it does not readily present as an ideal steward of transparent and accountable governance.

Concerns can also be raised about the capacity of NIA to implement the mandate assigned to it in the Bill that includes policy formulation, implementation and monitoring. As recent as 2007, the Auditor General reported on a lack of information security at NIA. As noted in the recently released 2007 report of the Auditor General, the significant information security control weaknesses witnessed at NIA emanated from a shortage of skilled personnel and vacancies not being filled for a considerable period of time. These weaknesses included:

- Sensitive transaction codes had not been locked in production to prevent general user access
- The failure to implement critical network and security monitoring facilities/ tools/ procedures

Although these specific issues were not brought to the fore in the 2008 audit report, other serious areas of concern were raised by the Auditor General which include:

- Lack of adequate policies and procedure to fully implement the Public Financial Management Act
- Lack of an approved risk management policy
- Concerns with procurement practices

In order to encourage independent oversight and efficient implementation, the creation of an independent body to provide training on classification and declassification and monitoring the implementation thereof should be considered. This task could be assigned to existing agencies such as the Human Rights Commission or the Inspector General. Such an approach is not contrary to the counter-intelligence mandate of NIA but rather removes excessive tasks from

the Agency that can be provided for the interests of public accountability and the imperative of transparent governance by an alternative actor. There is international precedent for this as illustrated in part 9 of this submission.

6. Hostile activity offences

During debates on the Protection of Information Bill in 2008, there was concern expressed by civil society groups and media organisations about the impact of the hostile activity offences and the need to include a public interest disclosure clause. As expressed in the briefing by the Ministry for State Security to the Ad Hoc Committee on 7 May 2010, the inclusion of a public interest defence clause was not included in the revised version because 'this clause creates legal uncertainty in the interpretation and application of the Bill.' Potential uncertainty in the application of the Bill should not suffice as sufficient reason to restrict rights enshrined in the constitution.

In 2006, the United States Congress considered controversial intelligence legislation to grant wider domestic powers to the intelligence apparatus in the context of counter-terrorism. One of the issues debated was legislation to criminalise the publication of classified information by the media. Geoffrey Stone, Professor of Law at the University of Chicago made the following argument:

> There is nothing inherent about government secrets that would make their publication of only 'slight value as a step to truth'. To the contrary, the publication of government secrets may be extraordinarily valuable to the proper functioning of a self-governing society. Indeed, the very notion that the United States would punish the press for publishing government secrets seems incompatible with the most fundamental tenets of public accountability[iv].

This holds as true for the US as it does for South Africa. Unfortunately, if we look across our continent the ability of the media to operate as an essential tool of public accountability is increasingly under threat and the undemocratic application of the tools of national security and secrecy is often at the forefront of the assault on media freedom. The International Press Institute provides the following analysis of media freedom on the African continent in 2009:

> African journalists faced a vast array of violations of their right to press freedom and freedom of expression in 2009. These included intimidation, harassment, threats, attacks, beatings, illegal detentions, arrests and imprisonment…Newspapers, broadcasters and journalists alike faced spurious lawsuits. Many reporters were slapped with criminal charges, often for alleged defamation and sedition, and very often for covering corruption or the activities of security forces.
>
> In Africa, some countries are worse press freedom offenders than others, and some techniques of repression are used more than others in certain countries. The laws of a country (and judges' fair interpretations of those laws) should help keep its journalists safe; unfortunately, several African countries passed potentially or explicitly restrictive legislation this year.

> Many maintain criminal defamation, national security and other laws that carry heavy prison sentences and which are used as tools to silence critical reporting. In several countries that were holding or preparing for elections, or in which there was a political crisis, journalists faced a gamut of press freedom violations. Among the favourite tools used to silence the media in Africa are criminal libel and insult laws, including laws that protect the reputations of public officials. Such legislation has been used to lock up journalists or bankrupt publications and broadcasters. These laws have a chilling effect on the media. Criminal libel charges were reportedly brought against the media and media professionals in Botswana, Cameroon, DRC, Equatorial Guinea, Gambia, Niger, Nigeria, Senegal, Sierra Leone, Somalia, Swaziland, Tanzania, Togo, Uganda and Zimbabwe.

With media freedom under threat across the continent, South Africa could serve as a beacon of liberal democratic principle – safeguarding the role of the media and other non-government organisations as bastions of public accountability and oversight. Read in conjunction with other aspects of the Bill such as the inclusion of sedition as part of the scope of counter-intelligence and the broad definitions of intelligence, national security and national interest, there is a serious concern that this Bill can be used to further the pattern of restriction on media freedom as seen in other parts of Africa.

A possible remedy to potential restrictions on investigative journalism and public accountability is the inclusion of a 'public interest clause.' As argued by FXI in 2008[v]:

> The crucial role of the media in promoting Constitution building and maintaining a watchful eye on the activities of Government will be adversely affected by this omission (*of a public interest clause)*…What is required is an exemption which would require only of the journalist to allege a bona fide interest. In the event that such bona fide interest was contended against by the state the onus would be on the State to prove the absence thereof in line with the normal criminal law onus of proof.

Similar sections of concern are Section 18 and 39, which make it an offence punishable by 3-5 years imprisonment for being in possession of classified information. Furthermore, Section 42 of the Bill makes an offence of classifying information to cover corruption, inefficiency or unlawful conduct. Such an offence is punishable by no more than 3 years imprisonment. Providing significantly more severe terms for possession of classified information (particularly without the possibility of a public interest defence) than for the use of classification to hide unlawful conduct, inefficiency or corruption cannot be easily reconciled with the constitutional priority assigned to transparent, democratic governance and the role of public accountability in a democratic dispensation

7. Information peddlers

The submission below is based on the minutes of the briefing provided to the Ad Hoc Committee by Mr Sinthumule Ramabulana on 1 June 2010. Although the briefing was public, the content thereof remains classified. The minutes of the meeting are publicly available on http://www.pmg.org.za. The following points relate to Section 40 of the Bill and the creation of an offence of providing false information to a national intelligence structure. The justification for this clause provided by the Ministry of State Security is based on an analysis of the dangers of information peddlers.

Mr Ramabulana explained that information peddlers are involved in the interception of communications, extortion, espionage, subversion, illegal business activities and blackmail. However, according to the Minister, upon arrest of some perpetrators, they were unable to be charged. The activities detailed by Mr Ramabulana all represent significant threats to the Republic and its people and are criminal acts and should be treated as such. It is not the distribution of false information that is the greatest threat but rather extortion, espionage and subversion. There seems to be a disconnect between wanting to prosecute for the provision of false information but not for the illegal interception of communication and the other offences mentioned.

Additionally, former apartheid era intelligence, defence and police operatives are positioned as the prime culprits of information peddling. This creates an association with a 'Third Force' style threat to internal stability. However, the examples stated during the briefing, such as the Special Browse Mole Report, originated in the current government structures.

This submission does not seek to suggest that there are not legitimate cases of espionage and disinformation. The real question becomes how to address the potential damage that can be done by such activities and whether or not current criminal legislation is adequate. We contend that actors trying to destabilise South Africa through subversion, bribery, espionage and extortion should be prosecuted for those crimes. The provision in the Bill provides for 3-5 year sentences for providing false information. If the real threat is subversion, then this sentence is not adequate and fails to address the real threat.

The second concern is that this provision puts the onus of verification on the supplier of information and not on the state intelligence apparatus. As mentioned by Mr Ramabulana, on receipt of unknowingly false information, the NIA had to review its intelligence estimates. This implies that the capacity to verify information and consult all sources does not exist within the intelligence structures. Further, members of the public are not encouraged to share information with the intelligence structures unless they are convinced and can defend the veracity thereof in a court of law if required. This discourages the building of relationships between the intelligence fraternity and the public and can have long-term consequences for the security of the Republic in an era characterised by the need for information sharing and partnership to counter threats.

8. Examples from international practice

Given the complexities associated with the protection of information and the tensions inherent in discussion about access to information and national security, this final section of the submission seeks to explore international examples in order to create a basis for comparison and to seek good practices.

In a review of access to information by the media in the Organization for Security and Co-operation in Europe (OSCE), a general finding was that many countries retain the right to classify too wide an array of information as state secrets[vi]. The report noted that the majority of OSCE participating states have not adjusted their rules of classification to the principles of freedom of information thus disregarding the primacy of the public's right to know[vii].

Although this was an indictment of the level of implementation and adherence to the right of access to implementation, it is evidence of the complexity of managing access to information and protecting legitimate national security concerns. The first major stumbling block is what information to protect. As in the South African Bill currently under debate, the starting point for many pieces of legislation is defining what information needs to be protected from disclosure. Terms such as national security are often employed, even without further defining what the concept is meant to entail.

Some extracts from international legislation are presented below[viii]:

- In **Lithuania**, a state secret is limited to information that would 'violate the sovereignty of the Republic of Lithuania, defence or economic power, pose harm to the constitutional system and political interests of the Republic of Lithuania, pose danger to the life, health and constitutional rights of individuals'.
- The **U.S**. Executive Order on Classification[ix] sets out eight areas that are eligible for classification:
    - Military plans, weapons systems, or operations;
    - Foreign government information;
    - Intelligence activities (including special activities), intelligence sources or methods, or cryptology;
    - Foreign relations or foreign activities of the US, including confidential sources;
    - Scientific, technological or economic matters relating to national security, which include defence against trans-national terrorism;
    - U.S. government programs for safeguarding nuclear materials or facilities;
    - Vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans or protection services relating to national security, which includes defence against trans-national terrorism;
    - Weapons of mass destruction

The Lithuanian and U.S. examples above are presented merely to illustrate alternative clauses, which can be employed to overcome reliance on unwieldy and inexact definitions of national security and national interest as in the Bill.

The second issue regarding which we can draw on international experience concerns the duration of classification. In the interests of promoting access to information, regulated information should only be classified for as long as it is necessary to protect the interests concerned from significant harm. For example[x]:

- The Law on Classified Information of **the former Yugoslav Republic of Macedonia** limits State Secrets to 10 years, Highly Confidential information to five years, Confidential information to three years and Internal information to two years.
- In **Albania**, secrets are limited to ten years under the Law on Classified Information.
- The **U.S**. Executive Order sets a default of ten years unless it can be shown that it needs a longer duration.

Similarly, in the pursuit of encouraging greater access to information, procedures for review of classification are required[xi]:

- The **Georgian** and **Estonian** State Secrets Act require that each possessor of secrets review the classification yearly and note when it has been declassified.
- In **Sweden**, the classification is re-evaluated each time the document is accessed.
- **Uzbekistan** and **Turkmenistan** require that information is reviewed every five years.

A good practice that can be garnered from international experience is the creation of a specialised body to make decisions on the categories of information to be classified and to review decisions on classification. A body independent of the intelligence and security services fulfilling such functions operates as a mechanism of oversight and a check on the excessive use of secrecy. Examples in this regard include[xii]:

- In **Bulgaria**, the Law for the Protection of Classified Information created the State Commission for the Security of Information (SCSI). The SCSI controls the handling of classified information and even provides training.
- In **France**, the 1998 law on classification of national security information created the *Commission consultative du secret de la défense nationale* (CCSDN). This gives advice on the declassification and release of national security information in court cases. The advice is published in the Official Journal.
- In **Hungary**, under the Secrecy Act of 1995, the Parliamentary Commissioner for Data Protection and Freedom of Information is entitled to change the classification of state and official secrets.
- In **Slovenia**, the Information Commissioner can check the accuracy of the classification.

Given these experiences and other examples, the OSCE has produced the following recommendations on classification rules[xiii]:

> The definition of state secrets should be limited only to data that directly relate to the national security of the state and where their unauthorized release would have identifiable and serious consequences. Information designated as "Official" or "work secrets" should not be considered for classification as state secrets. Limits on their disclosure should be found in the access to information law.
>
> Information relating to violations of the law or human rights, maladministration or administrative errors, threats to public health or the environment, the health of senior elected officials, statistical, social-economic or cultural information, basic scientific information, or that which is merely embarrassing to individuals or organizations should not be classified as a state or official secret.
>
> Information should only be classified as a state secret for a limited period of time where the release of the information would cause a serious harm to the interests of the nation. Information that is classified should be regularly reviewed and have a date after which it will be declassified and released. It should be presumed that no information should be classified for more than 15 years unless compelling reasons can be show for withholding it.
>
> Governments should institute a review of all secret information over 15 years old and automatically declassify and release it. All information that was designated as secret by a previous non-democratic government should be declassified and presumptively released unless it is shown that its release would endanger the national security or be an unwarranted invasion of privacy.
>
> An independent body that is not part of the intelligence, military or security services should have oversight over classified information and ensure that the system is operating properly, receive complaints about improperly classified information and review and order the declassification of information.
>
> There should be sanctions for those who deliberately and improperly designate information as secret or maintain excessive secrecy.

The Protection of Information Bill contains clauses that are in line with international good practice and democratic imperatives, for example restrictions on the reasons for classification. Other aspects as mentioned in this submission could be strengthened so as to ensure constitutionality and adherence to international legal standards, norms and practices. The issue of offences and penalties also requires further mention.

The following international practices and experiences in this regard can be noted[xiv]:

- In the **United States**, there are no provisions on disclosure of state secrets. The closest law is the Espionage Act adopted in 1917, which includes limited prohibitions on the disclosure of defence information with the intent to harm the U.S. It is generally accepted that this does not apply to the publication of state secrets by newspapers, and there has never been a prosecution of a journalist or newspaper in the history of the law.
- In **Norway**, the duty of secrecy, defined in the Security Act and the Penal Code, does not apply to members of the public in general.
- In **Georgia**, the Law on Freedom of Speech and Expression says that the prohibition on publishing secrets only applies to officials and government employees.
- In contrast, the **Belarusian** Press Law bans the mass media from publishing state or other protected secrets.
- In **Austria**, the criminal code provides that state secrets are not violated when there is a justified public or private interest.
- In **Moldova**, Article 7(5) of the Law on Access to Information states that no one can be punished if the public interest in knowing the information is larger than the damage that can result from its dissemination.
- In **Georgia**, the Law on Freedom of Speech and Expression says that those who disclose state secrets are not liable 'if the purpose of disclosure of a secret was protection of the lawful interests of the society, and if the protected good exceed the caused damage.'

The OSCE provides the following recommendations on criminal sanctions for the breach of secrecy[xv]:

> Criminal and Civil Code prohibitions should only apply to officials and others who have a specific legal duty to maintain confidentiality. 'Whistleblowers' who disclose secret information of public interest to the media should not be subject to legal, administrative or employment-related sanctions.
>
> The test of public interest in the publication should become an integral part of jurisprudence on disclosure of information.

A final international example for consideration is that of **Canada** and the Security of Information Act C-36 2001. This Act was introduced as a revision on the Official Secrets Act that had been in place since 1939 and was viewed by some critics as 'out of date, complex, repetitive, vague, inconsistent, lacking in principle and overinclusive'[xvi]. Similar to the complex issues facing the Ad Hoc Committee in South Africa, the Canadians had difficulties with provisions on espionage and leaking information. The Security of Information Act addressed some of these contentions through new definitions and concepts. An example that is relevant to the South African case today is the manner in which offences related to prejudicing and harming the interests of the state are defined. The following extract explains:

The old *OSA*[2] created espionage offences where the Crown could prove that disclosure was for 'a **purpose** prejudicial to the safety or interests of the state' (undefined); the new *Security of Information Act*, in subsections 3(1)(a) to (n), defines that phrase in detail to include:

- Committing an offence punishable by two years or more to advance a political, religious or ideological purpose or to benefit a foreign entity or terrorist group
- Committing inside or outside of Canada a terrorist activity (importing that definition also from the Criminal Code)
- Interfering with a service or system, public or private, that has significant adverse impact on the health, safety, security or economic or financial well-being of the people of Canada or the functioning of any government in Canada (i.e. harming Canada's critical infrastructure)
- Impairing the military capability of the Canadian Forces
- Impairing or threatening the capabilities of the Government of Canada in relation to security and intelligence
- Impairing or threatening the capability to conduct diplomatic relations or international negotiations.

For the purposes of the *Security of Information Act*, harm is caused to Canadian interests if a foreign entity or terrorist group engages in any of these activities[xvii].

Through defining how harm is caused and what is understood as offences that prejudice the interest of the state, vague reference to harm and prejudice are contextualised and this allows for the more focused use of secrecy and the need to protect information.

Regarding disclosure offences, the Canadian Act provides offences for the disclosure of protected information by current and former employees of defined government entities[xviii]. There are no offences for the media or private individuals. Further, a public interest clause protects current and former employees from prosecution if information has been disclosed for the purpose of disclosing an offence or illegal activity[xix].

The above international examples have been provided as illustrations of the manner in which various states have used legislation to protect information and national security imperatives while at the same time securing vital rights and pillars of democratic governance.

9. Conclusion

It is our belief that this Bill requires significant amendment in order to align it with the Constitution, other intelligence legislation, and international democratic principles, norms and practices.

[2] Official Secrets Act

Furthermore, the Bill, as currently conceived, fails to address the needs articulated by the Ministry for State Security on the requirement for a new information protection mechanism. In the briefing given to the Ad Hoc Committee on the Protection of Information Bill on 7 May 2010, the need for a new information protection mechanism was explained as follows[xx]:

> The aim then is to provide a statutory framework which provides direction to those in government who are charged with information protection; substantially reduce the amount of state information that is protected from disclosure; provide more effective protection to that information that truly requires safeguarding; and to align the information protection regime with the values, rights and freedoms enshrined in the Constitution.

For reasons detailed in this submission, it is our contention that the Bill as currently articulated is unable to fulfil the aims as set out by the Ministry for State Security. Given the inconsistencies in the criteria for classification and the expanded definitions of intelligence and counter-intelligence, the Bill provides scope for more information to be classified and fails to provide coherence or clarity in what should be protected information. The use of expansive definitions and concepts such as national interest and national security creates room for more secrecy and does not guarantee transparency and public accountability.

We recognise the complexities associated with the need to protect sensitive information from disclosure and to guarantee constitutional imperatives. Thus, this submission drew from various international examples to present alternatives. There is no specific model that can be applied to South Africa that will take into account the particular security context of the State and its people, the ideological and historical interests and the political stakes. However, any legislation that can potentially limit public accountability and enhance the capacity of the State to restrict participation, transparency and accountability should be viewed with much circumspection. The rights enshrined in the Constitution are part of the highest law in the land and all efforts should be employed to ensure that the proposed protection of information legislation guarantees those rights and limitations where necessary are limited to the strictest degree.

We thank the Ad Hoc Committee for the opportunity to make this submission and wish the honourable members well in the difficult deliberations ahead.

10. Notes

[i] Speech by the Minister of Intelligence Services, LN Sisulu (MP), on the occasion of the Secret Services Budget Vote, National Assembly, Cape Town, 17 June 2003. Available online at: http://www.search.gov.za/info/previewDocument.jsp?dk=%2Fdata%2Fstatic%2Finfo%2Fspeeches%2F2003%2F03070113461001.htm%40Gov&q=%28+%28%28sisulu%29%3CIN%3ETitle%29+%29%3CAND%3E%28category%3Ccontains%3Es%29&t=L+Sisulu%3A+Intelligence+Services+Dept+Budget+Vote+2003%2F2004 (last accessed 21 June 2010)

[ii] http://www.duhaime.org/legaldictionary/S/Sedition.aspx

[iii] ISS Submission on Intelligence Governance and Oversight in South Africa: Ministerial Review Commission on Intelligence. Available online: http://www.issafrica.org/pgcontent.php?UID=4039 (last accessed 21 June 2010)

[iv] International Press Institute, February 2010. *WPFR: Africa Overview: No Light at the End of the Tunnel.* Available online: http://www.freemedia.at/index.php?id=78&tx_ttnews[tt_news]=4802&cHash=07f10e6635 (last accessed 21 June 2010)

[v] FXI Submission on Protection of Information Bill. Friday, 20 June 2008. Available online: http://www.fxi.org.za/content/view/198/1/ (last accessed 21 June 2010)

[vi] Miklós Harszti, *Access to information by the media in the OSCE region: trends and recommendations. Summary of preliminary results of the survey.* Vienna, 30 April 2007

[vii] Ibid

[viii] Ibid

[ix] US Executive Order 13,526 (USEO) issued by President Barack Obama, December 2009. Section 1.4

[x] [x] Miklós Harszti, *Access to information by the media in the OSCE region: trends and recommendations. Summary of preliminary results of the survey.* Vienna, 30 April 2007

[xi] Ibid

[xii] Ibid

[xiii] Ibid

[xiv] Ibid

[xv] Ibid

[xvi] Law Reform Commission Working Paper 49 quoted in *Backgrounder No.12 – Security Information Act,* April 2004. Canadian Security Intelligence Service. Available online: http://www.csis-scra.gc.ca/bckgrndrs/bckgrndr12-eng.asp (last accessed 21 June 2010)

[xvii] Ibid

[xviii] Ibid

[xix] Ibid

[xx] Presentation available on http://www.pmg.org.za (last accessed 9 June 2010)