THE SECURITISATION OF INFORMATION WITH REFERENCE TO SOUTH AFRICA'S PROTECTION OF STATE INFORMATION BILL, 2010

by

Mikela Ellinas

A mini-dissertation submitted in partial fulfilment for the degree

MASTER OF SECURITY STUDIES

in the Department of Political Sciences
Faculty of Humanities
University of Pretoria

Supervisor:
Professor Anton du Plessis

October 2016

© University of Pretoria

ABSTRACT

The aim of this study is to analyse whether or not information has been securitised in South Africa. The degree of possible securitisation is assessed to determine the consequences of this securitised situation for the information-security nexus in South Africa. This premise is based primarily on the introduction of the *Protection of State Information Bill*, *2010* (hereinafter the Bill) which forms the case study. The Bill is posited by the state as a contribution to the country's information society and an enhancement of security-law to allow the State to combat threats in the Information Age. However, the Bill has received fierce criticism as a detractor to the democratic project of South Africa.

The analysis of the paper is grounded in the framework of Securitisation Theory, derived from Critical Security Studies within the field of Security Studies. This theory explores the consideration of an issue or entity, as a security subject, ultimately removing the issue or entity from the public-political discourse. Accordingly, the study concludes that a partial securitisation of information has occurred in South Africa, but with justifiable defence and necessary cause. In spite of the often pejorative perspective of a securitised environment, this outcome is not necessarily detrimental to the democratic project. Not only does the proposed security law enhance the security of the country to facilitate the pursuit of national interests, it allows the state to compete more effectively and aggressively with its counterparts in the international milieu in the Information Age.

Key terms:

- Information access
- Information Bill
- Information security
- National interest
- National security
- Press freedom
- Securitisation
- Securitisation Theory
- South Africa
- State Information

© University of Pretoria

TABLE OF CONTENTS

© University of Pretoria

© University of Pretoria

© University of Pretoria

LIST OF FIGURES AND TABLES

© University of Pretoria

LIST OF ABBREVIATIONS AND ACRONYMS

ANC	African National Congress
BCM	Black Consciousness Movement
BBC	British Broadcasting Corporation
COMSEC	Electronic Communications Security
COPRI	Copenhagen Peace Research Institute
CSS	Critical Security Studies
DA	Democratic Alliance
FIFA	Federation International of Football Association
GCHQ	Government Communications Headquarters
GNU	Government of National Unity
ICT	Information and Communication Technology
IFP	Inkatha Freedom Party
IR	International Relations (as an academic discipline)
JCPS	Justice, Crime Prevention and Security
MAD	Mutually Assured Destruction
MISS	Minimum Information Security Standards
MNC	Multinational corporations
NA	National Assembly
NCC	National Communications Centre
NCOP	National Council of Provinces
NEC	National Executive Committee
NGO	Non-governmental organisation
NIA	National Intelligence Agency
NMF	Nelson Mandela Foundation
NPO	Non-profit organisation
NSA	National Security Agency
ODAC	Open Democracy Advice Centre
OIC	Office for Interception Centres

© University of Pretoria

OSISA	Open Society Initiative for Southern Africa
PAIA	Promotion of Access to Information Act
PMG	Parliamentary Monitoring Group
PMSA	Print Media South Africa
R2K	Right2Know
SAHA	South African History Archive
SAHRC	South African Human Rights Council
SANAI	South African National Academy of Intelligence
SANDF	South African National Defence Force
SANEF	South African National Editors Forum
SAPA	South African Press Association
SAPS	South African Police Service
SASS	South African Secret Service
SSA	State Security Agency
UK	United Kingdom
UNDP	United Nations Development Programme
USA (or US)	United States of America

© University of Pretoria

CHAPTER ONE

INTRODUCTION

1. Identification of the research theme

The world operates on a fast and formidable trajectory that requires actors within it to take cognisance of its changes and the consequences thereof. South Africa operates within this environment as a state and nation in the process of democratic consolidation, and as a *de facto* regional hegemon, a purported continental powerhouse in Africa, and a prominent player in the international arena. To sustain this projection as it interacts in a globalised environment, South Africa has to ensure the safety and security of its own national interests. To achieve this level of security, the intelligence services of the country have been expanded and restructured through a statutory and institutional overhaul in 2009[1]. As the process of intelligence-gathering relies fundamentally on information, so too has the information-security nexus been adapted to be more amenable to the 21st century security-demands of the state.

Part and parcel of this reformation was the introduction of the *Protection of State Information Bill* (hereinafter the Bill or alternatively the Information Bill) to Parliament in 2008 and again in 2010, with its promulgation pending. The seemingly sudden spotlight on security is notable and worth examining as South Africa recently celebrated 20 years of democracy. In light of this seminal piece of proposed legislation, coupled with the dramatic changes to the intelligence structures, South Africa is arguably a prime example of how certain issues are endowed with a security label, namely they become securitised. This concept stems from Securitisation Theory associated with Critical Security Studies (CSS) within the field of Security Studies. This study therefore examines whether information in South Africa has been securitised or not, by applying the theory to the Bill.

The 21st century has been heralded as the 'Information Age' owing to the abundance, accessibility and power of information, as well as the means through which it is disseminated in a globalised world. The innovations in information and communications technology (ICT)

[1] This process itself has been questioned by opposition parties, civil society actors, academics and affected role-players, as the extent of this overhaul and subsequent expansion – rationalised by the demands of national security – is viewed as detrimental to democratic consolidation of the state.

© University of Pretoria

have resulted in information dominating daily existence[2]. The world is commonly referred to as a globalised entity because of the closeness of communities, connected through trans-boundary technological phenomena and processes. The prominence of a variety of actors who wield power in this global village is also remarkable, with the dynamics of the distribution of power in the form of information posing a transformative threat to the *status quo*. Citizens no longer take the information received from public broadcasters at face value, and search for all manner of alternative sources of information to learn the truth and be better informed.

The *status quo* has also been affected by the changing state security environment. From a security perspective information becomes intelligence through a process of analysis and, in terms of the traditional security paradigm, the possession and protection of intelligence is a government priority. The intelligence milieu has become complex since the general public is more aware than ever before of state matters, government political processes and stakeholder decisions made on their behalf. On the one hand, the freedom to access state information is one of the most protected and used rights of democratic citizenry. On the other hand, even democratic states claim a right to protect information. The exercise of this right to access information by citizens and the right to protect information by the state respectively, has come under more scrutiny in the Information Age as those in power strive for a balance between openness and secrecy.

ICT developments in the 21st century have undeniably given rise to a situation where information has spread in a form that can be either virulent or benevolent. The Arab Spring protests[3] (2011) and the 'Occupy Wall Street' campaign[4] (2011) demonstrated the determination of the public to be more involved in the decisions of government, underscoring the positive ability of information to empower people. The case involving Edward Snowden

[2] The proliferation of media channels with daily 24-hour coverage of news and current developments; wireless internet sources with mobile accessibility; and the pervasiveness of social media, have all contributed to this.

[3] The Arab Spring protests refer to a series of uprisings that occurred during the Spring of 2011, in Arab states across North Africa and the Gulf. The term 'Arab Spring' was popularised by the Western media when a successful uprising in Tunisia emboldened similar anti-government protests in other Arab countries. The use of social media was rife and prominent in the spread of the protests, with information for the cause going viral (Totten 2014).

[4] Inspired by popular uprisings in the Arab world, Occupy Wall Street is a people-owned movement that began on 17 September 2011 in Manhattan's Financial District and that has spread globally. The movement is committed to "making technologies, knowledge, and culture open to all to freely access, create, modify, and distribute" (Occupy Wall Street: 2011).

© University of Pretoria

(June 2013)[5], the revelation of the UK and US global surveillance programme *Prism* (2014)[6] and the disclosure of the multi-state intelligence espionage through *Echelon* (2013)[7] exposed the detrimental aspects of both freedom to and the protection of information, and of the ease with which information can be gathered, publicised and exploited.

As this demand for more transparency propagates, there is a corresponding need for governments to protect sensitive state information. This represents the challenge of achieving a balance between openness (for democratic auspices) and secrecy (for national security), in the pursuit of national interests. States rely on intelligence to achieve national security and gain an advantage in international relations, which in essence is the pursuit of national interests. Contestation arises when the balance is skewed to the point of being deemed an existential threat to the state. Governments wishing to protect knowledge employ the adage of 'national security' to justify freedom of action and therefore the capability to remove access to information from the general public. Even in democratic states where transparency and accountability are prerequisites, governments are required to adopt measures to protect national interests and pursue policies that enhance national security. Comprehensive security legislation therefore becomes paramount for national security.

Considering the aforesaid, the aim of this study is to explore the concept of information in South Africa, in terms of its transformation, utilisation, accessibility and protection, in order to analyse whether or not information has become a security issue – and as a result has been securitised. The latter has as its referent object the Information Bill introduced in South Africa, which is analysed by applying Securitisation Theory.

---

[5] Edward Snowden, a former CIA contractor, exposed details of extensive internet, social media sites and phone surveillance by American and British intelligence, given his access to such information (British Broadcasting Corporation (BBC) 2014).

[6] The Snowden leaks revealed that the NSA, in a surveillance programme known as *Prism*, tapped directly into the servers of nine internet firms, including Facebook, Google, Microsoft and Yahoo, to track online communication. The UK electronic eavesdropping agency Government Communications Headquarters (GCHQ) was accused of also using *Prism* for similar purposes (BBC 2014).

[7] *Echelon* is a surveillance program involving all-encompassing high-speed computers and algorithms which ingest and sort key words and text scooped-up by a global network of satellites from undersea cables and land-based microwave towers. *Echelon* is supported by the US, UK, New Zealand, Australia and Canada, although the US and the UK deny its existence (Bomford 1999).

© University of Pretoria

The theoretical relevance of the study pertains to the validity and reliability of securitisation as an analytical tool when it comes to the issue and/or right of open access to information in a democracy. The practical relevance of the study is framed, on the one hand, by Currie's[8] (2003: 60) opinion that "if there is one right contained in the Constitution that symbiotically connects all other rights, it is the right of access to information"[9] and, on the other hand, by the Constitutional obligation[10] of state and government to limit specific rights in the overarching protection of the state and the people who reside within it. Specifically, the actions of the state to achieve this balance require examination, hence the focus on the Bill and the potential outcome of the securitisation of information.

2. Literature overview

The exploration of literature on the information-security nexus indicates an accumulation of scholarship converging on these core concepts and themes. The literature involves the fields of Strategic and Security Studies, along with the emergence of Critical Security Studies. In respect of the latter, most of the literature details the scholarship of the so-called Copenhagen School and the theory of securitisation, which are applied to the securitisation of information in South Africa. More specifically, the literature concerns the following sub-themes:

(a) Security Studies: The foundation of contemporary Security Studies stems from scholarship on international relations and the events of the second-half of the 20th century. Snyder (1999a; 2012a), Kolodziej (2005) and Fierke (2007) were instrumental in emphasising the military focus of realist propositions of security. At its core, traditional Security Studies focuses on the security of the state – actions of the state to ensure its own security and actions by other state actors that affect or influence this security. National security is the pre-eminent objective, thus protecting national interests and preserving the security of the nation. A vast body of scholarship has explored this concept of national security, especially what it represents, how it is formed, what it signifies and how it alters policy and international relations (see for example Wolfers 1952: Lantis 2002; Zelikow 2003; and Kirchner & Sperling 2010).

---

[8] Professor Iain Currie is a prominent expert on South African information, constitutional and administrative law and on the *Promotion of Access to Information Act, 2000* (Act 2 of 2000).
[9] Safeguarded in the Bill of Rights in section 32 of the *Constitution of the Republic of South Africa, 1996* (Act 36 of 1996).
[10] Section 36 of the *Constitution, 1996* (Act 36 of 1996) addresses the limitation of these rights.

© University of Pretoria

As bipolarity dissipated during the late-1980s and the landscape of war transformed, it became essential to consider that the security of the state could also be compromised by non-military threats. The resultant expansion of the concept of security involves the realisation that there can be more than one type of entity that needs to be secured, and that threats to these entities in terms of the horizontal broadening thereof, can emanate from non-military spheres. The vertical deepening of security also indicates that security is not the sole responsibility of, nor provided by the state, leading to the current notion that the actors who achieve or ensure security have transcended the state.

Authors such as Rosenau (1980), Ayoob (1997) and Aradau (2004) identified non-military or alternative areas influencing security. This approach emphasised the external locus of the threat to security, often pinning the state as the biggest source of threat to individuals. According to these authors, states have become the primary perpetrators of insecurity. The narrower theoretical approach of Strategic Studies encompassing realist scholarship that emphasises external military threats to the state still prevailed but CSS was introduced into Security Studies to accommodate the re-thinking of security.

As CCS scholarship emerged that included more issues and how security was to be achieved, for whom and by whom, certain scholars, known as the Copenhagen School, addressed the question of how these issues came to be thought of as and designated in terms of security. Although the main thesis of this School was to “question the primacy of the military element and the state in the conceptualization of security” (Buzan, Wæver & de Wilde 1998: 1), it also included the work of Constructivists who at an ontological and epistemological level challenged and deconstructed existing conceptions of international relations. Amongst others their focus was on the conception of security and how issues are framed. If security issues emanate from a number of spheres, it stands to reason that there is a decisive process that designates the term ‘security’ to them. As a rudimentary postulate: “Power holders can always try to use the instrument of *securitization* of an issue to gain control over it. By definition, something is a security problem when the elites declare it to be so” (Wæver 1995: 54; original italics). CSS explores not only the designation of security issues, but the extent to which securitisation can occur, who is responsible for this securitisation, and the consequences thereof.

© University of Pretoria

(b) Securitisation theory: Commencing with the writers of the Copenhagen School, the works of Buzan and Wæver (see below) were instrumental in providing the theory to conceptualise security and security issues during the post-Cold War era. Seminal works such as *People, States, and Fear: An Agenda for International Security Studies in the post-Cold War era* (Buzan 1991), *Securitization and Desecuritization* (Wæver 1995), and *Security: A New Framework for Analysis* (Buzan, Wæver & de Wilde 1998) prescribed the departure from the military emphasis and contended that the overuse of security as a symbol for potential military threats to the state (and the policies to ensure protection from such threats) perpetuated a nefarious idea of security. It was from this perspective that securitisation emerged in terms of which it was posited that certain actors are able to set the security agenda, ultimately to their own benefit.

By using Securitisation Theory, scholars such as Terry *et al.* (1999) and Hughes and Meng (2011) have explored the 'security' rationale of specific issues. In this respect securitisation entails the removal of an issue from the regular field of politics, allowing it to be addressed through security-related mechanisms of government. Conversely, scholarship emerged that theorised the desecuritisation of issues. For example, Booth (1991) provided the trajectory of this critique by offering emancipatory theories that moved the focus from state 'militarised' issues to the preferred solution of individuals being freed from the restrictions of the state. Ayoob (1997) and Aradau (2004) have similarly been critical of CSS, in the process questioning the appropriateness and application of it to non-Western situations. Lyotard (1984) and Alker (2005) also criticise CSS scholarship on its over-emphasis of and reliance on emancipation as the ultimate solution. However, this criticism is one-dimensional as no alternative solution is proffered.

In the post-Cold War environment of international relations more authors emerged who either contested or augmented the Copenhagen School, adding new directions to the theory. Consequently, a second generation of Constructivist scholars emerged. Authors such as Huysmans (1998a; 1998b) and Balzacq (2005) made significant contributions by offering a practical expression of securitisation in the 21st century and how this relates to non-military security issues. The notion that security is "made and re-made by human inter-subjective understandings" (Smith 2006: 39) is not a 'given' phenomenon or end-state to be achieved.

© University of Pretoria

(c) The information-security nexus: Along with the concept of security the centrality of the state also came under scrutiny with some scholars (see below) questioning the validity of its protection through measures made in the name of national security. The notion of national security is also contested and sensitive based on environmental conditionalities. The concept also becomes more complex as new factors emerge in the international landscape. This bears out the realist contention of Louw (1978: 17) that national security "is a concept that in a restless dynamic world has to be re-interpreted and adapted to changing conditions so as to be relevant and valid as a policy for action in each age". However, from a state-centric vantage point, it is the responsibility of the government to maintain a national security policy as an effective instrument and to integrate it into an effective national plan at both the levels of formulation and implementation.

More recently scholarship emerged that linked security and national security to information. Collecting, compiling and conserving state information is critical for governments; and intelligence (secretive state information) is vital to the functioning of the state. As much as governments must protect intelligence to achieve security, in a democracy they are obliged to allow public access to certain information as long as this does not compromise national security. The challenge is to determine how much and what kind of information can be accessed and made public. Lyon (2003) and Haggerty & Ericson (2006) elaborated on the methods used and how they have changed in the Information Age, a development that alters the barriers of security by either expanding or limiting the information an actor can gain from the targeted information society. In a democratic state the information-security nexus relies on accountability, transparency and accessibility. Haggerty and Samatas (2010: 2) explain that "accountability implies that citizens need access to a range of information about the actions of their representatives and a free pass to assess the behaviour of their government." In this respect, the information-security nexus has been explored extensively by, amongst others, Jones (1996), Bruneau (2008) and Ransom (2008). Their main emphasis and contribution reside therein that they espouse the importance of the accessibility and availability of information in democracies to ensure a culture of open and free communication at all levels.

The literature in this field differentiates between types of government as governance requirements differ between states. This has to be borne in mind since this thesis concerns

© University of Pretoria

democratic South Africa as it exists today, in contrast to its authoritarian past. In authoritarian regimes the intelligence services operate in terms of a counter-intelligence paradigm, that is "protecting the states' secrets from … anyone outside the central core of power, and as almost anything can be defined as a state secret, the scope of that which is to be controlled is immense" (Bruneau 2008: 516). In democratic societies the intelligence services are also active and arguably operate on similar levels as the former, but with legislative control and accountability that allow and promote access to state information[11]. In this way a balance is maintained between what should or should not be regulated and restricted because "without controls, information security is difficult, if not impossible, to apply in any environment" (Jones 1996: 15). It is evident that information law on security ameliorates the existing information society.

(d) Information security in South Africa: Given its recent history, information has become a sensitive issue in South Africa. For this reason South Africa has been and remains protective of its media operating in the robust information society[12]. In 2004, at the ten year mark of South Africa's democracy, prominent stakeholders in the media and press industry in South Africa analysed the situation to assess improvements in press freedom. In summation the former Chairman of Naspers,[13] Koos Bekker (2004: 147), indicated that "the newspaper industry has transformed in many significant respects over the last ten years and has benefited from … a new dispensation in which press freedom is protected by the constitution." This confirms the existence of a beneficial information-security regime in which the public has (some) access to state information and is able to exercise this right freely and fairly. Numerous security and information laws have also been promulgated, namely the *Promotion of Access to Information Act, 2000* (Act 2 of 2000) and the *Protection of Personal Information Act, 2013* (Act 4 of 2013), along with the tabling of the *Cyber Crimes and Cyber Security Bill, 2015.*

Given the advances made since 1994 with regard to freedom of information legislation, Vale (2003) and Africa (2009) explored the notion of secretive government and the dangers of this to South African democracy since "(a)ny reversal or even qualification of the fundamental

[11] South Africa operates a civilian intelligence service which is distinguished in its authority and purview.
[12] South Africa's first newspaper, *The South African Commercial Advertiser* established by Fairbairn and Pringle in 1824, achieved a victory over the colonial government when the principles of the freedom of the press were upheld in court Shaw (2001: 25); demonstrating the longevity of the free press in South Africa.
[13] Naspers is a multinational emerging markets media group with a big stake in the African media industry.

© University of Pretoria

rights provided for now will be subject to the test of constitutionalism" (Africa 2009: 23). Literature on South Africa's information society has since been transformed with the introduction of the Information Bill in 2008. The most incisive examination is Currie and Klaaren's (2011) report for the Nelson Mandela Centre of Memory under the Nelson Mandela Foundation (NMF). It details the progression of the Bill through the legislative process, compares its various versions, contextualises the legislation for a more thorough understanding of its aims, and assesses the current backlash. Critique of the Bill has also emerged from civil society groups (most prominently the Right2Know - R2K), media stakeholders, editors and journalists, and the general public. Prominent South African writers have expressed their concern, most notably Andre Brink, Nadine Gordimer, and Zakes Mda. Other authors who have contributed to the critique and the role of the media include McDonald (2011), Sparks (2011), Friedman (2013) and Yin (2013).

This literature overview covered the scholarship and contributions on Security Studies, Securitisation Theory and the Information-Security nexus, as well as on Information Security in South Africa. It is evident that this area of research requires further exploration as it begs many questions on government procedures and processes and on actions taken and policies implemented in the name of national security.

3. Formulation and demarcation of the research problem

The underlying research problem of this study concerns the ideal-type relationship between democratic values and the need to protect information when deemed in the interest of (national) security; in other words the balance between openness and secrecy. Accordingly, with reference to the Information Bill, the primary research question is: Does the Information Bill securitise information or not? Secondary questions that arise from the primary question are: How are information and (national) security related? What is the rationale of the Information Bill and how does it protect security-related information? Does the Information Bill politicise, securitise and/or desecuritise information and who is responsible for this? What are the consequences of this development for South Africa's (national) security? Is Securitisation Theory an appropriate theoretical framework to explore securitisation through an act or bill?

© University of Pretoria

The primary assumption in response to the main question is that information has been partially securitised through the introduction of the Information Bill without necessarily hindering the development of democracy or detracting from democratic norms regarding information access. The secondary assumptions in response to the subsidiary questions are: that information and security are inextricably linked in the Information Age to the extent that the apparent incommensurability of the security of information and public access to information has reached unprecedented levels; that the rationale of the Bill is to transform the South African intelligence environment with the inclusion of provisions for information security if in the national interest; that the state, aided by fortuitous conditions, is the main agent of the securitised information environment and that the Bill is indicative of a partial and qualified securitisation of information, to be completed when and if the Bill is promulgated; that this securitisation is not necessarily a pejorative outcome for the local information society, but rather that the Bill contributes to an overarching national security paradigm; and that Securitisation Theory is a valid analytical tool to explore securitisation through a bill or act.

Accordingly, the objectives of this study are to:

- explore the information-security nexus in conceptual and practical terms, and to present, explain and critique Securitisation Theory as a means to analyse this relationship;
- describe the official framing of information and security in the South African context and to provide an overview of the origins and rationale of legislation (the Information Bill) to protect information;
- apply the elements of Securitisation Theory to the Information Bill to determine the nature and scope of the securitisation, if any, of information through this Bill;
- assess the consequences of the research findings for South African democracy;
- evaluate, based on this case study, the appropriateness of Securitisation Theory to explore practical manifestations of securitisation.

The study is demarcated in conceptual, temporal and practical terms. At a conceptual level the study is confined to the concepts security, national security and information, and to Securitisation Theory as an analytical tool. The specific time-frame of the study covers events

© University of Pretoria

between 2007 and 2016; that is from the initial conception of the Information Bill to subsequent developments. For background and contextual purposes reference is made to earlier antecedents and developments. Since the research focuses on the Information Bill, and apart from passing references to generic international examples, the study is limited to the South African case study.

4. Methodology

The study adopts a qualitative approach to the theory of descuritisation in relation to the issue of information. The research design is that of a two-pronged explorative literature-documentary study involving a theory-based case study grounded in academic literature and official documentation. The theoretical approach, within the broad ambit of CSS but not excluding selected and compatible elements of realism and liberalism, is based on the seminal contribution on securitisation of Wæver (1995). The tenets of Securitisation Theory are applied to the South African case study. The general approach of the study is descriptive-analytical. The method of the study is empirical in that it concerns proposed legislation; inductive in that general inferences are based on factual particulars; and qualitative in that a reasoned assessment is made. Due to length constraints the study is non-comparative.

Use is made of primary and secondary data sources. The primary data sources are public domain documentation and viewpoints of an official nature. The Bill itself provides the most substantial source of information but official documentation related to it is also used, such as media statements released by government; transcripts of parliamentary debates and standing commissions that assess the revisions to the Information Bill; and existing legislation that informs the passage of the Bill. These are supplemented by secondary sources captured from media reporting; opinion pieces by prominent public figures; and scholarly works in the form of books and journal articles that pertains to themes of the Bill.

5. Structure of the research

The study consists of five chapters that present a progression of the argument from the identification, formulation and demarcation of the research theme and problem, through the description and analysis of the case study, to a concluding evaluation of the research findings and subsequent recommendations.

© University of Pretoria

Chapter One - Introduction: As a general introduction this chapter identifies the research theme, provides a literature overview, identifies and demarcates the research problem, explains the research methodology and indicates the structure of the research.

Chapter Two - Security, information and the securitisation of information: select theoretical perspectives: This chapter provides a brief overview of the development of security theories and the inputs on the *security* concept by prominent scholars. This is extended to the information-security nexus, with the aim to determine what kind of information is drawn into the security domain. As a framework for analysis, specific attention is paid to the Securitisation Theory of the Copenhagen school, highlighting its tenets, its progression and the critique of the theory, including counter-arguments for desecuritisation.

Chapter Three - The *Protection of State Information Bill, 2010* in the South African information-security landscape: a contextualisation: This chapter provides an overview of the political-security landscape of South Africa at the time that the Bill was introduced and indicates the progress that has been made towards upholding the right to freedom of information. This is followed by a detailed discussion of the Bill, with the inclusion of its introduction; the related legislative process; its key provisions; and the critique of the legislation.

Chapter Four - The *Protection of State Information Bill, 2010* and Securitisation Theory: An analysis: This chapter analyses the Information Bill in terms of the conceptual-theoretical framework of Securitisation Theory. As such and in respect of the Bill it covers the theoretical elements of the securitising speech act; the securitising move which involves the presentation of an existential threat or not; the persuasion of the audience by an authoritative securitising agent; and the significance of historical context. In conclusion an assessment is made of whether or not securitisation has occurred and, if so, to what extent and with what impact.

Chapter Five - Evaluation and recommendations: This chapter serves a two-fold purpose. Firstly, it summarises and evaluates the research findings in order to assess the extent to which the research objectives were realised, the research questions were answered and the research thesis was verified or falsified. Secondly and based on these findings, it makes policy recommendations and suggests areas of future research.

© University of Pretoria

6. Conclusion

In the 21st century, information is a vital commodity given its contradictory ubiquity in daily life, offering both the freedom to know more and the power to control more. As a result of the current fluid nature of international relations, state actors are exposed to a greater range of threats originating from more varied sources. To mitigate this resultant vulnerability, states pursue strategies to protect their national interests and national security. This includes the regulation of access to information, to a point where it may arguably constitute the securitisation of information.

This securitised development may appear nefarious from actors outside the decision-making core of the state, but securitisation is often necessary and can be justified to fulfill national security. In South Africa, this negative perception is emphasised when juxtaposed with the history of the country and the current, relatively new democratic state. Information itself is a sensitive concept and a contested space in the democratic project. The underlying theme of this study is to determine whether information itself (or the access to it) is threatened.

Based on the aforesaid identification of the research theme, the literature overview, the identification and demarcation of the research problem, the indication of the research methodology and the structure of the research, attention is forthwith given to conceptual and relational dimensions of the security-information nexus. The objective is to clarify the core and related concepts and to provide a theoretical framework that can be applied to explore, describe and explain the South African case study.

© University of Pretoria

CHAPTER TWO

SECURITY, INFORMATION AND THE SECURITISATION OF INFORMATION: SELECT THEORETICAL PERSPECTIVES

1. Introduction

The aim of this chapter, being an extended and critical literature review, is to provide a conceptual and theoretical framework to contextualise information within the ambit of national security. It examines the contemporary development of security thinking and its impact on the information-security nexus; and provides an account of Securitisation Theory and of its underlying assumptions, elements and critique. In explaining the theory of securitisation, attention is paid to various schools of thought, namely the Welsh, Copenhagen and Paris Schools who contributed to the tenets, progression and critique of security theories in International Relations (IR). The main section of this chapter focuses on the theory of securitisation and desecuritisation. The chapter concludes with an assessment of the concept of information in Security Studies, focusing on the information-security nexus, to determine what kind of information is drawn into the security domain.

2. The changing nature and scope of Security Studies

Since the mid-1980s the study of security underwent radical change that was a result and reflection of the evolving nature of the international system. In this respect the ending of the Cold War (1989/1990) represented a watershed moment in time that signified a near-paradigmatic shift between so-called ‘old and new’ security thinking.

2.1. Traditional Security Studies

Prior to the 1980s and within IR, scholars approached the study of security through the outlook of the discipline of Strategic Studies, mainly due to the primacy of military affairs. Although alternative conceptualisations of security existed, they were overshadowed by state-centric militaristic thinking and thus not exposed in the mainstream discipline until the end of the Cold War. Accordingly, international relations were seen to be conducted by state actors whose principal objective was to secure sovereignty and territorial integrity and to anticipate the threat of war by external state actors. Hence Wæver’s (1995: 49; original italics)

© University of Pretoria

viewpoint: “Security is influenced in important ways by *dynamics* at the level of individuals and the global system, but not by propagating unclear terms such as individual security and global security. The *concept* of security refers to the state.” This mind-set, by implication, emphasised the concept of national security which became the rationale of state actors and the justification of their actions. As confirmed by Buzan (1991: 11): “The appeal to national security as a justification for actions and policies which would otherwise have to be explained is a political tool of immense convenience for a large variety of sectional interests in all types of state”.

Considering that national security emanated from the military power of state actors and their disposition to equate security with military defence, states amassed large defence forces to combat military threats on land, sea and in the air, and to secure themselves against external military threats which increased with the introduction of nuclear weapons. The possession of nuclear weapons provided the ultimate security to states, through the posture of Mutually Assured Destruction (MAD) and the zero-sum nature of the nuclear threat/power. The possession and potential use of nuclear weapons framed the perception of security during the Cold War. The strategic thinking and school of thought representative of this state- and military-centric approach, ultimately ensconced as the dominant theory in Strategic Studies, became known as Traditional Security Studies. As (what were deemed) alternative theories became prominent; an umbrella field of Security Studies emerged under which all notions of security could be studied, divided into further sub-sections whereby specific security assumptions could be addressed. Important to note for the theoretical distinctions that ensued is that “security studies and strategic studies differ not in their basic assumptions about how the world works but in what we consider security threats” (Snyder 2012a: 4).

The transformed playing field at the end of the 20th century demanded the adaptation of disciplines to remain relevant in the globalised world. This reconceptualisation of security was critical as “globalisation requires a much more nuanced and subtle notion of security than was needed when the world was essentially divided into two main blocks” (Smith 2006: 33). While Snyder (1999b), Kolodziej (2005) and Fierke (2007) were instrumental in pointing out the military focus of realist propositions of security – considering that “(o)ne of the distinctive elements of strategic studies has been its focus on military strategy” (Snyder 1999a: 3) – it

© University of Pretoria

became evident that the militaristic statist view of security was too narrow to address new threats and security issues. This had profound consequences for the language of IR beyond the 20th century, as traditional concepts were re-evaluated. As Snyder (2012a: 9) indicates, the very existence and relevance of security (strategic) studies depended on the redefinition of security, with a necessary "shift in thinking about security, in particular, the relevance of security as the primary goal of states".

Initially, the arena from which threats to security (viewed from the perspective of different actors) could emanate was horizontally broadened to include non-military issues. Arguably the most seminal contribution on this was that of Buzan (1989), who initiated the idea that threats could emerge from "five sectors: military, political, economic, environmental and societal" (Buzan 1991:15). Buzan and other scholars (e.g. McRae & Hubert 2001 and Thomas 2004) also advocated for a broadened agenda of security, but nevertheless maintained the primacy of the state as the object to be secured (i.e. the referent object of security). Furthermore, contributions emerged that broadened the security agenda by adding (hitherto dormant) issues, analysed through traditional perspectives, for example those of Roberts (1990) on human rights; Weiner (1992) on migration, and Levy (1995) on environmental security.

2.2. Critical Security Studies

The new approach to security espoused 'critical' theories that examined the root of key concepts in disciplines, as opposed to merely accepting them as a-historical and a-social 'assumptions'. Within the field of Security Studies this approach – amongst others representative of the so-called Welsh School – culminated in what became known as Critical Security Studies (CSS). Valuable contributions to CSS were made by Booth (1991), Krause and Williams (1997), and Wyn Jones (1999) who were instrumental in providing the foundations from which alternative ideas expanded, creating a wave of critical theories that have at their core a circumstantial and subjective conception of security. Thus CSS encouraged the questioning of "the primacy of the military element and the state in the conceptualization of security" (Buzan, Wæver & de Wilde 1998: 1). As contended by Fierke (2007: 1), "(t)hese critical approaches have highlighted the politics of security rather than just the military dimension", ensuring that Security Studies and security studies remain relevant in the 21st century.

© University of Pretoria

To give effect to the expansion of the scope of the new approach, Wyn Jones (1999: 166) describes the core of CSS as "broadening, deepening, extending and focusing." A literal summation of these terms is provided by Peoples and Vaughn-Williams (2010: 17): 'Broadening' refers to a conception of security studies that includes a range of issues beyond military force under the rubric of security. 'Deepening' implies a theoretical approach to security that connects understandings of security to deeply rooted assumptions about the nature of political life more generally. 'Extending' denotes the expansion of the security studies agenda to recognise not only a multiplicity of issues, but also a multiplicity of actors beyond the state as sites of insecurity including, most fundamentally, individual human beings. Finally, CSS claims to provide an approach to security that is ultimately 'focused' in the sense that it is grounded in a particular normative goal: that of human emancipation.

Given the contested nature of the security concept, dissention exists in and amongst scholars in different European schools, as their focuses vary on what should be included in a security conceptualisation, who should conduct security and what the ultimate goal of security entails. The following sections explore the principles, proponents and problems of these theoretical schools, concluding with thoughts on the application of CSS to national security.

2.2.1. CSS principles, exponents and schools of thought

The 'critical security studies' developed by Booth (1991) was influenced by the Gramscian[14] and Frankfurt school or tradition of 'critical theory', making a distinction between 'critical theory' and 'problem-solving theory' (Bilgin 2008: 92). Problem-solving theories approach a situation as a given, without reflecting on how this problem came to be; hence these theories aim to find solutions based on the existing reality. In contrast, critical theories by their very definition are critical of existing structures, systems and methods of thinking as a means to an alternative and better end. These ideas draw on Max Horkheimer who distinguished between 'traditional theory' and 'critical theory'. Traditional theory is seen to be rigid in its conceptions, with embedded ideas that need to be approached as such; critical theory rejects the notion of

[14] Robert Cox re-introduced IR scholars to the work of Antonio Gramsci, adopting a critical approach to theory.

© University of Pretoria

such stringent conceptions and posits that the theorists cannot be separated from the world they are analysing (Bilgin 2008: 93).

As a derivative of this critical theory disposition, emancipation is central to CSS being the ultimate objective of security. Booth (1991: 319) equates emancipation with security because "emancipation, not power or order, produces true security". For this reason states should recognise that emancipation is posited as the end-goal of security; and that all security concerns (policies, actions, approaches) should be focused on the emancipation of society. However, this does seem abstract in that laws and prohibitions (traditionally set and implemented by the state) are required to prevent anarchy. Did CSS not emerge as a response to exceptional situations? Emanating from the study of emancipation, it is necessary to question the type of freedom that ensues. Freedom and survival are two concepts explored by this school of thought, as society is not meant to simply survive but actually thrive. Hence the argument that "(s)urvival merely implies the continuance of existence in conditions where life is threatened, whereas security denotes a genuine absence of threats and the consequent maximisation not only of an individual's life-chances but also of their life-*choices*" (Peoples & Vaughn-Williams 2010: 25; original italics).

Within CSS several 'schools' of thought emerged that proffered a distinct approach to security thinking. The two most dominant schools were the Welsh School and the Copenhagen School, so named for their places of origin[15]. Both schools agreed on the need to expand the sectors or topics of security, but differed as to the deepened nature of security and the role of the state in political affairs. The Welsh School proposed politicising issues as opposed to securitising issues "so as to be able to de-centre the military and state-focused threats that dominate traditional security agendas" (Bilgin 2008: 98). This is in contrast to the calls for desecuritisation made by the Copenhagen School who believed that "those issues that are labelled as 'security' concerns will be captured by state elites and addressed through the application of zero-sum military and/or political practices, which may not help address human insecurities" (Buzan, Wæver & de Wilde 1998). The Copenhagen School termed the latter

[15] Ken Booth and Richard Wyn-Jones attended the University of Wales, in Aberystwyth; Ole Waver and Barry Buzan were linked to the Copenhagen Peace Research Institute (COPRI).

© University of Pretoria

process ‘securitisation’, as a means to remove specific issues from the regular realm of politics, implying less restraint on decision-makers and less concern for public opinion. The Copenhagen School postulates that “the articulation of urgency and extreme measures is what establishes a boundary between ‘security proper’ and concepts that bear only a semantic resemblance to ‘security’” (Buzan & Hansen 2009: 215), thus inculcating securitisation.

A third, less publicised school of thought, is the Paris School[16] which adopted a more sociological approach by “concentrating on how security practices are conducted across a range of different contexts, and often in ways that diminish any supposed distinction between internal (policing) and external (military) security” (Peoples & Vaughn-Williams 2010: 10). Post-structural exponents of the Paris School focused on the ‘action’ aspects of security, questioning “how security practices are conducted across a range of different contexts, and often in ways that diminish any supposed distinction between internal (policing) and external (military) security” (Peoples & Vaughan-Williams 2010: 10). The scholarship of the Paris School strongly rejects the idea of emancipation as the core of security thinking, as it creates a reliance of the nation on the state mechanism and perpetuates the domination of the nation by the state. For this reason post-structuralists posit “society as the referent object (to) underscore the appeal of these advocates to collective identity and a subtle widening of the understanding of institutions” (Mutimer 1999: 24).

A major point of criticism of CSS is this division of schools of thought as it leads to the exclusionary categorisation of ideas. This kind of ‘mapping’ can have limiting effects for any deviations and expansions of specific ideas, regardless of how organised a structure it seems to propose. Another criticism is the Euro-centric perspective offered by the CSS schools, which is seen as blatant opposition to the traditional security conceptualisations offered by Security Studies – and more specifically Strategic Studies – and which is dominated by US scholarship (Peoples & Vaughn-Williams 2010: 10). This critique is relevant to the study of security in general, in that it cannot be viewed impartially and must be contextualised.

[16] This approach is named for scholars working at the Paris Institute of Political Sciences.

© University of Pretoria

By traversing the political-security spectrum beyond securitisation, desecuritisation becomes prevalent. Desecuritisation moves away from the securitisation of non-military issues and even the militarisation of politics that have come to dominate both post-Cold War international relations and IR. This trend emerged during the 1990s when Booth (1991 & 2005), as an exponent of the Welsh School, offered emancipatory theories to move the focus from 'militarised' issues, premised by the state, to individuals freed from the restrictions of the state. Similarly, Ayoob (1997) and Aradau (2004) were also critical of CSS with respect to the position of states and peripheral actors, but remained wary of the emphasis on emancipation and how this relates to non-Western situations. Lyotard (1984) and Alker (2005) also criticised CSS due to its over-emphasis of and reliance on emancipation as the 'ultimate solution'[17].

2.2.2. Alternative propositions to CCS

Taking cognisance of the acceptance of a broadened security agenda in IR, various scholars explored the idea of a deepened concept of security which questions the notion of what needs to be secured, i.e. the referent object of security. Authors such as Rosenau (1980), Ayoob (1997) and Aradau (2004) identified alternative levels of influence, as it became common practise to view the state as the main cause of insecurity. These ideas gained credence as a narrative of the prominence and protection of the individual and therefore societies became paramount. A watershed moment was the 1994 report of the United Nations Development Programme (UNDP) that presented the idea of 'human security' as the focus of its work (UNDP 1994). The idea that the individual's security needed to be the primary focus of state actions, through non-military means, became the foundation for development thinking in the new millennium and also had a profound effect on security thinking.

In spite of these developments, mainstream scholarship of Security Studies was not as susceptible to these new ideas. The argument was that these expansions of security "would destroy intellectual coherence and make it more difficult to devise solutions to any of these important problems" (Walt 1991: 213). Apart from drawing attention to the theoretical limitations of these ideas, the impracticality of including any issue on the security agenda that

[17] See also Frisch 2002 for further scholarship on the critique of emancipation theory.

© University of Pretoria

could threaten the individual (as the referent object of human security) was stressed. This is in contrast to those who contend that CSS is for "the voiceless, the unrepresented, and the powerless, and its purpose is their emancipation" (Wyn Jones 1999: 159)[18]. Thus the concept of security remains contested and complex.

Consequently 'security' has become a grey area of study, with little definitive separation of what constitutes a security threat or not, and how a security threat should be resolved and by whom. With reference to the previous distinction between 'old' Traditional Security Studies and 'new' CSS, the field of study and accompanying theoretical approaches were divided into Security Studies, which encompassed a broader and deepened perspective by analysing all forms and levels of security, and Strategic Studies with its narrower focus on external military threats to the state. Even after the Cold War there was confusion and uncertainty in IR as few theories dominated on security thinking by indicating future directions.

In a discipline that studies human behaviour, society and systems, complete impartiality is unattainable. Subjectivity and partiality characterise the study of security as the subjects of the study are *themselves* subjective and partial. Wæver's (1995: 51) justification of a new approach is that "politicians already use the term (security) in relation to problems that are non-military in character but are still regarded as existential threats to the political order – the state". For this reason it is crucial to have a clear understanding of the study of security and its conceptions, as the term is used widely to refer to a broad range of objects and subjects in common and scholarly language.

2.3. Security and national security in the Information Age

As an introduction to the 21st century, the events of 11 September 2001 (9/11) and the actions and reactions that followed would come to define subsequent international relations and IR. With all the doubts and criticism that abounded about CSS, the events of 9/11 substantiated the critical approaches to thinking about security, adding a renewed relevancy to the discipline. Bilgin (2008: 90) sees the context of 9/11 as the event that "underscored the need to engage directly with issues related to war and peace, hard and soft power, state and non-

[18] For a thorough and contemporary criticism of CSS, see Hynek & Chandler 2013.

© University of Pretoria

state actors in world politics" (see also: Peoples & Vaughn-Williams 2010: 7). However, the sequence of events on 9/11 and thereafter have led to a re-introduction of realist elements and neo-realisms into local and global politics.

A particular notion of security materialises from background, circumstance, objective and resources, and these factors determine the actions to assure or achieve this particular idea of security. Hence the relevancy that "the formula of the national interest has come to be practically synonymous with the formula of national security" (Wolfers 1952: 482), where actors justify their actions using a 'national security' defence in order to pursue or protect 'national interests'. Understanding the national interests of states (and the values that guide them) provides a clearer perspective of national security, and what actions (or non-actions) states will justify in order to secure or enhance their security.

2.3.1. National interest and national security

Traditionally, national security was defined "as the condition of freedom from external physical threat which a nation-state enjoys" (Louw 1978a: 10). Presently, this definition is limited as threats to the state can emanate internally and are not always physical forms of aggressive action by an external actor. As indicated, threats and responses to threats to national security are multi-faceted. Nonetheless, for Buzan, Wæver & de Wilde (1998: 36), security is fundamentally about survival: it comes into play when an issue is represented as posing an *existential threat* to the continued survival of a referent object.

Thus, for a state the "pursuit of national objectives becomes the cause and purpose of all the actions of a security nature that a nation undertakes" (Barber 1978: 43). The state's *raison d'être* becomes geared, directly and indirectly, towards securing the national interest which is ultimately linked to a guarantee of national security. Although national security is an ubiquitous and all-encompassing concept, it remains exclusive to a particular state and its interests. In the Information Age it is vital that states re-assess their interests, particularly as the paradox of power continues to shift and more distinctions need to be considered – specifically those between hard and soft power (Nye 1999: 24). The notion of national security requires constant revision, because "the information revolution has redefined who can pose a significant threat by diffusing and redistributing power to traditionally weaker state actors and

© University of Pretoria

non-state actors, empowering them to do harm" (Goldman 2004a: 2). The idea of national security and the generic use of security in foreign affairs becomes portentous for the actions of actors as they navigate the globalised landscape.

Another dynamic to consider in the Information Age is the involvement by and interest of the general public, having become more pronounced as information is almost instantaneously communicated across the globe. The abundance and accessibility of information is almost boundary-less to the point that "the information revolution has redefined what it means to be vulnerable by making the most advanced societies the most vulnerable to attack, simply because they are more information dependent" (Goldman 2004a: 2). In this vein, citizenry continues to be concerned about the undertakings of their government and its national security policy (and those of foreign counterparts), using the freedom of information on the internet and related technology to demand more transparency and accountability of the state. "Accountability implies that citizens need access to a range of information about the actions of their representatives and a free pass to assess the behaviour of their government" (Haggerty & Samatas 2010: 2), making this phenomenon more effective in democratic states where principles of accountability and transparency are systemic.

Notwithstanding this generalisation, the pervasiveness of the internet and the information it delivers was exemplified by the Arab Spring in 2011. These events dismantled the established notion that only democratic states enable robust action, emphasising the point that (oppressed) citizenry the world over are making use of the technological and digital platforms available to demand more access to information. The Arab Spring demonstrated the willingness (that heretofore had been dormant and inaccessible) of citizenry to use the resources available to them to publicly disseminate new information. Consequently, fewer boundaries and even less limitations exist on what the general public considers to be within their jurisdiction.

From the perspective of the citizens of a democratic state, accountability and transparency are prerequisites for an effective state, although this is not always achieved. Even within a democratic system the amount of information to which the citizenry has access and the degree of influence the public has over government behaviour, are determined by the state because "freedom of information is an ideologically-determined political instrument that can

© University of Pretoria

be deployed to achieve a range of different agendas" (Darch & Underwood 2010: 4). On the one hand, it is accepted that government has the right to restrict public access to specific state information; in this respect, the pervasiveness of the internet and its propagation of information have prompted governments to take extra precautions. On the other hand, both citizens and government have particular roles and accordingly are responsible for democratic consolidation; while citizens must conduct oversight of government as well. To optimise governance, governments must pursue equilibrium between transparency and secrecy, to ensure democracy and national security.

2.3.2. The national security role of government and the nation

At its apex the government-citizenry information-relationship is reliant on trust, namely that the decision-makers will harbour information as necessary, and by the same token not abuse extraordinary power by expediently restricting access to such information. This relationship entails a level of secrecy that automatically denotes the possibility of surreptitious behaviour. As Africa (2009: 17) warns, because of "the potential for abuse (that)…(s)ecrecy carries, citizens must be assured that there are clear parameters and policy guidelines for the exercise of secrecy and transparency." If trust exists, citizens will more willingly rely on their government to act on their behalf and in their favour, thus allowing more freedom on the part of the decision-making elite.

To guarantee national security, extraordinary measures are adopted, often to the short-term displeasure of the general public. Notwithstanding that "public support is central to how a democracy organizes itself for national security" (Goldman 2004a: 7), public approval and a legitimate and accepted cause in the name of the national interest is necessary (and desired) for policy to be implemented. As government is privy to confidential information, "the policy process that guides security is closed off from open and public contestation by calls to nationalism, or nation-building, or national interest" (Vale 2003: 20). What remains to be tested from the citizen-government dynamic is whether or not this trust is exploited by government.

The national security policy of a state is formulated by the government and is usually not particular to one administration (that holds office for a limited term) but rather remains

© University of Pretoria

embedded in the over-arching strategy of the country (Goldman 2008: 43). As a rule, security policy only alters with radical regime change. For example and in the case of South Africa, security policy was only adjusted after 1994 to align with the values and interests of the new polity, as the security concerns of the new regime contrasted from those of the previous regime. This verifies Barber's (1978: 37) assumption that "security policies reflect the traits and values of a nation's citizens and institutions, and tend to take on the characteristics of the overall policies and procedures that guide the affairs of government."

Strategies are formulated on the basis of policies. A lack of a security policy is an indication of a greater lack of nationhood and of values to which a country subscribes. With reference to the necessity of a national security strategy, retired US Army Colonel David Peddle (quoted by Engelbrecht 2011) confirmed that "every reasonable country has one, after defining what their vital interests and national interests are (as) this strategy will then allow for a calculated and proportional response to any real or perceived threat to the state." It is essential for a state to implement a comprehensive and adaptable national security policy, an imperative that becomes more critical when state insecurity results from the uncertainties of today's globalised world. Determining what issues to address is explained in terms of Securitisation Theory.

3. Securitisation Theory

Securitisation Theory explains the process of how an issue becomes a security issue and the consequences of this process. Wæver (1995) was one of the original founders of this theory, not excluding the contributions of Buzan (1989) and de Wilde (along with Buzan and Wæver, 1998). Since they form the basis of the framework that is applied in this study, the core assumptions, features and elements of this theory – also summarised and critiqued by Peoples and Vaughan-Williams (2010) – are forthwith discussed.

3.1. Assumptions and elements of Securitisation Theory

The core assumption of Securitisation Theory, as a point of departure, is that a particular matter or subject becomes a security issue when it "is presented as posing an existential threat to a designated referent object" (Buzan, Wæver & de Wilde 1998: 21). This existential threat is the product of a subjective judgement, as dissimilar referent objects will be threatened

© University of Pretoria

differently. By labelling this issue posing a so-called existential threat as a 'security issue', it is elevated above other non-security or political issues, removed from the general political spectrum and placed within the security realm. In addition, by creating this perspective of the issue, the approach to it changes as "an agent claims a need for and a right to treat it by extraordinary means" (Buzan *et al.* 1998: 26). It is this exceptional status that is contentious, as the issue is no longer openly dealt with in the public domain and all pretentions to transparency and general legitimacy - when under public scrutiny - are eroded.

Based on and as an extension of this core assumption, Securitisation Theory contains additional conceptual elements that are deductively linked. These conceptual elements, amongst others, are the referent object, securitising actors, the speech act, the securitising move and extraordinary measures. Buzan, Wæver & de Wilde (1998: 36) provide a concise definition of these concepts and their relationship: the referent objects are things (ranging from the state to the individual and from the political regime to the environment) that are seen to be existentially threatened and that have a legitimate claim to survival. The securitising actors are actors (possessing authority or power) who securitise issues by declaring a referent object existentially threatened. This declaration is done in the form of and in fact constitutes a speech act, whereby "the utterance itself is the act" (Wæver 1995: 55). This explicit claim alludes to the argument of Wæver, mentioned above, that 'security' is already utilised in various forms by political practitioners, who designate a security issue by referring to it as such.

As a core component of securitisation theory, the speech act occurs "when an issue not previously thought of as a security threat comes to be *spoken of* as a security issue by important political actors" (Peoples & Vaughan-Williams 2010: 78; original italics)[19]. However, the speech act itself is not sufficient to claim securitisation, but forms part of the securitising move.[20] Three conditions must be present for this move to be complete, namely the presentation of an existential threat to legitimise the use of extraordinary measures to combat that threat; a securitising actor who is in a position of authority to convince an audience of the severity of

[19] 'Speaking security' as a speech act draws on the Speech Act Theory of Austin (1962) who posits that many utterances are equivalent to actions, therefore the speech act is a move towards securitisation.
[20] For a re-evaluation of Speech Act Philosophy and how it relates to the evolution of Securitisation Theory, see Balzacq 2011b.

© University of Pretoria

the issue and the necessity for such extraordinary measures; and any historical connotations that relate to the issue and emphasise the need to securitise (Peoples & Vaughan-Williams 2010: 79). When the target audience accepts that extraordinary measures are required to address an existential issue that finds similarities in history, the securitising move is complete.

The required legitimacy of the securitising agent's authority depends on the type of government in charge. This authority will also determine the ease by which the audience can be persuaded to accept the presentation of an existential threat, because "the issue is securitized only if and when the audience accepts it as such" (Buzan, Wæver & de Wilde 1998: 25). An autocratic government does not require audience approval in the decision-making process whereas a democratic government must gain public approval (through electoral processes, the conviction of constituencies, the rule of law) to apply extraordinary measures to an issue to complete the securitising move. This has become more difficult in the Information Age, considering that people have become empowered by instant and pervasive knowledge. In this way, a dialogue is created, providing a further platform from which the issue will be addressed, and thus influencing the decision-making process. In this way, the issue is politicised.

The difference between the politicisation and securitisation of an issue can be understood by allocating it a position on a spectrum (Wæver 1995 & 2011) based on its severity (or security-ness). The process of securitisation can be thought of as an issue traversing a spectrum, changing its status as it is purposefully moved by political agents and decision-makers to different points. Each phase offers different consequences and outcomes for the issue and the situation at hand. Although some issues intrinsically may be non-political, an issue commences in the 'politicisation phase' being in the public domain, as no issues that require state action can be considered neutral. Once the authoritative agent removes this issue from the public discourse and mobilises state resources to address it, it becomes set in the 'securitisation phase'. When an issue has moved beyond the point of being addressed in terms of security, it enters the 'desecuritisation phase' where it becomes delinked from a security conceptualisation and returns to the public and political domain (see Figure 1 below).

© University of Pretoria

Figure 1: The securitisation spectrum

(adapted from Buzan, Wæver & de Wilde 1998: 23)

3.2. Critique of securitisation and the case for desecuritisation

The politicisation of an issue brings it into the open and makes it a matter of public choice and something to be decided upon, that is a part of the normal politics of public deliberation in a democracy. The securitisation of an issue, by contrast, removes it from the political contestation of normal politics and justifies its prioritisation over other issues, as well as decisive action by political leaders. This may work to silence opposition, as leaders may exploit threats for domestic purposes and act without democratic control or constraint. In this respect, security is a negative term that points to a removal of an issue from the realm of discursive politics (Fierke 2007: 108).

Furthermore, "securitisation highlights the dynamics by which some threats as opposed to others come to be understood under the rubric of security and the significance of this naming as an act of construction" (Fierke 2007: 103). This is the definitive aspect of this theory, namely how it is decided that one issue has preference over another. Giving traction to this idea is that "(t)he state has a particular authority in this regard: if the *state* says something is a security problem, then it is almost necessarily so" (Mutimer 1999: 89). Likewise, Mutimer (1999: 89) even refers to the withholding of information from the public by the state, as an example of the securitisation of an issue. The state is privileged in the process of securitisation and the tendency is for it to (even) militarise issues – in terms of extraordinary measures – when securitising them (Wæver 1995). Furthermore, Wæver's concern is not what constitutes a new security agenda but rather the concept of desecuritisation.

As Securitisation Theory promotes the separation of issues on a spectrum, some scholars have promoted the idea of moving away from this over-emphasis of a security perspective. The security label is not necessarily an optimum solution "as securitisation of an issue brings

© University of Pretoria

with it a particular type of emergency politics where the space (and time) allowed for deliberation, participation, and bargaining is necessarily constricted and brings into play a particular, militarised mode of thinking" (Peoples & Vaughan-Williams 2010: 83). It is because of this recourse to military-focused solutions for most security issues that proponents of desecuritisation argue for the normalisation of politics in addressing an issue.

Hansen (2000) is critical of the concept of securitisation because of its failure to address 'the silent security dilemma'. He explains that the 'security of silence' occurs when the potential subject of (in)security has no, or limited possibility of speaking its security problems" (Buzan & Hansen 2009: 216). Because the securitising move is fundamentally enacted by agents in power, the theory automatically elevates the role of these agents and creates superiority in the process which alienates the referent objects ultimately affected by the threat/issue. Another criticism, expressed by Eriksson (2001a) and admitted by Wæver (2000), is that within the security realm even the analyst of securitisation contributes to the securitising move and essentially to the securitisation process. A pertinent criticism is made by Williams (2003: 524) where he dispels the capability of a theory "so closely tied to speech for its explanatory and ethical position" to represent the current dynamics of the Information Age. The profound notion of a speech act is somewhat diminished when there is an overload of information, delivered continuously through various forms of media, that penetrate daily life.

The transformative and radical environment of contemporary international relations being what it is, allowed more authors to emerge who either contested the writings of the Copenhagen School, or augmented their work by adding a new conceptualisation of the theory. Consequently, a second generation of scholars can be identified who produced work that branches off from the initial theory of securitisation. This generation includes scholars such as Balzacq (2005) and Huysmans (1998a) who made significant contributions to the literature as constructivists. Balzacq's (2011a) isolation of three core assumptions of Securitisation Theory offers a practical breakdown of the process and how it can be determined if securitisation has occurred. These three core assumptions (Balzacq 2011a: 8-15) are:

> 1) *The centrality of the audience – … an 'empowering audience' must agree with the claims made by the securitizing actor. The empowering audience is the audience which: a)*

© University of Pretoria

has a direct causal connection with the issue; and b) has the ability to enable the securitizing actor to adopt measures in order to tackle the threat ….

2) The co-dependency of agency and context – … the semantic repertoire of security is a combination of textual meaning … and cultural meaning. Thus, the performative dimension of security rests between semantic regularity and contextual circumstances ….

3) The dispositif and the structuring force of practices – … securitization occurs in a field of struggles. It thus consists of practices which instantiate intersubjective understandings … The dispositif connects different practices ….

Balzacq's (2011a) deconstruction (above) emphasises three core assumptions of securitisation that provide a set of standards for insights that previous pathways were unable to reveal. They offer a practical expression of securitisation in the 21st century and how it relates to current non-military security issues. This deconstruction also proffers a constructivist perspective on security that emphasises social and non-material structures. His theorising provides the most practical example for this study, and as such these considerations will be applied along with the elements of securitisation in respect of the South African case study.

4. The information-security nexus

Information is intrinsically linked to security, through the power of information and in that it informs the intelligence process which is the purview of the security industry. As the conceptions and understandings of security and information are cultivated to represent 21st century conditions, it becomes more pertinent to reconsider matters that need protection and how this protection should be enacted.

4.1 The protection of information

As more information is shared in the international arena, governments will aim to protect themselves and their state intelligence, tantamount to 'information seclusion'. This protectionism is reinforced by Jones' (1996: 21) indication that "barriers can be built around such issues as privacy, intellectual property rights, trans-border data flow, and protectionist policies." This approach to information and the reformulation of information security is essential in the digital world where "everything and everywhere becomes potentially dangerous as

© University of Pretoria

nothing consists of fixed properties, independent of the information systems in which they are produced and reproduced" (Fierke 2007: 117). More vigilance is required to protect information if used as a tool of power to ensure national security. If information is considered to be a component of power, it "is the most transferable and useful force at all political levels" (Armistead 2004: 9). This utility of information explains the desire for states to control the access to information at all costs. Because of the number of players in the 'game' of world politics and the copious factors governments need to contend with in this complex, multi-polar world, it is expected and accepted (within reason) that states will aim to protect themselves against this diminishment of control by using secrecy.

Autocratic behaviour by states to deliberately restrict society's access to information sends a pejorative message to the masses, who feel further alienated from what may be an already bulwarked political system. Nevertheless, Lipschutz (1995a: 215) posits that "if we consider the concept in terms of societal and state disintegration, we are forced to conclude that the threat to security arises primarily from the activities of members of the society and the citizens of the affected state." The masses themselves often prove to be fickle and radical in their opinions of and loyalty (or disloyalty) towards government, which necessitates a certain level of protection of information and resources; as well as the preservation of state processes.

In the Information Age, "(f)reedom of information and freedom of expression are some of the greatest achievements of the great democratic revolution" (Ngcobo 2013). This is the emancipation Booth posited. The challenge to this 'greatest achievement' is that its success lies in its continuous utilisation by various actors, to give credence to transformative legislation. Evidently, "(t)he idea of freedom of information rests, rather, on the necessity for some citizens to pay attention at least some of the time (on behalf of the rest of us) in order to identify and correct occasional or even frequent instances of incompetence, dishonesty or ignorance in governments that are otherwise moderately efficient and effective" (Darch & Underwood 2010: 3). The contemporary information-security nexus involves complex dynamics manifested in the level of public activism and scrutiny, and the need for governing bodies to protect and conceal information for security reasons.

© University of Pretoria

4.2. Freedom of information legislation

A disjuncture pervades the information matrix: on the one more theoretical hand, freedom of information is enshrined in constitutions with laws enacted to allow access to information and promote accessibility and availability of this information; on the other more practical hand, a significant number of people are not able to mobilise resources to appeal for information – and if they are successful enough in this initial step, they are not necessarily guaranteed official approval to access the information.

For some people by way of their vocation– including journalists, academics and researchers – this access to information promoted by a freedom of information principle in legislation is often their livelihood. For example, "(i)nvestigative journalists and non-governmental organisations fighting corruption rely on the right of access to information to expose it" (Ngcobo 2013), accentuating the necessity of systemic and procedural access to information. Initiatives that create constitutionally-binding legislation to secure access to information is praised the world over, especially in still-developing democratic states in which an open-access information paradigm is encouraged.

Nonetheless, "(e)ven though those in power must consider requests for information held by the state from members of the public, they are in a very powerful position, and information inadvertently becomes a lever of power" (Africa 2009: 34). Simultaneously, granting *de facto* access to the media bestows power on them and on members of the public once they have the information in their possession. The challenge is to utilise this power once gained. A survey conducted for the workshop on 'National Security and the Right to Information Principles' (Nyirenda & Polaki 2013: 22) of the Open Society Initiative for Southern Africa (OSISA) reported that of the countries surveyed, most "have constitutional provisions for the right to information but then adversely faced implementation challenges." To ensure access and effectiveness, accurate implementation and oversight of information policy are required (as with any policy).

As much as freedom of information legislation holds promise of a more democratic and participatory system, the initiation of this legislation is often celebrated prematurely, with little consideration given to its implementation and its efficacy (or lack thereof). Darch and

© University of Pretoria

Underwood (2010: 50) explain that “while freedom of information advocacy promises much – better democratic practice, less corruption, more media freedom and thus better news reporting, even socio-economic development itself – the payoffs in the admittedly short term have been incremental improvements rather than spectacular breakthroughs.” Notably, this same legislation is supposed to be implemented by practitioners who aim to remain in power and ensure their own protection.

In summary, freedom to information should be for the benefit of the general public. If more access and availability is encouraged, less secrecy is cultivated. Two challenges exist to developing a freedom of information culture in any given state: first, “enforcement or encouragement of compliance among civil servants who control information; and second, the promotion and management of demand among those who might potentially benefit from access to the information” (Darch & Underwood 2010: 92). It is this information culture that is significant and which relates to and even competes with the security culture of the state.

4.3. The protection of information for national security

The security culture of the state, especially in democracies, is not an absolute. “The ‘security of the state’ argument may be generally accepted as a justification for secrecy, but in most countries a caveat requires, in theory, a clear link to some credible threat of force” (Darch & Underwood 2010: 174). If the public has an understanding of the national interest of the state, and therefore the security measures required to protect these interests, this would diminish misperceptions about the motives of government. Arguably, a national security policy to this effect could contribute to a more inclusive information-security milieu.

An extensive body of scholarship explores the information-security nexus, including Jones (1996), Bruneau (2008) and Ransom (2008) who espouse the importance of accessibility and availability of information in democracies, to ensure a culture of open and free communication at all levels. This scholarship argues for the free-flow of information, advocating for more transparency and accountability from government who often fails on this count. It is also evident that clear conceptions of information and national security are required before any legislation can be developed on their relationship, especially since this relationship plays a vital role in the functioning of the state. It is almost contradictory that as indispensable as

© University of Pretoria

information is, “we do not have a satisfactory integrated definition of what it is” (Darch & Underwood 2010: 258, referring to South Africa).

Klaaren (cited by Nyirenda & Polaki 2013: 4), in considering ‘national security and the right to information principles’, explored the relationship of the right of access to information and national security, arguing that access to national security information (in South Africa in particular) is influenced by the continuing conceptual entrenchment of the constitutional right to access to information and the on-going transformation of the security sector including its shifting constitutional regulation. Although government or a leadership elite used to control information, the technological advances have shattered their monopoly over it. In reality, the government can no longer control information. This is because it does not own the contemporary sources or the means of delivery of information.

Thus the relentless pursuit of the control of information continues. Information becomes a currency of power in the current era, and states have developed new methods of ensuring they are information-wealthier than the next. Ultimately information is about acuity, “because information is an enabler, a ‘source multiplier’, a tool that increases one’s ability to shape the operational environment” (Armistead 2004: 1). This axiom is not the preserve of state and government only but applies equally to all political actors.

5. Conclusion

The aim of this chapter was to provide a conceptual and theoretical framework to position information within the ambit of national security, in order to allow an analysis and assessment of the securitisation of information in respect of the South African case study. Using contemporary Security Studies as a context and Critical Security Studies as a point of departure it provided an account of the nature, scope, elements and critique of Securitisation Theory. The contemporary meaning and understanding of the concepts of security, national security, and information were not only clarified, but also explained in the context of an information-security nexus. Because of the competitive and implicit contradictory nature of the two core concepts (information and security), attention was paid to the meaning and scope of this relationship. Intrinsic to this relationship is the dynamic between openness and secrecy whereby an equilibrium between the two notions is the ideal for good state governance.

© University of Pretoria

Three key findings are identified. Firstly, concerning Security Studies, this field remains adept to the changed and changing environment which it studies. Secondly, Securitisation Theory is enriched by a variety of scholars and schools of thought to become amenable to the current international ambit, making it practicable as an assessment tool. Thirdly, regarding the information-security nexus, the fluidity of concepts is imperative in the Information Age, to allow for adaptability to the reality, and maintain a relevance and practicality for common usage. This is also significant to inform the environment in which this nexus operates. In a practical sense, the conceptual-theoretical framework culminated in a reference to the information-security regime in South Africa. This is the focus of the next chapter on the information-security landscape of South Africa that frames the Information Bill.

© University of Pretoria

CHAPTER THREE

THE *PROTECTION OF STATE INFORMATION BILL, 2010* IN THE SOUTH AFRICAN INFORMATION-SECURITY LANDSCAPE: A CONTEXTUALISATION

1. Introduction

The aim of this chapter is to introduce and contextualise the case study, namely the *Protection of State Information Bill, 2010* of South Africa. The chapter, which is predominantly descriptive in nature, commences by looking at the various domains (historical, security and legal) that contextualise the South African environment into which this Bill is introduced. Concerning the Bill itself an account is provided of its premise, its introduction and development, its aim and legal parameters, as well as the debate on and criticism of it. The time period under scrutiny ranges from the pre-1994 apartheid to the post-1994 democratic era. Because of the nefarious utilisation of information by the pre-1994 regime, this distinction needs to be made since the current role conceptions differ. Furthermore, two decades after the first inclusive elections, it is imperative to assess the democratic context of and manner in which information and security are linked in the information landscape. This account of the context and the particulars of the Bill is a prerequisite for the analysis (see Chapter 4) of it in terms of Securitisation Theory.

2. The information landscape of South Africa

The current information landscape differs vastly from that of the pre-1994 regime, specifically regarding the principles that underpin the democratic dispensation[21]. Contrary to the pre-1994 era, information is legitimately and legally accessible through a constitution that upholds the rights to information access and freedom of expression. This information landscape within which the Information Bill is positioned, is forthwith discussed with reference to its historical, political security and legal context.

[21] For more detail on the changed landscape of South Africa's information-security nexus with regard to the new democratic dispensation, see Booth and Vale 1995; Elbe 2003; Vale 2003.

© University of Pretoria

2.1 The historical context

The plethora of legislation that was enacted during the apartheid era included the *Protection of Information Act, 1982* (Act 84 of 1982) (hereinafter the Information Act), to be repealed with the promulgation of the Information Bill[22]. The Information Act's primary aim is "to provide for the protection from disclosure of certain information," instituted to prevent any unwarranted disclosure, dissemination, obtainment and/or possession of information detrimental to the institutional processes of the state with the threat of persecution. The Act is vague and non-descript, allowing room for manoeuvre on the part of the Government in persecuting offenders. For example, within the Act 'certain information' was not defined comprehensively, resulting in a wide range of prohibited activities relating to information that could be deemed "prejudicial to security or interests of the Republic" (Act 84 of 1982: Article 5(1) & 10(1)). This approach allowed flexibility to persecute offenders in the name of national security.

The addition of more stringent legislation[23] by the apartheid government, to suppress the rising militancy of opposition forces, created a securitised environment that impacted on and dictated nearly every facet of life – including (amongst others) the restriction of public access to information. In particular press freedom was targeted due to security concerns, being a source of publically-disseminated information with "the main statutory restraints … in the areas of defense, security, police, and prisons reporting" (Heard 1987: 256). Restrictions on the press limited publishable content on internal and external security issues and on the kind of publications suitable for public sale and dissemination. Furthermore, during the 1970s the Government also established the Department of Information responsible for controlling and disseminating official information, entrenching the Government's monopoly on information.

---

[22] The *Protection of Information Act, 1982* (Act 84 of 1982) has in part been amended and supplemented by the *Intelligence Services Act, 1994* (Act 39 of 1994); the *Justice Laws Rationalisation Act, 1996* (Act 18 of 1996); the *Intelligence Services Act, 2002* (Act 65 of 2002); the *Electronic Communications Security (Pty) Ltd Act, 2002* (Act 68 of 2002); and the *General Intelligence Laws Amendment Act, 2003* (Act 52 of 2003).

[23] Statutory restrictions on the freedom of the press in the interests of state security included the Internal Security Act, 1982 (Act 74 of 1982); the *Defence Act, 1957* (Act 44 of 1957); the *Police Act, 1958* (Act 7 of 1958); the *Prisons Act, 1959* (Act 8 of 1959); the *Nuclear Energy Act* (now Act 131 of 1993); the *National Key Points Act, 1980* (Act 102 of 1980); the *Publications Act, 1974 (Act 42 of 1974);* the *Petroleum Products Act, 1977* (Act 120 of 1977); the *Armaments Development and Production Act* (57 of 1968); the *National Supplies Procurement Act , 1970* (Act 89 of 1970); the *Intimidation Act, 1982* (Act 72 of 1982); and the *Demonstrations in or Near Court Buildings Prohibition Act, 1982* (Act 71 of 1982). (see Burns 1985: 227-231).

© University of Pretoria

During this era the tense relationship between government and press was "reflected in the Government banishment orders placed on reporters" (Burns 1985: 226) when their reporting exposed state wrong-doings. The Government was partial to the media as long as they offered a positive account. The media (as a private or public entity providing in part a public service) had a responsibility to the people to deliver truthful, non-partisan reporting to fulfil its role as a watchdog and information service. Despite sensationalism being *sine qua non*, a balance is required to inculcate trust between government, the media and the public at large. If achieved, this engenders a greater respect for governance. Patently this was not the case pre-1994, but the dynamics of this relationship and responsibility of both parties remain critical.

Writing in 1985 about the then political-social climate, Burns (1985: 248) argued that a large amount of self-censorship was required by the press to avoid persecution as "wide legislative provisions (did) not define prohibited criminal conduct clearly." Thus critical information was habitually not reported. A watershed event curtailing freedom of expression and information occurred on 20 October 1977. The Government banned the Black Consciousness Movement (BCM)[24] and aligned anti-apartheid activists and organisations. Three newspapers were shut down. As the move was an attempt to 'gag the media and muzzle those' exposing the Government's clandestine activities, the day was deemed Black Wednesday (South African History Archive (SAHA) 2011). In the present day, in an effort to recall 'Black Wednesday' the South African media dubbed 22 October 2011, the day the Bill was passed in Parliament but referred to the President for amendments, as 'Black Tuesday'[25].

In the early 1990s, the interim Government of National Unity (GNU) formulated new laws for a country, striving to distance itself from the previous regime's autocratic rule. To facilitate a smoother transition and ease legislative bureaucracy, not all apartheid-era legislation was repealed. Since then various government entities worked towards the eradication of the old laws, to better represent a democratic South Africa. This process is on-going, allowing systemic remnants of the former dispensation to prevail until laws are repealed and policies

[24] The BCM is an umbrella term used to describe the black consciousness ideology and the different organisations and groups centred around it. Following the October 1977 banning, the main black consciousness organisations were persistently harassed by the police. (O'Malley 1991 resource hosted on the Nelson Mandela Centre of Memory webpage).
[25] See appendix D for a satirical representation of this.

© University of Pretoria

are adjusted to become more compatible with and suitable to the current democratic environment.

2.2. The political-security context

The political-security context of information in South Africa is framed by the juxtaposition of the need for openness and secrecy. Openness, amongst others, is dependent on media and civil society participation. Secrecy is a product of the security realm and the securitisation of issues in the national interest of the state. In South Africa, a stable relationship between openness and secrecy is critical.

In the globalised political-security context and compared to the security realm of the previous dispensation, South African state institutions have adopted an understanding of security and the national interest that is more comprehensive in nature and that includes human security. The current landscape is governed by the *White Paper on Intelligence* (RSA 1994) – the definitive document on South African security to date, as well as the Minimum Information Security Standards (MISS) (RSA 1996) – compiled as official policy on information security[26]. These documents require revision to inform 21st century practices, while still being aligned with the state's national and human security objectives. This imperative provides impetus to the creation and consolidation of transformative legislation and institutions within the political-security domain.

According to the *White Paper on Intelligence* (RSA 1994 section 3.3, paragraph 6) "(s)ecurity is a holistic phenomenon and incorporates political, social, economic and environmental issues; (t)he objectives of security policy go beyond achieving an absence of war to encompass the pursuit of democracy, sustainable economic development and social justice." In theory, this approach creates a strong foundation for a democratic South Africa to achieve a balance between openness and secrecy, hitherto aided by the intelligence services and democratic institutions of the country. Through the MISS a sound foundation is adhered to, at least on paper, in the processes to formulate policies and to deliver information security

[26] The *National Archives and Records Service of South Africa Act, 1996* (Act 43 of 1996) is aimed at promoting effective record-keeping of state information and making this readily available and accessible – on request and to be approved through a process and in line with the relevant legislation.

© University of Pretoria

services that are sufficiently flexible to facilitate change. The MISS (RSA 1996) acknowledges that:

> *Our need for secrecy and therefore information security measures in a democratic and open society with transparency in its governmental administration according to the policy proposals regarding the intended Open Democracy Act have been taken into account. Our security standards and procedures must result in the fair and equitable treatment of those upon whom we rely to guard the nation's security.*

The White Paper and the MISS envelop the 'secrecy' aspect of the democratic equilibrium, while recognising the necessity not to impinge on 'openness' which is pursued and promoted by various actors in a watchdog capacity. However, the successful adoption of a human security perspective "depends on the existence of legitimate institutions that gain the trust of the population and have some enforcement capacity" (Kaldor 2007: 187). In this respect the following observations are made:

Firstly, concerning the role of the free press and politico-civic emancipation, South Africa has always maintained a robust civil society amplified by a vociferous media. Notwithstanding the numerous pre-1994 laws that prohibited anti-government publications, the printed and visual media continued to act as a commentator, reporter and (to some extent) analyst of the times. This role has been compounded in the new South Africa by the expansion of online media. As Bekker (2004: 147) explains: "South Africa is fortunate in having an independent newspaper industry that strives to achieve standards of journalism and management compatible with those in mature democracies." Despite this achievement, Sullivan[27] (2004: 171) contends that "there are still too many laws inhibiting the press." Having made the remark ten years ago, it is noted that the situation has not improved and arguably has worsened.

Secondly, the expansion of the scope of the security services in South Africa is seen as incongruent with the primacy of freedoms of expression and access to information. The legacy of apartheid-era legislation in the information-security realm justifies the on-going amendments and repeals of legislation, to streamline bureaucracy and to create appropriate information-security architecture. According to the State Security Agency (SSA) (RSA SSA

[27] Peter Sullivan, former group editor-in-chief of Independent Newspapers in South Africa held this position until 2010.

© University of Pretoria

2013), "this bill seeks to deal with present and clear challenges of protecting valuable state information against alteration, loss and destruction which would ensure citizens are not inconvenienced unnecessarily." The bureaucracy – having been tasked to provide protection under outdated legislation – was overloaded with the storage and classification of massive amounts of information that did not require protection. Hence, particular government departments underwent a reformulation of roles and responsibilities.[28]

In 2009, President Jacob Zuma reshuffled cabinet and instituted a reformation of government departments that included the state intelligence services, namely, the National Intelligence Agency (NIA), the South African Secret Service (SASS), the South African National Academy of Intelligence (SANAI), the National Communications Centre (NCC), the Office for Interception Centres (OIC), and Electronic Communications Security (COMSEC). The SSA that amalgamated the domestic and foreign branches of intelligence – namely NIA and SASS – represented not only a name and hierarchical change but also a unitary focus on security. The remaining entities were incorporated into the SSA structure.[29] In this respect the SSA was an institutional adaptation, resulting from a combined effort on the part of the Ministers of State Security, Police, Defence, Home Affairs, Justice and Correctional Services to create a more effective and efficient civilian intelligence architecture.

Thirdly, a transparent information and intelligence platform, amongst others by way of an investigative press, is vital to challenge vague and clandestine government activity. Helen Suzman (1991: 44), the famed South African politician and human rights activist, conceded that "there is certain information of a strategic nature which requires special protection". Quoting Professor Baxter of Duke University,[30] she emphasised that "any open system of government must recognize that the considerations which justify the restrictions of public access to official information are limited ones"; but that "free access to such information is a

[28] Arguably the need to ease the bureaucratic burden and streamline the operations of government is not the only reason for the reformation of the SSA and other government departments during the 2009 cabinet reshuffle.
[29] During this amalgamation, the names of these entities changed: SANAI became the Intelligence Academy (IA); and the National Communications Centre became National Communications.
[30] Professor Lawrence G. Baxter is the William B. McGuire Professor of the Practice of Law at Duke University (US). He was instrumental in reshaping areas of law in South Africa and has written extensively on government abuse and public policy with specific reference to South Africa.

© University of Pretoria

necessary prerequisite for public accountability and an essential feature of modern democratic theory" (Suzman 1991: 44). The protection of national security is the *raison d'etre* which allows for the often extreme behaviour associated with protecting the state, but consideration must be given to whether this is compatible with the national interest.

2.3 The legal context

South Africa boasts a firm legal foundation, derived from the *Constitution of the Republic of South Africa, 1996* (Act 108 of 1996) (hereinafter the Constitution) and the separation of the three branches of government[31], that underpin policy-making, policy implementation and policy evaluation. This legal framework also contextualises South Africa's information society, and includes relevant constitutional provisions for access to information.[32]

2.3.1. Constitutional provisions

The Constitution is the supreme law of the land and provides the foundation for South Africa as a constitutional democracy under rule of law. It includes the Bill of Rights (Chapter 2 of the Constitution) that as "a cornerstone of democracy in South Africa … enshrines the rights of all people in our country" and requires that "the state must respect, protect, promote and fulfil the rights" subject to stipulated limitations (section 7(1-3)). Included in the Bill of Rights is the right of access to information (section 32). In this respect South Africa maintains a liberal approach to information considering that national legislation must be effected to ensure "(e)veryone 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(1-3)). Although Section 32 does not provide a specific caveat to justifiably protect information against public access, the Section 7(3) provision for limitations of rights apply as contained in Section 36. Similar to other rights in the Bill of Rights, the right of access to information may be justifiably limited with this judgement being subjective, conditional and

[31] The three branches of government are the Executive, Legislative and Judicial.
[32] Legislation on the access to information includes: the *Promotion of Access to Information Act, 2000* (Act 2 of 2000); the *Protection of Personal Information Act, 2013* (Act 4 of 2013); the *National Archives and Records Service of South Africa Act, 1996* (Act 43 of 1996); the *Legal Deposit Act, 1997* (Act 54 of 1997); the *Protected Disclosures Act, 2000* (Act 26 of 2000); the *Promotion of Equality and Unfair Discrimination, 2000* (Act 4 of 2000); and the *Promotion of Administrative Justice Act, 2000* (Act 3 of 2000).

© University of Pretoria

circumstantial. According to Section 36(1) “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.” (for the latter see section 36(1)(a-e)). Furthermore and except for the aforesaid, “no law may limit” any entrenched right (section 36(2)).

In spite of this limitation, provision and fulfilment of rights still favour the public, at least in principle and is pursued further with the Bill which aims for “a better balance between the constitutional provisions of access to information and the limitation of that access in the interest of advancing our national security” (RSA SSA 2013). To create this equilibrium, the Constitution bridges the gap between an openly democratic society and a protected state operating to defend national interests. The latter is the subject matter of Chapter 11 of the Constitution on *Security Services*, based on the governing principle amongst others that “(n)ational security must be pursued in compliance with the law” (section 198(d)).

2.3.2 The promotion of access to information

To give effect to the Constitutional provisions, the *Promotion of Access to Information Act*, *2000* (Act 2 of 2000) (hereinafter the Access to Information Act) was introduced. This Act provides the legal framework for an open society with equitable access to information held by any entity, including the state.

(a) Rationale: The implementation of the Access to Information Act heralded a new era as transparency and freedom of access are promoted, ensuring every citizen the legislated opportunity to access information. The Preamble of the Act recognises that the system of the previous government “resulted in a secretive and unresponsive culture in public and private bodies which often led to an abuse of power and human rights violations.” It is with this in mind that the Access to Information Act signalled a transformed and progressive information society. In this respect then Minister of Justice and Constitutional Development, Penuell Maduna, emphasised the precedent of this legislation by “turning on the light to bring to an end the secrecy and silence that characterised decades of apartheid rule and administration” (SAPA 2000).

© University of Pretoria

According to the Preamble of the Access to Information Act, the aim is to "foster a culture of transparency and accountability in public and private bodies by giving effect to the right of access to information" and 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." This rationale is based on the consensus that freedom of information legislation is beneficial and necessary to promote transparency and that it embeds an ethos of protecting human rights. This correlates with the viewpoint that "(South Africa) must go further than merely passing a law, and should involve implanting the roots of freedom of information behaviour and creating a freedom of information culture, in order to remove the barriers of secrecy" (Darch & Underwood 2010: 217). The Access to Information Act portends this freedom of information culture in South Africa.

(b) Key provisions: They key provisions of the Access to Information Act refer to objectives, provisos for refusal of disclosure, and mandatory disclosure in the public interest (see Appendix A). Firstly, the objectives of the Act are to promote a culture of openness and accessibility with regard to information that appeals to the democratic principles of the country and Constitution. This Act essentially provides a mechanism to request access to information.

Secondly, the Act (Chapter 2 Section 5 Part 1) makes provision for its utilisation in conjunction with, and in respect of, other corresponding legislation that might allow or disallow access to specific information. It further stipulates (section 11-13) that requests for access to records can be made of a public body and/or a private body and prescribes the manner in which this request must be submitted as well as the manner in which the access can be granted, should the request follow the legislative procedures. More importantly, Chapter 4 of the Act concerns grounds for refusal of access to records (section 33-46). Section 41 of the Act specifically makes provision for records that concern the defence, security and international relations of South Africa, which are protected from disclosure where a refusal for such records may be granted and justified.

Thirdly, the Act contains a public interest clause (Chapter 4 Section 46 Part 2) which stipulates a mandatory disclosure (of records) in the public interest. However, this stipulation is governed by the requirement of the Act to work in conjunction with corresponding

© University of Pretoria

legislation, and is limited by section 26 of the Constitution. In its application, the Act has to determine the hierarchy of limitations and the granting of requested access.

(c) Assessment: The Access to Information Act provides for a stringent promotion of access to public and private records and furthermore grants access to the requested records, in so far as the disclosure of the information will not cause harm or whereby the disclosure of particular records is necessary in order to prevent harm. At least in principle, the Act strikes a balance between openness towards the public in fulfilling their right to know and have access to information, and secrecy of state information that by its very nature demands to be concealed. It was envisioned that "the new Act will also change inherited attitudes to secrecy and censorship" (Shaw 2001: 33). Thus it provides a legal foundation for a more open information culture in which a robust media and civil society is free from fear in reporting on state actions, thereby perpetuating the openness of a democratic system.

Notwithstanding this significance, its implementation has been deemed to be disappointing. This is reflected in the minimal amount of requests for access and the inefficiency of the bureaucratic process when requests are made (Darch & Underwood 2010: 237). As much as it is the responsibility of the citizenry to be fully aware of their rights to demand more proficiency in the implementation of legislation, the onus is on the state to ensure an effective and efficient performance in the implementation of legislation in instances when citizens are active and demanding of these rights. Although the Act has hitherto not become the revolutionary catalyst for transparency as intended, it fosters a notion of accessibility which had until recently been absent in South Africa.

2.3.3 The protection of personal information

The *Protection of Personal Information Act, 2013* (Act 4 of 2013) (hereinafter the Personal Information Act) provides the legislative authority that allows individuals to claim their right to privacy (in terms of Section 14 of the Constitution) and to the protection of their personal information. The ethos of the Information Bill and the Personal Information Act are intertwined, given the overarching aim of both pieces of legislation to protect state and personal information, respectively; and considering their application and alignment in terms of the Access to Information Act (Preamble of the Personal Information Act). This

© University of Pretoria

synchronisation of legislation is essential for the progression of the information society, and to ensure that the encouragement of access to information and not the concealment of information remains the priority.

In summary and as stated in its Preamble, the Personal Information Act will "regulate, in harmony with international standards, the processing of personal information by public and private bodies in a manner that gives effect to the right to privacy subject to justifiable limitations that are aimed at protecting other rights and important interests". This acknowledges the (Constitutional) limitations of specific rights and guarantees respect for restrictions on information, but within a framework that promotes protection of personal information and the free flow of information. In this way the legislation contributes to a South African information culture that upholds the constitutional right to privacy of personal information, and provides a regulatory framework to guarantee and monitor the legislated protection of the rights of all within the borders of the country. It is within this historical, political-security and legal context that the issue arises whether or not the Information Bill contributes to or is beneficial for South Africa's information landscape.

3. The protection of state information

Whereas the previous discussion clarified the macro context of the *Protection of State Information Bill***,** *2010*, the micro-level aspects pertaining to its introduction, content and ramifications are forthwith considered. Attention is given to its nature and scope, its key provisions, its legislative process and its critique.

3.1. The nature and scope of the Information Bill

The nature and scope of the Bill is extremely extensive, being a complex piece of proposed legislation. A sense of this is obtained by considering its aim and objectives and taking heed of the definitions of its key concepts (see Appendix B).

The Bill was introduced during the reform of the South African intelligence services, as part of the reconsideration of the protection of state information. The South African government required a more modern and responsive regulatory framework to combat the threats posed to the country by a transformative security paradigm, and to contest the vulnerable areas of

© University of Pretoria

"espionage, information-peddling, counter-espionage, and alteration of critical databases" (RSA SSA 2010a). To only adjust the names and structures of government security entities, when a large-scale re-evaluation of the security framework of the country was vital, would have been insufficient and debilitating reform. Hence the introduction of concurrent legislation, to enforce policy changes on state operations that serve the national interest and that combat internal and external threats to the country.

3.1.1. Aim and objectives

The aim of the Bill is "to provide for the protection of certain information from destruction, loss or unlawful disclosure; to regulate the manner in which information may be protected; and to repeal the *Protection of Information Act, 1982*" (RSA Bill 2010). In addition the intention is to create a new framework for the classification and declassification of state information by stipulating which information requires different forms of protection and the disclosure permitted therewith. This is expected to reduce the copious amount of state documents amassed pre- and post-1994, and the administration and operational costs thereof. The Bill will "balance the presumption of secrecy with a presumption of openness" (RSA SSA 2010a) so that only the essential elements of state operations are protected, and to allow records to be accessed by the public should this be warranted.

The objectives of the Bill (Chapter 1 Section 2 in RSA Bill 2010) posit an effort towards streamlining the operational processes of Government with regard to information. These objectives stipulate a contemporary approach to information dissemination, storage, classification, protection and usage that informs the work of the intelligence services in the present Information Age. Critically, these objectives highlight the necessity for a revised information-security framework to address the persecution of those found to be acting with disregard for the law.

The approach, to re-envision a consolidated information-security paradigm that enhances the national security of the country, is comprehensive. The objectives are sufficiently progressive and broad to allow flexibility in addressing different aspects of information and to adapt to a changing environment. In contrast and by overseeing a wider scope of what can be considered state information, they also produce undesirable aspects (see Section 3.4) due to

© University of Pretoria

their potentially restrictive or intrusive nature. This counter-impact epitomises the complexity of this piece of legislation and the environment in which it functions.

3.1.2 Definition of concepts

The key concepts in the Bill contribute to the nuanced approach the legislation adopts in 'improving' the information landscape (see Appendix B). The central concepts (regarding this study) are information and security (Chapter 1 Section 1). In essence, information relates to "any facts, particulars or details of any kind, whether true or false, and contained in any form". To address technological advancements in the production, storage and destruction of information, the definition indicates an extensive range of devices and formats that pertain to information usage. This includes a definition of ICT, to also protect the state against the intensifying dynamics of cyber-intelligence and the related fields of cybercrimes and cyber-espionage.

Security is seen as a condition of protection, resulting from the use of certain measures, against hostile acts. To these, as a further contextualisation and qualification, are added the related concepts of national security (in principle defined as freedom from fear, want and indignity); a state security matter (dealt with by the SSA); protected information (state information requiring protection); and legitimate interest (constitutionally, legally and/or institutionally mandated). Of note is the information-security nexus underscored by the concept of information security (Chapter 1 Section 1), defined as "the safeguarding or protecting of information in whatever form". The definitions in the Bill are not prescriptive but rather allow for flexibility, so as to approach particular scenarios conditionally.

3.2 Key provisions of the Information Bill

The most significant provisions of the Bill are briefly presented (see Appendix B for detail where applicable). These primarily concern the principles of the Bill; the national interest context of sensitive information and the classification and declassification of information. In this respect it must be kept in mind that the existing provisions of the Bill could still be altered through the consultative legislative process (discussed in the next section).

© University of Pretoria

Firstly, Chapter 2 Section 4 of the Bill concerns the General Principles of State Information, principally that "(s)tate information may … be protected against unlawful disclosure, destruction, alteration or loss." This clause vindicates the adaption of the legislation as it addresses events prior to 1994 when copious amounts of information were destroyed to conceal apartheid-era activities. It underscores the notion that the new information paradigm is geared to serve an expedient role for recording purposes and equally for the longevity of information. The principles (Section 6) exemplify the credible, transparent and regulated information society the legislation aims to advance; the notion that the restriction of information on national security grounds be the exception rather than the rule; and the congruence of the legislation and civil liberties pertaining to freedom of expression and access to information, being mindful not to infringe on these rights.

Secondly, a significant aspect of the Bill is the Chapter 5 Section 17 stipulations on *Sensitive Information: National Interest of Republic* that specifically relate to the information that requires protection from disclosure. This conception is necessarily broad to encompass what is or may be significant to the security of the state. In this respect, Currie and Klaaren (2011: 14) defend the broad scope of the Information Bill when compared to other official secrets law on the basis that "its scope was principally a product of its legislative history and its intention not only to provide for the protection of state secrets in the narrow sense but also to provide for a comprehensive regime of government confidentiality that would replace the existing regime." Since national security is practised to allow a state the opportunity to pursue its national interests, a prerequisite is an enabling environment to advance these national interests. In this respect, the Bill (Chapter 6 Section 11) provides an extensive indication of South Africa's national interest (see Appendix B). According to Chapter 6 Section 11, the specific and broad national interest of the state embodies the national values as enshrined in the Constitution. This section also makes reference to the correlation to the Access to Information Act. In this way, the Bill underscores the importance of synchronising with existing legislation to enhance the information culture in South Africa.

Thirdly, the need for a continuous classification, declassification and downgrading of information (Chapter 6) speaks to a revised system for processing categories of information, and for these processes to occur within a regulatory framework. This need is borne out by the

© University of Pretoria

SSA's (RSA SSA 2010a) viewpoint that "the Bill provides for a process that will facilitate the flow of information in a more coordinated approach, within the provisions of the Constitution." The Bill presents an updated approach to the scope and nature of classification and declassification of state information (see Appendix C).

On the one hand, regarding the rubric of designations to attribute levels of security classification, the Bill redrafted the classification criteria in the three security levels of 'confidential, secret and top secret'. Specifically it addressed the criticism that these were vague; that the threshold of classifiability was too low; and that this would lead to over-classification and therefore be vulnerable to cynical classification (Currie & Klaaren 2011: 18). In addition and as contended in the Executive Summary of the Bill (RSA 2010), the legislation advances "a comprehensive statutory foundation for the classification and declassification of information … likely to result in a more stable and cost-effective set of policies and a more consistent application of rules and procedures." Therefore its subsequent amendments addressed the claim that the Bill was too broad in scope, and aimed to emphasise specificity in the application of security levels.

On the other hand, regarding access to classified information in terms of the Access to Information Act, the Bill deals with the issue of requests for access. Section 28(1) of the Bill indicates how it relates to the Access to Information Act, and in an effort not to hinder access to information defers the granting of access to this Act. However, the *proviso* is that this information does not pertain to the restrictions in the proposed Information Bill which could override the provisions of the existing Access to Information Act. This deference is a reversal of the function to over-rule compared to earlier versions of the Information Bill, with jurisdiction given to the Access to Information Act to exercise due restriction in national security matters. This submission is fundamental "to any determination of the constitutionality of the Bill because, without it, the Bill clearly infringes the right to freedom of information" (Currie & Klaaren 2011: 27). This implies in principle that even 'top secret' information could in terms of the Access to Information Act be accessed if deemed prudent.

Finally, what is notable is that the Bill does not contain an explicit 'public-interest defence' clause. The Bill integrates the public-interest override of the Access to Information Act which stipulates the circumstances under which a request for access to information must be

© University of Pretoria

granted (see Appendix A). For instance when disclosure would reveal non-compliance with the law or a particular risk, or when the disclosure "clearly outweighs the harm contemplated in the provision in question" (Section 46). Related to the justification of information disclosure in the public interest is the extent to which said disclosure is criminalised, which prescribes whether the disclosure in the public interest is justified or not. Presently the Bill (Chapter 11 of RSA Bill 2010) criminalises the sheer access to, and possession and consequential disclosure of the information. The mere possession is criminalised and not the potential consequences of possession or disclosure of the information (Currie and Klaaren 2011: 24). What is further troublesome about the public-interest defence is the ambiguity of the concept, which much like the contested concept of national security, can be argued to support the particular interests of the requestor of information.

The Bill demonstrates a direct and succinct purpose within the information-society nexus with clear aims and objectives to improve the information-security framework. The principles of the Bill are commendable, but the practise of legislation is the veritable test of its soundness. As indicated, specific clauses of the Bill are contentious, drawing public criticism (see section 3.4). In so far as the Bill's implementation is analogous with what is already stipulated in legislation, it should not contravene or be in contention with existing laws. This is guaranteed as a result of the extensive legislative process.

3.3 The legislative process of the Information Bill

The Bill (in a preparatory form) has been in circulation since 2006/2007 as a response to the reforms on the inadequacies of the state information system. The first official draft version of the Bill was introduced to Parliament in 2008 and the second in 2010. Since then the Bill has been submitted to Parliament and returned to the President for review and/or amendment of contentious aspects, and to edit technical errors before it can be ratified and promulgated into law. Since this chronological sequence of the legislative process has a bearing on the securitisation of information, a brief overview of it is presented[33].

[33] The Parliamentary Monitoring Group (PMG) offers a comprehensive timeline of the legislative process; www.pmg.org.za.

© University of Pretoria

Chapter 4 of the Constitution makes provision for the legislative process. Parliament consists of the National Assembly (NA) and the National Council of Provinces (NCOP), both of which participate in the legislative process. In terms of parliamentary procedure, the State Law Advisers and the Ministry of State Security opined that the Bill be dealt with in accordance with the procedure established by Section 75 of the Constitution which refers to 'Ordinary Bills not affecting provinces'. Parliament must accept or reject the Bill, with or without amendments, and thereafter submit it to the President for assent.

The formulation of the Bill was led by the former Ministry of Intelligence (now the SSA) and included representatives from the departments of Defence and Justice, the South African Police Service (SAPS) and the South African National Defence Force (SANDF). The 2008 version of the Bill, one of three pieces of intelligence-related legislation considered by an Ad Hoc Parliamentary Committee on Intelligence Legislation, was withdrawn towards the end of 2008 after the Committee had voiced serious concerns about certain aspects and the pressure to complete amendments in a short space of time (Hartley 2008).

At that point institutional changes occurred within the intelligence services, along with the fact that the withdrawal of the Bill coincided with the resignation of former President Thabo Mbeki. At the time it seemed that the process would become more inclusive of South African society in order to portray a more unified and accepted piece of legislation. In this respect the former Intelligence Minister, Ronnie Kasrils[34] (2010), admitted that "prior to the submission of the Bill to Parliament in 2008 my technical drafting committee obtained extensive inputs from public sector departments and legal experts. They did not however have an opportunity to sit down with civil society experts." As it would be seen, civil society reaction to the Bill would become more robust and outspoken.

The new Minister Siyabonga Cwele of the newly formed SSA oversaw a revised version of the Bill, introduced in 2010 to a newly-elected Parliament as the *Protection of Information Bill 6 of 2010*. The Ad Hoc Committee on Protection of State Information Bill of the NCOP and the

[34] Minister Kasrils spearheaded the formulation and introduction of the Bill to Parliament when he was in office.

© University of Pretoria

NA[35] was formed in September 2010 to address the revision of the Bill in light of the public furore. The 2010 version of the Bill differed significantly from its predecessor but still did not meet public approval as many of the stipulations and penalties had become more severe, with redundancies of administration removed almost as compensation. The most significant changes are summarised by Currie & Klaaren 2011: 12: the deletion of the automatic declassification provisions; the introduction of severe minimum sentences to the already stiff penalties provided for in the criminal penalties provisions; the reformulation of the criminal penalties as turning on the fact of classification of a record rather than on its intrinsic classifiability; the introduction of a new offence of disclosure of a 'state security matter'; the introduction of a new general principle of state information to the effect that all the other principles are subordinate to the national security of the country and to ensure its resoluteness; and the removal of the 2008 requirement that each classification decision have a written justification

The revision and second release of the Bill garnered far more attention in the media than previously, with numerous publications showcasing the public outrage (including journalists, civil rights groups and political commentators) against the proposed legislation. The SSA (RSA SSA 2013) responded by referring to the positive aspects of the public hearings on the Bill, commending the participatory process through which the Bill had evolved into a more acceptable piece of legislation. This included both the process and the final normative and practical outcomes of the (expected) promulgation of the Bill. Addressing the public response, the SSA (RSA SSA 2010b) praised the democratic process that unfolded, encouraged the debate and public interest on national security and intelligence, and exclaimed that "this is a sign of our maturing democracy SSA." This process reiterated and reinforced the values of the Constitution in general and of the legislative process in particular.

In 2011 the Bill went before the NCOP Ad Hoc Committee where it was amended after further public hearings and submissions. Following this it served before and was approved by the NA in 2012 (RSA NCOP 2012). President Jacob Zuma did not ratify the Bill in 2013, stating

[35] The Ad Hoc Committee on Protection of State Information Bill (NA) was led by the chairperson, Ms M Smuts (Democratic Alliance) and included six additional members representing the African National Congress (ANC). The Ad Hoc Committee on the Protection of State Information Bill (National Council Of Provinces) was led by the chairperson Mr JJ Gunda and included 8 additional members (ANC 5, DP 2 and Inkatha Freedom Party (IFP) 1).

© University of Pretoria

technical errors that required revision – thus he referred it to the NA for reconsideration, a standard procedure in terms of section 79(1) of the Constitution. Following this deliberative 'hither and tither' of the legislative process, the Ministry (RSA SSA 2013) expressed their appreciation for and concurrence with this process, having "enriched the bill, creating a better balance between the constitutional provisions of access to information and the limitation of that access in the interest of advancing our national security." The Bill has been sent back to the President for ratification where it remains unsigned (RSA PMG 2014). Since then and apart from not being ratified, neither extensive media coverage of the Bill nor any reports (of the Justice, Crime Prevention and Security (JCPS)) cluster or in the media archive of the SSA provides any indication of further developments or future prospects.

3.4 Critique of the Information Bill

With the temporary stasis of the legislative process it is possible to review the critique of the Bill. This critique – if considered in terms of arguments for and against – is indicative of the consequences of the Bill's implementation on security and information. As such, the critique provides an additional context for the question on the securitisation of information.

Having been met with resistance in the form of the Government's determination to pass the Bill, and with the realisation that the public might be powerless to prevent it from being promulgated into law, activists tried to at least improve specific clauses of the Bill – found to be draconian in nature and detrimental to the functioning of a free press in South Africa – by providing inputs at the public hearings of the Ad Hoc Committee on Protection of State Information Bill (NA and NCOP). As the Bill still is embroiled in the legislative process, greater awareness has evolved with each new development, as more entities have became involved in the consultative process and the public interest in the Bill has increased.

3.4.1 Commendation of the Bill

Although to be expected that the commendation of the Bill mainly emanates from the State, the SSA has indicated its support for the Bill throughout the legislative process to ensure that the legislation helps to "avoid making it more difficult for citizens … to obtain information from government departments and other organs" (RSA SSA 2010b). Essentially the SSA accentuated the normative benefits of the Bill for the country and further afield, "in

© University of Pretoria

transforming our society from a culture of secrecy and repression to one of transparency, accountability and responsiveness and to become a leading precedent for open and democratic governments the world over" (RSA SSA 2010b). These supporters spoke to a more nuanced notion of the information-security landscape in which they operate, where the benefits of the Bill's provisions could be realised; the challenge being to align these gradations with those of the broader public good.

An overarching criticism of the *Protection of Information Act*, *1982* is its lack of specificity on espionage and subversion that makes these actions easy and even attractive to perpetrate. To accommodate a more effective persecution paradigm, the Bill aims to repeal the Information Act. Hence the argument that the proposed legislation should be sufficiently stringent in its framework and application to act as a deterrent to anyone committing intelligence activities against the state. The more rigid and severe provisions of punishment and sentencing for crimes committed in terms of the Bill confront those acting with impunity in the current realm with more severe consequences and are concurrent with international norms and standards for security law. The SSA has emphasised the underlying notion of human security in the Bill and that the focus of the objectives is protection and not non-disclosure of valuable information (RSA PMG 2012b, c & d).

Another positive aspect of the Bill is its recognition of the maladministration of state information by the previous regime through the "classification, reclassification and declassification of sensitive information which later becomes accessible (RSA SSA 2013). Since the *Protection of Information Act*, *1982* did not make such provisions, having records on file is regarded as essential to promote transparency and to eliminate secrecy. However, these records are only useful if they can be accessed by relevant parties, specifically civil society stakeholders who use this information to conduct oversight. The streamlined functioning of the proposed reforms should ensure that the Bill contributes to an open information-security landscape. The provisions of the Bill underline this approach.

In response to the public interest defence clause - a major concern of the critics - the Ministry defended its efforts to align the Bill with the *Promotion of Access to Information Act, 2000*; the *Protected Disclosures Act, 2000* (Act 26 of 2000); and the *Companies Act*, *2008* (Act 71 of 2008) – that is with existing legislation that protects the public's 'right to know' and prevents

© University of Pretoria

unlawful and unnecessary concealment of state information. Kasrils (2010) indicated that the 2008 version of the Bill contained a public-interest defence clause as it "is a vital requirement and if not included would certainly generate the impression of a government and ruling party wishing to conceal its own misdemeanours by obstructing investigative journalism." However, hitherto, the ANC as ruling party is steadfast in its exclusion of such a clause – a perception created in the public arena that amplifies criticism against the Bill.

The Bill also included the Classification Review Panel which has immense powers to oversee and review the classification powers of the Security Services and Oversight Structures (see Chapter 11 of the Constitution) (RSA SSA 2011). Kasrils (quoted by Ferreira 2012) posited that "the government must fight a tendency among ministers to clamp down on transparency and 'improve' the bill that is seen as an attack on media freedom and a return to apartheid-era repression." In order for the Bill to be the intended progressive benchmark, the original principles underpinning the legislation must remain fundamental to each revision and amendment.

A final important argument in support of the Bill is the Government's acknowledgement of the role of ICT (in the current and future arena of state operations) and the need to include digital- and cyber-related features that are imperative for the security of a country of South Africa's standing. According to Duvenage (2016), South Africa is not cyber secure, resulting in the "compromise of sensitive information, impeded functionality of systems and other detrimental effects of other malicious cyber activities (of various forms and motives)". Notwithstanding the fact that cyber-intelligence has only become a serious national security priority of South Africa over the last decade, the inclusion of ICT in the legislation accentuates a forward-thinking approach. The enhancement of the critical information infrastructure of the state is vital to ensure and maintain a competitive advantage in global politics.

3.4.2 Criticism of the Bill

The Bill has been criticised by public interest groups, pro-freedom press and non-profit/non-governmental organisations (NPO/NGO), media forums and political analysts. The most prominent criticism emerged from the R2K, the South African National Editors Forum (SANEF), the Black Sash, Human Rights Watch, Print Media South Africa (PMSA) and the

© University of Pretoria

Freedom of Expression Institute, alongside the DA as the official opposition party in Parliament.

The overarching criticism of the Bill, which has been expressed most vocally by the mainstream media houses of the country, is that it is an affront to South Africa's democracy as a whole. The Bill is seen as a restriction on the free press and, as such, the limitation of access to information is tantamount to a regression of a hard-won and yet infant democracy. Nic Dawes, the former editor-in-chief of the prominent *Mail & Guardian* newspaper expressed his disappointment with the details of the Bill which he claims detracts from the initial positive and necessary aim of the legislation. He argued that "its intentions—to create an appropriate democratic framework for the management of sensitive information—were laudable. But these were rendered meaningless by the provisions that would have a chilling effect on the dissemination of information by the media or elected officials in the pursuit of democracy" (quoted by Donnelly 2010). The role of the Bill in consolidating specific aspects of information security and protection in a democratic South Africa is significant, but its criticism renders it difficult to trust the initial ethos of its objectives.

In a newspaper editorial in the *Mail & Guardian* (2013), the negative consequences of the passing of the Bill were summarised as follow: "The tendency by governments to shift their more dubious activities away from public oversight by way of security classification is a global phenomenon. We would be foolish to think ours is immune to such temptations. This is even more so with the adoption of the Protection of State Information Bill." The Bill is taken at face-value by its dissenters who focus on specific clauses that detract from the primary goal of the Bill in the information-security nexus.

Andre Brink (2010), the famed South African author and recognised 'opinion-maker', encapsulated the severity of the situation in South Africa in an Op-Ed piece in the *New York Times*: "South Africa faces its starkest challenge yet in the form of two pieces of anti-press legislation that would make even the most authoritarian government proud." Referring to the Bill, Brink drew a comparison to language typically utilised by the apartheid regime in its censorship of information, viewing the Bill as an encroachment on the very essence of the country's democracy. He was clearly troubled by the introduction of this legislation, as he believed it erodes freedom of expression as the last remaining citadel of South African

© University of Pretoria

democracy. To emphasise his opinion, Brink (2010) admonished the former Mbeki administration and the current government for their dismissal and fear of criticism, to the extent that "a new kind of silence that is threatening to take the place of ordinary communication" is begotten. The recall to the ethos of the apartheid-era underscores the concern with the actions of Government, and the suspected regression to a draconian environment characterised by limitations of and restrictions on civil liberties.

Another dominant criticism of the legislation is the lack of a substantial and efficient public defence clause, in that so-called whistleblowers would be deterred by the law for the mere possession of so-called illicit information. The SANEF, PMSA and the South African Human Rights Council (SAHRC) made submissions during the public hearings that expressed their concerns in this regard (RSA PMG 2012e). Following these public hearings, amendments to the Bill were made which serve to satisfy the complaints. Specifically, the Bill now includes "protection of whistleblowers and those who expose corruption from prosecution and a public interest override that provides a simple mechanism for a person to apply for access to an organ of state for access to a document and if refused may appeal to the head of an organ of state, the relevant Minister or can apply to the court (RSA SSA 2012; see Appendix C where applicable).

Furthermore, the Bill was criticised for its unconstitutionality. These claims derive from the perception of incompatibility of it with specific clauses of the Bill of Rights (Chapter 2 of the Constitution), namely Section 16 *Freedom of Expression* and Section 32 *Access to Information*. There are no specific clauses in the Bill itself that contravene the Constitution but on a normative basis, it is seen to disrepute the very notion of constitutionalism. According to clause 7(2) of the Bill of Rights, "the state must respect, promote and fulfil the rights in the Bill of Rights", but equally pertinent is the restriction placed within the Bill of Rights (Section 36) whereby the these rights are subject to specified limitations. The criticism of the Bill is that Government may, as a national security measure, utilise the constitutional limitation of rights to justify the concealment of information expediently for personal political advantage.

What is problematic at this stage of the legislative process is the scepticism that now surrounds the Bill, which is not likely to dissipate going forward. Over the last five years, public awareness of the Bill has increased, with civil society actors becoming more

© University of Pretoria

pronounced and vitriolic in their opposition. In a sense, these actors have amplified the furore surrounding the Bill, endowing it with attention it probably would not have received initially. The reaction to the Bill and the tumultuous legislative process that has ensued contributes to the felicity conditions that enable a situation of securitisation.

4. Conclusion

This chapter presented a description of the context and detail concerning the Information Bill. The Bill was premised with reference to its historical, political-security and legal context; its aim, objectives, key provisions and development process; and its critique in terms of arguments both in support and against the proposed legislation and/or specific aspects thereof. The legislation aspires the reformulation and regulation of the information-security nexus within which the state operates, with the aim of improving the security framework of the country. Practically, the Bill reformulates the classification and declassification system to reduce excessive amounts of state information that are routinely classified. This is to be done by repealing and replacing the existing archaic *Protection of Information Act, 1982* that currently defines the information-security landscape in South Africa. The role of the Bill in consolidating specific aspects of information, security and protection is significant, but its criticism compromises trust in its initial ethos. It would seem that the manner in which the Bill has been viewed publically, by its fiercest critics, is the antithesis of how the Government intended it to be received. The bellicose atmosphere surrounding the Bill during the legislative process contributed to the suspicion and scepticism of it, prompting the premonition to analyse the Bill as a potential case in point of the securitisation of information in South Africa.

Supporters of the Bill espouse that it should be seen as part of an over-arching restructuring of the information-security nexus, with the ultimate goal of protecting the national interest and ensuring national security for a globalised state in the 21st century. By its detractors, the Bill has been criticised for its draconian approach to restricting information from the public, using the arbitrary notion of national security as justification for its concealment. Critics claim it infringes on Constitutional rights, namely freedom of expression and access to information, making it detrimental to democracy. Nevertheless, amendments to the Bill have proven instructive and fruitful as clauses that provide more protection for whistle-blowers and

© University of Pretoria

acknowledge a defence in the public interest, have been included – although these amendments have not gone far enough to satisfy the disparagers.

The systemic legislative process, the subjection to critique by civil society actors, and the reformist work of the Ad Hoc Committee on the Protection of State Information (NA and NCOP) demonstrate the substantial and progressive process, as well as the level of consultation and participation in the democratic arena. This collaboration to produce a piece of legislation that will ultimately contribute positively to South Africa's proliferating information society should be condoned, to the extent that it is not abused by the state. The consequence of such a situation would be the deliberate securitisation of information to benefit those in power.

By introducing the context and specifics of the case study – the Information Bill – in a structured manner this chapter was primarily descriptive in nature. It contextualised the Bill and depicted the factors that arguably may have created enabling (or felicity) conditions for the securitisation of information in South Africa. Hence the analysis of this possibility in the next chapter involves the application of the tenets and elements of securitisation theory (as discussed in Chapter 2) to the case study (as described in this Chapter).

© University of Pretoria

CHAPTER FOUR

THE *PROTECTION OF STATE INFORMATION BILL, 2010* AND SECURITISATION THEORY: AN ANALYSIS

1. Introduction

The aim of this chapter is to determine whether or not a securitisation of information has occurred in South Africa, and to assess the impact of this information-security relationship on the broader security environment of the country. For analytical purposes, the tenets and elements of Securitisation Theory are applied to the case study. The underlying assumption is that this information-security nexus is, amongst others, indicative not only of the current security thinking of state and government, but also of the national security concerns and accordingly of the relationship between information, national security and national security policy.

As a point of departure and introduction, the politicisation of information is briefly explained within the South African context. With reference to the case study the following elements of Securitisation Theory will be explored in sequence: the securitising speech-act; the securitising move with the inclusion of the presentation of an existential threat, the persuasion of the audience by an authoritative securitising agent, and the significance of historical context; the preponderance of extraordinary measures; and the possibility of desecuritisation. This forms the basis for an assessment of whether or not information has been securitised in South Africa.

2. The application of Securitisation Theory to the Information Bill

The securitisation of an issue, which would entail its positioning at one end of the political-security spectrum and removing it from the regular public-political environment at the other end, depends on how political and security actors (a government in particular) approach and manage it.

2.1 The politicisation of information

Keeping in mind the illustration of the spectrum (see Figure 1), politicisation is addressed first. Significantly, the notion of information as it is used in a habitual manner is not neutral, and is thus already placed along the spectrum. It could be argued that information, intrinsically and to the extent that it (purportedly) comprises of and conveys objective empirical data, is non-political. Information then becomes political through its nature, gathering, interpretation and

© University of Pretoria

use in the official domain of governance, being integral to all policy, policy-making and policy implementation within a state bureaucracy. This is even more so the case when official perspectives of, and policy and legislation on, information as such are enacted upon by state institutions, namely the security services. Accordingly and in the South African case, politicisation is evidenced by three developments, namely the legislation on information, political contestation over information, and the administrative institutionalisation of information generation and use.

Firstly, the fact that information is extensively covered by legislation in South Africa, both pre- and post-1994, is indicative of its politicisation. Legislation[36] has been created and implemented that aims to protect both public and private information – with regard to the scope of its use, its dissemination and its necessary concealment. The seminal *Promotion of Access to Information Act, 2000* offers a platform to exercise the right to access information, thereby encouraging a more transparent available information society. Notwithstanding, the existing and all-encompassing *Protection of Information Act, 1982*, that will be repealed with the expected promulgation of the Bill, is also indicative of its politicisation. The Bill itself, as a product of the legislative process and formulated by Government, is politicised.

Secondly, the controversies surrounding the Bill and contestation of information and access to it also confirms the politicisation thereof. Both detractors and supporters of the Bill are at pains to demonstrate how the proposed legislation is an exercise of rights, albeit from opposing perspectives. This is underscored by the purported deficiencies of the Bill, and counter-arguments thereto, as contended by both supporters and critics of it. In addition and as a point of reference, the proposed legislation is a political instrument to control state information, specifically to prevent it from being used against the Government in any way. This use of legislation on information and its alleged manipulation (or potential manipulation) is also a form of politicisation. In contrast, and as a form of political contestation, those who oppose the Bill perceive the expansion of the security services and the consequential control over information to be incongruent with the broadening of freedoms of expression and

[36] This legislation includes but is not limited to, the *Protection of Personal Information Act, 2013* (Act 4 of 2013); the *Protected Disclosures Act, 2000* (Act 26 of 2000); and the *Companies Act, 2008* (Act 71 of 2008).

© University of Pretoria

information access. As Holden and Plaut (2012: 128) contend, the mere introduction of authoritarian laws perpetuating a culture of secrecy will engender “a crackdown on the free flow of information by those so happy to use disinformation for their own ends”. In the case of South Africa, the intelligence services and the media, through information, have become engulfed in each other’s domain of operations.

Thirdly, from the operational perspective of the state and intricately connected to information as a resource, the intelligence structure and institutional framework of security services politicise information as part of the state administration that makes use of information at the very core of its functionality. A horizontal extension of this, in the South African case, has been the politicisation of the intelligence services. This is exemplified by the structural changes of the intelligence services in 2009 and the expansion of the role and jurisdiction of the JCPS cluster at the behest of the President as head of government. This large-scale operational and structural adjustment of the intelligence services is foreboding due to the extra power it bestows on Government. As skeptical as this expansion may be, it must be viewed in light of the uncertainty of the local and global operational environment in which the state operates.

In navigating the political-security spectrum, it is expected that the politicisation of an issue (or entity) is systematically followed by the securitisation of that issue (or entity). What follows below is whether or not information – beyond politicisation – has been securitised through the introduction of the Bill (if not in its entirety, then partially); and whether or not, and to what extent information has (deliberately) been moved (implicitly) beyond ‘normal’ politics? A response to these questions requires an application of the remaining elements of securitisation theory to the South African example.

2.2 The securitisation of information

As a domain-opposite and horizontal extension of politicisation, that implies the removal of the issue or entity from the political realm and transferring it to the strategic realm of security, securitisation involves a ‘speech-act’, a ’securitising move’, and extraordinary measures.

© University of Pretoria

2.2.1 The securitising speech-act

The primary tenet of the theory of securitisation, in anticipation of an instance of securitisation, is the speech-act: i.e. the act of 'saying security' in relation to an issue – "(t)he *word* 'security' is the act" (Wæver 1995: 55). In the South African context of an expanded intelligence environment and a growing sense of security paranoia, the Information Bill is the speech-act itself, by explicitly providing a security context to information and more specifically state information on state security matters of a valuable, sensitive and secret nature (these words and definitions are used in the Bill itself). The mere reference to national security (based on national interest) as the underlying concept for the justification of limits to the access to information immediately envelopes the legislation in a security context. These security justifications are evidenced by the following sections of the legislation that demonstrate the preoccupation with achieving security, in both the restriction and protection of information in the name of national security, and in its disclosure for the safety and security of the public.

For example and amongst others, and as one of the underlying principles of the legislation, in Chapter 2 Section 4(e) it is contended that "the free flow of state information can promote safety and security", whereby the necessity of the disclosure of state information is understood to be a contributing factor to a better informed and more aware citizenry, and to a safer and more secure public arena. In spite of the list of general principles that underpin the applications of the legislation, a recourse to national security is predominant, evidenced amongst others by article (j) in Chapter 2: "in balancing the legitimate interests referred to in paragraphs (a) to (i) the relevant Minister, relevant official or a court must have due regard to the security of the Republic, in that the national security of the Republic may not be compromised". In respect of 'saying security', the state has contributed to the speech-act securitisation through media releases by the SSA with regard to the introduction of the legislation: "this Bill has been the subject of discussion across various platforms and has earned the status of the most talked about security law" (RSA SSA 2012); and "the Bill would contribute to an improved national security status of the Republic" (RSA SSA 2013). These reiterations accentuate the speech-act of saying security.

The exclusivity engendered by the potential limits on the access to state information perpetuates the sentiment of the detractors of the legislation that this issue of information is

© University of Pretoria

now removed from the public-political domain, to be dealt with on a select basis by a restricted (and arguably exclusive elite) group of government officials (or even securocrats). From a superficial perspective of the speech-act as the utterance of security, the legislation performs this function. Notwithstanding this indication of the securitising speech-act, critical to its credibility, is whether the Bill itself – in its entirety – presupposes a limitation of rights grounded by section 36 of the Bill of Rights (detailed in Chapter Three); or if each individual request for access to information brought to the state and the exercise of the proposed legislation to restrict access to the requested information, could possibly have a limitation. Information itself is not necessarily securitised if the Bill itself does not constitute a limitation of the aforementioned rights, hence not shifting information to a separate 'security-enhanced' realm. If only specific sections of the Bill 'securitise' information by means of denying access to that information for legitimate national security reasons – which is justifiable, tolerable and even expected (within the legitimate mandate of governance of the democratic state), then the Bill cannot be representative of a speech-act in and of itself, as it has been depicted by some of its critics. Rather, the Bill can be thought of as securitising some aspects of information. This kind of securitisation is not necessarily as surreptitious or detrimental as it may seem, or as is espoused by the disparagers.

But how can the word 'security' (used in respect of information) be performative, or explicate an action, if no-one accepts it or the audience isn't taken into consideration? This has been a main criticism leveled against the 'speech-act' element in Securitisation Theory, in that *only* the utterance of 'security' is too simplistic and superficial to produce a security paradigm shift. Scholarship augments the foundational notion of 'security' as the speech act, whereby "it is important to note that the security speech act is not defined by uttering the word *security.* What is essential is the designation of an existential threat requiring emergency action or special measures and the acceptance of that designation by a significant audience" (Buzan, Wæver & de Wilde 1998: 27; original italics). The speech-act requires more action than the mere utterance of the word security in order to sufficiently and substantially designate the issue to the security domain. What in fact is required is a securitising move that also involves the extraction of a deeper understanding of the speech-act: the designation of an existential threat and its acceptance by an audience concomitant to the process, contextualised by history.

© University of Pretoria

2.2.2 The securitising move

Whereas the speech act refers to 'saying security' in relation to information as an issue, the securitisation move involves the 'labelling' of the information issue as a security issue. Considering specific clauses in the draft legislation, principle 'g' (Section 6) for example refers to "some confidentiality and secrecy … to protect national security". This labels the underlying notion of the legislation as having a national security perspective. But this presumption of confidentiality and secrecy is a reasonable limitation and utilisation of concealment of information where national security is at stake, and it implies respect for the restrictive provisions in the Constitution. Section 11 (2) and (3) details the multidimensional national interests of the state which encompass the sensitive information that must be protected by the state, whereby the relevant legislation must be implemented to give effect to the protection of sensitive information. The definitions outlined in the Information Bill for security, information, legitimate interests and state security refer to a tolerable and reasonable expectation of protection and fulfilment of objectives of the legislative framework on which the Bill was based.

As the antithesis of 'labelling' information as a security issue, the General Principles of State Information (Section 6) of the Bill reveal a commitment – at least in principle – to a transparent and accountable information society that does not have the concealment of information as its primary aim. For example and in the practical application of the security law, the classification rubric proposes legitimate grades for the designation of information according to sensitivity. However, the classification is an independent judgment interpreted by the acting authority. This implies that, to begin with, not all information is necessarily labelled as 'security' but rather particular information that will be separately classified and thus afforded a security label. But the perspective of the Bill is still one of it being a labelling agent of security, which creates an inclination towards securitisation. If the state authorities have labelled security with reference to the Bill in a legitimate and legal manner that is expected of security law, it would be prudent to examine parties external to the state to locate the forms of securitisation-labelling that have contributed to the overall securitising move.

Ardent scrutiny of the media releases and public-awareness campaigns of the opponents to the Bill reveals a form of labelling that enhances a security perspective of the issue of information should it be passed, with specific reference to the right to access to information

© University of Pretoria

and its intended concealment by the government of the day. Blatant and purposeful references to the Bill as 'draconian' and the 'Secrecy Bill' have augmented the pejorative sentiments towards the legislation. This has contributed to secrecy paranoia that seems to have abounded in the last decade. As shown with the criticism of the Bill, its disparagers emphasised the security aspects at length. It can be argued that this represents an alternative and external actor to the Government who is responsible for the continued securitisation of information. The Government may have introduced the original speech-act, but it is players that occupy civil society space that have spurred the securitising move, creating the security-consciousness around the legislation. The opposing rhetoric to the Bill further enables the felicity conditions required to complete the securitising move.

This completion requires conditionalities to be met, namely the existence of an existential threat legitimising the use of extraordinary measures to combat that threat; the existence of a securitising actor who is in a position of authority to convince the audience of the severity of the issue; and the existence of historical connotations of threat, danger and harm, or of a history of hostile sentiments that spur and provide momentum to the securitising move (Peoples & Vaughan-Williams 2010: 79). The potential practical manifestations of securitisation through these three conditions are forthwith assessed.

(a) The presentation of an existential threat: An existential threat has been formulated by conceptualising information as security in the Information Age and, more significantly, the potential dangers to entities due to the disclosure and the security necessity of protecting certain information. In a dynamic world a revised and improved security framework is required to enhance a government's ability to ensure national security. The pursuit of national security to secure national interests consistently carries risks, as new threats emerge with changing environments that challenge existing notions or approaches to security. Cases in point were the immediate post-Cold War and the post-9/11 eras. As information about these threats and environments is integral to ensuring national security, it forms a vital part of the intelligence process that informs the decision-makers on their policy formulation roles. Consequently, creating a framework that prescribes a more effective and yet more nebulous information-security matrix is crucial to state and national security.

© University of Pretoria

Traditionally associated with the notion of national security being the ultimate objective of a state, "it is assumed that the state 'has to survive'" (Peoples & Vaughan-Williams 2010: 76). However, does the use of 'national security' within the Information Bill as a defence of its objectives and applications mean that the legislation responds to an existential threat? With the utilisation of 'national security' specifically, does the Bill project information into the security realm? Perhaps this development is a consequence of the stringent security-conscious applications of the legislation and not a purposeful action of the Bill. The Government has emphasised the troublesome loopholes in the existing legislation – specifically the Information Act – that must be amended to generate a more efficient information-security environment and to prevent weaknesses in the intelligence structure that can be exploited by external forces. The introduction of the Bill has been justified as part and parcel of this enhanced security framework, as a prerequisite tool for the protection of South Africa's national security.

The notion of 'national security' is utilised throughout the Bill, either to reinforce one of the objectives of the Bill which is to support the protection of national security, or to ensure that the concept of national security is used expediently as an override where discrepancies exist in terms of the classification and disclosure of information. The most notable utilisation of the national security defence is presented in the principles of the Bill, whereby all its principles (Chapter 2 Section 6 (a-j)) – as progressive and protective as they are towards human rights with regard to access to information and the transparency of South Africa's democratic system – are superseded by Clause j which states that all principles are "subject to the security of the Republic, in that the national security of the Republic may not be compromised". The pre-eminence of national security underlies the application and implementation of the legislation. Examples of the use of national security as a defence for specific provisions of the Bill are indicated in Section 17 (a) (c); Section 21 (1).

A national security defence is indicative of an existential threat, as the lack of that security measure would create a vulnerability to the continued existence of the entity under protection. The Government has intended the Bill to be perceived as enhancing the overall security structure of the state, to ensure continued protection, now and in the future, making provision for potential threats. Notwithstanding, the overuse of the national security defence however

© University of Pretoria

justified, has augmented the perception that the Bill addresses an existential threat that is manifest and needs to be addressed. The objects of the Bill (see Appendix B) outline the issues and systems that require regulation and improvement, to allow the Bill optimum application in the future as the new and improved information-security law for the country. These objects and the definition of national security utilised in the Bill are rudimentary defences for security legislation which can be interpreted as addressing a security vulnerability and not a manifest existential threat to the state.

In this scenario, the *state* is the referent object of security that faces the existential threat. The provisions of the Bill represent an attempt to protect state information from unwarranted disclosure, unnecessary classification and an outdated information-security paradigm within which to operate. The existence of the state in the Information Age and the efficient functioning of the government bureaucracy in the security-information nexus is under threat itself, and faces an existential threat.

In contrast, opposition forces within civil society believe their rights of freedom to access information and their very livelihoods and vocation are at stake, should the Bill come to pass. This threat is both at an individual level restricting the work of the free press and at a national level, whereby the activists claim the state's democratic future is threatened. Hence their argument that the Bill poses an 'existential' threat. However and arguably, the curtailment of liberal democratic rights does not necessarily pose an existential threat, but rather a limitation for the sake of a security requirement or *'security good'*. As much as the rights of these individuals and groups are enshrined in the Constitution, so too are the limitations to these rights where such a limitation is warranted for the protection of the national security of the Republic of South Africa.

What is questionable is the extent to which the media needs to be restricted in order for the security framework to be secure in its practice. The revised version of the legislation negates the appeal to an existential threat that the original version of the Bill intended to present, as the additional sections that remove a public defence clause and limit the access to information of the media create a dubious perception about the proposed legislation in its entirety. The audience is more likely to accept the proposed legislation if the aims of guaranteeing national security by developing a stronger security framework are not clouded

© University of Pretoria

by accusations from civil society of the state (potentially) controlling the press and concealing misconduct and/or maladministration by the state and government. In defence of the legislation, the SSA (RSA SSA 2013) explained that the introduction of the Bill will ultimately "creat(e) a better balance between the constitutional provisions of access to information and the limitation of that access in the interest of advancing our national security." The opponents of the Bill posit a mutually exclusive view of national security and information, implying a binary perspective of the information-security nexus.

(b) The persuasion of the audience by an authoritative securitising agent: The relevant targeted audience has to be persuaded by the securitising agent to accept the change in designation of the issue on the politico-security spectrum. Complete and effective securitisation is determined by the extent to which the audience acknowledges the argument put forth by the securitising agent, and accepts the changes to the *status quo* created by the securitisation of the issue. For the audience to be effectively convinced, the securitising agent must have the relevant authority, whether it be based on legal or moral grounds. In South Africa, the government of the day has been democratically elected to make decisions on behalf of its constituency, thus being a legitimate, legal and moral authority.

The Government at large[37] is the primary securitising agent who formulates and implements the policies on matters of security. It is supported in this endeavour by the democratically elected Parliament (the NA and the NCOP), who passes legislation. The legitimacy of the securitising actor, in this case the Government (based on the tripartite alliance dominated by the ANC) and more specifically the SSA (the department that initiated the Bill and will be responsible for its eventual implementation) is not questioned, *per se*, as their authority was gained through legitimate democratic processes. The population (at least in principle) trusts the government to make decisions in their best interest, especially regarding their security, since, quite significantly "one of the fundamental ways in which the post-apartheid intelligence dispensation differs from the apartheid legacy (is) that of its legitimacy. The services are established in terms of the Constitution, which lays the basis for their legislative framework"

[37] In this case the Government is made up by the relevant executive decision-making bodies, the National Executive Committee (NEC), the JCPS and the relevant government departments directly involved, the SSA.

© University of Pretoria

(Africa 2009: 76). This underscores the profound task of ensuring the authority and uncompromising rule of the Constitution. Equally significant is the maintenance of the separation of powers, the autonomy of the judiciary and the prudence of Parliament to promote and pass laws that contribute to effective governance. As soon as the public begins to doubt the legitimacy of government and/or the state institutions, the authority of the state dissipates.

As a case in point, the performance and actions of Government of late are also in part responsible for the reluctance of the public to succumb to the idea of the state expanding the intelligence services and restricting information, especially at a time when South Africans have become accustomed to a democratic process, at least in terms of their understanding of democracy. Over the years unsettled issues from each government administration have compounded, notwithstanding that these "unresolved tensions have deepened under the Zuma administration" (Africa 2012: 127). Consequently, the current administration is dealing with a disillusioned and yet active political public who have come to view Government propositions with skepticism by default. Credibility is vital for the continued authority of the securitising agent, making "certain issues and objects easier to securitize than others depending on the associated connotations" (Peoples & Vaughan-Williams 2010: 79). The contentious dynamics surrounding the Zuma administration and the post-Local Government Election dynamics fuel the battle of the persuasion of the audience.

In the same light, the legislative process that the Bill has followed is equally significant as it demonstrates the legality of the legislative process, the legitimacy of the securitising agent in conducting its task, as well as the legitimate persuasion of the audience (in this case the public, the media, civil society, and the free press). Detractors of the Bill – vibrant, vocal and influential as they are, have been vociferous in their opposition to the Bill, making their ultimate persuasion in terms of their securitising move a greater challenge to the Government. The robustness of South Africa's civil society and the influence of the private sector underlie the contestation of the legislation and underscore the reasons why the public cannot be so easily persuaded to accept the Government's securitising move.

Thus it can be said that the persuasion of the South African audience is more delicate and complex than the Government had initially anticipated. This challenge also spurred the creation of the Ad Hoc Committee on Protection of State Information Bill (NA and NCOP) and

© University of Pretoria

various consultative engagements that have since been put forth by members of civil society and government institutions. The fact that the Government has taken the criticism of and submissions made by the opponents of the Bill into consideration, is evidence of a partial acceptance of the perspective of the opposing side. By allowing concessions during the legislative process, the securitising agent was able to gradually create a more agreeable piece of legislation to be passed, ultimately persuading the audience in the second securitising move to eventual acceptance (even if reluctantly) with securitisation as the final result.

(c) The significance of historical context: The recent history of South Africa since the 1970s is a forewarning of what kind of governance and policies must be prevented from coming to fruition in the new South Africa. This process of governance is to be expected, especially with regard to the security milieu because "South Africa emerged from a bitter past where some of the intelligence and security agencies were in the forefront of oppression against opponents of the apartheid regime, and there is a fear of returning to a situation where the agencies interfere in politics" (Africa 2012: 101). This underscores the public skepticism of the expansion of the security services. With reference to the securitising move, what is important is whether the historical context contributes to securitisation or not; whether there exists an inclination to avoid any kind of recurrence of or reverting to the security paradigm of the past: or whether a higher security alert is welcomed since it may offer the country and the populace greater protection in an age of uncertainty and unchartered waters, being in the early stages of the democratic dispensation in the 21st century.

In contrast to the governance structures in place today, the apartheid-era governance required and practiced near-complete control of the press. A secretive and impenetrable security network, to protect the regime and maintain its dominance, relied on "a pervasive, repressive security apparatus" (Africa 2011: 1). With the transition to democracy, these processes had to be deregulated and dissolved. In its running of the country for the past twenty years, the ANC-led tripartite government has been sensitive to and considerate of the history of the country, often using the policies and practices of the apartheid era as an example of the contrast that is being cultivated in a democratic South Africa.

Ironically the original conception of the Bill is still respected, in spite of its vague conceptions and broad utilisations of national security and associated notions. Especially so in terms of its

© University of Pretoria

aim to create a better regulated and systemic information-security framework within which government officials can operate; and to safeguard state information that informs intelligence and counter-intelligence, with the protection of the country in mind. Despite these measures, the areas of focus were the absence of a public-interest defence clause, the hefty sentences and punitive measures, and the broad scope of the application of the Bill. This has produced a pejorative perspective of the Bill, which fostered the likeness to the draconian restrictions on individual freedoms and human rights reminiscent of the apartheid state. As a result, the government has not only failed to emphasise the positive and necessary secretive aspects of the Information Bill, but has exacerbated the anti-secrecy sentiment of the targeted audience by retaliating to the criticisms of the press.

The media simply has to remind its audience of the dark days of the apartheid regime – the darkness as an analogy of the concealment of information – in which the press was restricted to the point of being ineffectual, unless it was reporting partisan to the state. The relatively short time lapsed since the end of apartheid is significant enough that any inclination towards a regression of policy, action or development is still conceivable and therefore a matter of concern. The Government, through the introduction of the Information Bill, has attempted to embed a revised framework for the security sector in the abolishment of an existing and active apartheid-era statute and by creating an information-security paradigm that guards against the encroachment on civil liberties as was the case in the past.

With regard to the significance of history, the Government adopts a directive that emphasises the necessity of this kind of legislation, to ensure the establishment of safeguards to protect the people and the country from any kind of atrocity, whether they be similar to those committed in the past or not. Supporters of the Bill posit the advances that the legislation will establish in terms of minimising an unchecked information-security sector, which was pervasive during apartheid. For example, the actions of the Bill that most represent a breakaway from laws prior to 1994 are to prevent the wholesale destruction of information; to prevent threatening entities from gaining access to state information; and to not rely on apartheid-era legislation.

© University of Pretoria

2.2.3 The preponderance of extraordinary measures

In conjunction with the three conditions of the securitising move, the magnanimity of extraordinary measures is crucial to the process of securitisation. It is expected that the securitisation of an issue, as it is removed from the public-political domain, allows for the prevalence and preference of extreme methods to address the issue and its surrounding circumstances. Congruent to the argument that an existential threat exists is the invocation of extraordinary measures to contest this threat; measures for example in the form of extra resources, emergency decrees and presidential proclamations. Essentially, survival through security "is when an issue is represented as posing an *existential threat* to the survival of a referent object" (Peoples & Vaughan-Williams 2010: 76), which then requires more extreme and unusual measures to combat. The national security defence within the Bill has been labelled by critics as vague and broad, in order to purposefully encompass a range of caveats for the restriction of information should the need arise. Precisely for this reason, this flexibility allows the state to attempt to combat all manner of threats that may arise, which is a prerequisite in the uncertain environment of the international arena within which South Africa is a key and keen role-player.

The Bill itself is a representation of an extraordinary measure by the state to fulfil a particular obligation, in this case to ensure national security. But within the realm of security law and minimal expectations of a state to protect itself, the Bill is ordinary, if not necessary. Apart from this one perception of an extraordinary measure, the Government has not conveyed any inclination to accelerate the legislative process in order to ratify the Bill any quicker. As a matter of fact, a more inclusive and consultative course of action has been adopted whereby the suggestions of interested parties have been considered and in several instances, been adopted. Whether this has been a strategic measure by the current administration to appease detractors or not, the legislation has ultimately benefited from this process.

So what can be termed 'extraordinary measures' are in actual fact rudimentary precautions on behalf of the state to protect itself (its people, its territory, its existence) against elusive threatening factors in an indeterminate global climate. Adopting measures with the purpose of enhancing a security framework to address the current national security needs of the state is not an extraordinary measure, but rather an expected development of a country that has

© University of Pretoria

national security as an objective. This national security encompasses the continued peaceful existence of its people within its territory.

2.3 The desecuritisation of information

While securitisation enhances the security component and conception of an issue or entity, 'desecuritisation' encourages the opposite notion of drawing the security connotations out of the original understanding or conception of an issue or entity. Desecuritisation involves "shifting issues from the realm of emergency politics back into the realm of 'normal' political deliberation and haggling" (Wæver 1998: 71), which indicates a reversal on the spectrum. Given the demonstration already used of the progression along the political-security continuum, it is warranted and necessary to observe how the concept of desecuritisation could factor into the debate on information-security in South Africa, especially considering the proposed Information Bill.

Through the legislative process several adjustments were made to the legislation, not only to make it more agreeable to its critics, but also to ensure it remains true to its normative (if somewhat tenuous) principles. Through revisions of the Bill, a stronger and wider public-interest defence clause has been added, which alludes to a desire, at least on paper, to not only protect the public's right to know and have full access to state information, when it is deemed in the public interest to know, but also to allow more credence of what the public has a right to know. The scope of information to be classified has been reduced, both in terms of what information becomes restricted (and at what level) and what type of information is to be protected. Consequently, the majority of commercial information that had previously been included has now been removed, narrowing the application of the Bill. These changes are indicative of a narrowing of the administrative and normative notions of *doing security*.

The most crucial change to the Bill during the legislative process has been the strengthening of the alignment of the Information Bill and the Access to Information Act. Most significantly, the Information Bill is no longer able to override this Act when it is deemed that the right to access to information is greater than the need to restrict that information. Any permission that grants access or disclosure of information by this Act must be in harmony with the lawful limitations of rights, as the Act is also bound by the limitations of Section 36 of the Constitution.

© University of Pretoria

In addition the mere discussion and analysis of an issue or object in terms of security, for example the public and academic discourse on the issue, involves 'talking security' and enhancing the security speak[38]. Subsequently, the fact that the Bill is not prominent in the news at this time could hint to a form of or beginnings of a descuritisation process. The Bill has still not been ratified and has disappeared from daily discourses, which are signs that suggest its removal from a securitisation space. It can also be argued that the lack of information about the Bill can be considered a deliberate avoidance strategy on behalf of the Government to remove 'security speak' surrounding the Bill that epitomises desecuritisation. However, the fact that the Bill is still embroiled in the legislative process speaks to the entrenched security consciousness.

In spite of the aforesaid, the Bill does not present a strong case for desecuritisation. The attempt at appeasing the critics of the Bill and adapting it to more amenable public demands does hint that the state does not want to exaggerate the security component to the extent that it engenders fear and suspicion with the public. Nonetheless, this is not an expression of desecuritisation as it is to be understood, along the political-security spectrum. Furthermore, if full securitisation does occur as a result of passing the Information Bill, it is difficult to see how information can be desecuritised. That is, de-coupled or separated from security entirely, since the two concepts are analogous to survival in the 21st century and critical to the successful operation of intelligence services now and in the future. The overall expansion of the intelligence services of which the introduction of the Bill is a consequence, can be placed more towards the securitisation than the desecuritisation end of the spectrum.

3. The Information Bill: A case of securitisation or not?

Based on the preceding analysis of the speech-act and the completion of the securitising move, an interim assessment of securitisation is conducted. It is evident that the Bill itself, in its entirety, offers the most expedient form of the speech-act, representing the act of 'saying security' as it positions information within a security paradigm, reinforcing the original fundamental purpose for the formulation of the legislation. The completion of the securitising

[38] See Eriksson (2001) for further reading on the dilemma of separating the securitising agent from the analysis of securitisation.

© University of Pretoria

move is more complex to articulate, as it involves three separate elements that need to coalesce to produce securitisation. It can be argued that throughout this process, as the Bill has undergone numerous adaptations, there have been degrees of the notion of securitisation, often having blurred the lines with politicisation.

The 2008 version of the Information Bill did not remove information from the public domain *per se*. Rather, it used information within the security framework as is necessary and readily accepted for a state, as certain information is understood to be secret and restricted from the public. As a result this kind of exclusivity to state information is not necessarily a securitisation, although it does incorporate elements that relate to Securitisation Theory. The Government did use the unspecified notion of national security to justify the extent of the limitation measures regarding information access in the legislation and the severity of the punishments and criminal designation of the possession and dissemination of state information, fostering a broader scope of action *vis-à-vis* the access to state information that can be considered unlawful.

Dissimilarly, the revised version of the Information Bill released in 2010 incorporated clauses that aimed specifically at the press and have been viewed as too restrictive on press freedom held in high esteem in the democratic processes of the country and grounded in the Constitution and the Bill of Rights. The Bill not only expanded the criminalisation of the possession and dissemination of state information but also prohibited the access to state information based on the judgments of the official involved. The latter included a clause that would support the release of this information in the name of public interest. This prohibition is where the proposed legislation has received most of its criticism, in that it is seen to be unconstitutional in excluding a public-interest defence clause that would uphold the freedom of access to information stipulated in the Bill of Rights of the Constitution. This prohibition creates the idea of the securitisation of information, as the state has made a notion to remove the access to information in the name of national security, without providing a platform to challenge whether an issue is considered part of national security or not.

The Bill was initially introduced into a period of progressive policy-making, at a time when government departments across the board were making strides in the implementation of policies to further their constitutional mandates. Specifically within the security field the then

© University of Pretoria

Minister Kasrils was adamant to reform the role of the civilian intelligence services. To contribute to policy implementation, a new security law was drafted to repeal outdated apartheid-era legislation that was hindering the operational capacity of the intelligence services. It was also anticipated that it would add value to a new security framework. Thus the motives do not exemplify full securitization but rather reflect a security consciousness.

The national situation in 2010 when the Bill was reintroduced was vastly different, having an impact on the way in which the revised legislation was then received by the public at large, ultimately altering the dialogue surrounding it. A new government administration was in place led by President Jacob Zuma; the country was on high security alert as host of the impending FIFA (International Federation of Football Association) World Cup; and changes to the government structures, including new political appointments, presented different dynamics within which the state bureaucracy still had to function. Not least of all, the amalgamation of the SSA with a new Minister (Cwele), offered its own dynamics.

In response to a growing sentiment that “the creation of the SSA reflects a growing securitisation of the South African state” (Africa 2012: 124), Minister Cwele refuted this inclination to a larger authoritarian state arguing that “the restructuring is a response to the disproportionate allocation of resources to the corporate services, and intended to ensure that the organs of intelligence focused on their core business” (Segar 2012). Significantly, the peripheral factors of this changed environment must be considered in determining the different reception of the Information Bill at different times during the legislative process.

Having demonstrated the introduction of the Bill as the speech-act and articulated the completion of the securitising move (through the persuasion of the audience, the existence of an existential threat, and the significance of historical context), the inference is that the Information Bill partially securitises information. The promulgation of the Bill will fully securitise information, but the result of this is not as dire as to be expected. The outcome of the Information Bill once promulgated and the outlook for information-security are dependent on the practical application of the legislation going forward. Table 1 (below) summarises the securitisation process of the Bill within the local information landscape.

© University of Pretoria

Table 1: The securitisation of information in South Africa

SECURITISATION SPECTRUM	THE INFORMATION BILL	SECURITISATION OUTCOME
Politicisation	• Information-security addressed by each government administration through legislation since 1994 • The development and initiation stages of the Bill throughout each administration • Spearheaded by Minister Ronnie Kasrils • Introduced by Minister Siyabonga Cwele • Prioritised by the SSA as part of the expansion and institutionalisation of civilian intelligence services • Political and civil society opposition to and criticism of the Bill • Public-political debate on the Bill in particular and the expansion of the intelligence services in general	• A mandate to address information-security through the legislative process: to create security law • Attention is paid to vulnerabilities in existing legislation • The reform and enhancement of South Africa's information society • The Government and public bodies debate information-security issues
Securitisation	• The continuation of the legislative process • The alignment of the Bill with provisions in the Constitution and existing information legislation • The intended use of the Bill to enhance SSA capabilities to combat threats in the Information Age • The perception that the Bill designates information as a security issue • The perception that the Bill is an extraordinary measure used by Government in response to threats	• Attention is given to information as the object to be secured • The disparagers focus on the aims of the Bill to conceal information and censor the free press • The SSA focuses on the protection and not the non-disclosure aims of the Bill
Speech-act	• The physical representation of security ('saying security') • The Bill itself as the speech-act • The use of national security as a primary justification for restrictions on information as necessary	• The Bill is a speech-act but not sufficient in and of itself to warrant securitisation • National security is justifiable and an expected defence of Government action, up to a point • The state has to pursue national interests and to attain national security priorities

© University of Pretoria

SECURITISATION SPECTRUM	THE INFORMATION BILL		SECURITISATION OUTCOME

Securitising move	• The designation of a security label to information
	• 3 conditions required to complete the securitising move:
	  ○ Presentation of an existential threat
	  ○ Persuasion of the audience
	  ○ Significance of the historical context
			• Expression of the securitisation process in practice
			• Information, as a security issue, becomes embedded in societal and political language
			• Various factors present themselves to contribute to the enabling conditions of securitisation

	Existential threat	• Necessary in terms of the comprehensive outline of security • Essential for the security framework and information-security advancement • Justified in terms of national security	• Heightened notion of an issue as an urgent threat to the country • The protection of information is viewed more critically • Greater threat awareness and an increased capability to reduce risk and avoid the manifestation of threats
	Persuasion of audience	• The Government has a democratic mandate to govern • The Government possesses legal authority as the securitising agent • Parliament is democratically elected and makes laws through a legitimate legislative process	• Government bodies recognise and accept the necessity of the Bill and the enhancement of the security of information • The public (media, civil society, activists) are not convinced of the merits of the Bill • The detractors of the Bill contribute to the 'publicisation' of the Bill, thereby augmenting the 'security speak' around the Bill
	Historical context	• The consideration of the significant and sensitive history of the country • Actions taken by Government to prevent reversions to and remnants of pre-1994 legislation • The Bill is to repeal apartheid-era legislation • The Bill does not aim to conceal information as apartheid-era laws did	• The Bill addresses apartheid-era issues and attempts to correct remnants of an inefficient, self-serving information society • The use of history by Government as a condition to justify the modernisation of the bureaucracy • The use of history by detractors to condemn similarities between the Bill and apartheid-era laws
Desecuritisation		• Currently this phase is not present • There is an awareness of the domination of the security paradigm • The sensitivity of the issue is too high to allow for the 'neutralisation' of information	• The context remains securitised and the issues of information within the security-information nexus are still prevalent and prominent.

© University of Pretoria

4. Conclusion

This chapter proffered an analysis of the securitisation of information through the application of Securitisation Theory to the Information Bill. The spectrum utilised demonstrated the progression of an issue, from politicisation to securitisation, and possibly to desecuritisation. The issue of information traversed from its intrinsic sensitive nature, becoming politicised through its prioritisation during different political eras and administrations, to a form of securitisation where specific elements manifested over the last decade, close to a point where a case could be made for complete securitisation. These elements include the speech-act, designated by the Information Bill itself, as the ultimate act of 'saying security'; in harmony with the three conditions required to conclude the securitising move.

To enhance South African national security the SSA posits that the Information Bill, contributing to security law, will assist the Agency to address present and future threats. Information about these threats and Government decisions on them are for the most part confidential, and must remain so through the restrictions in the Bill. The posture of the SSA is based on the understanding that information – and thus intelligence – is at the core of combating these threats, or at the very least in comprehending them. An obsolete information-security framework weakens the state's capacity to address an insidious existential threat.

The Government exercised its legal authority to introduce and promote the Bill, subject to the persuasion of Parliament and its pending promulgation. The Government has been democratically elected and given a mandate to govern. Notwithstanding, the legitimacy of the Government has been questioned to the extent that the audience – being the general public – remains unconvinced of the efficacy of the Bill and the intentions of Government. Despite this anti-Government sentiment, the securitising agent has the legal power to pass the Bill and implement the Act, as a final step towards complete securitisation.

In completing the securitising move, the Government has bemoaned the maladministration of the apartheid state with regard to information, emphasising the need to protect the current dispensation by means of a relevant and effective information-security paradigm. Although the perceived draconian nature of the intelligence services as well as the misuse and concealment of information during the apartheid dispensation encouraged the present desire

© University of Pretoria

to ensure complete transparency and the removal of secrecy, it is neither practical nor desirable. While historical context is significant, it should not hinder the development of an intelligence service that is able to address the challenges of a dynamic world.

To provide for and utilise extraordinary measures, the introduction of the Bill is the only means to contribute to the process of securitisation. The legislation may be an extreme resort for a democratic government, but is not beyond the boundary of acceptable security law. Significantly, the Government has not expedited the legislative process, allowing due diligence for public consultation and amendments to the Bill. Although the current absence of news on the Bill lends itself to arguments in support of desecuritisation, it is expected that the Bill (or a similar piece of legislation) will eventually be promulgated, finalising the securitisation effort.

In this analytical chapter the case study on the South African Information Bill was examined and explained by applying the tenets and elements of Securitisation Theory. Aspects of securitisation were demonstrated but equally pertinent are the elements of securitisation that are not present, belying the complex conundrum facing the state and government in their efforts to reconcile transparency and security. From the analysis it is evident that partial securitisation of information has occurred. This development does not necessarily erode the democratic project in South Africa, if the legislation is used ethically, responsibly and effectively to enhance the current information-security environment. The consequences of this outcome are dealt with in the concluding chapter.

© University of Pretoria

CHAPTER FIVE

EVALUATION AND RECOMMENDATIONS

The aim of this study was to apply Securitisation Theory to a practical case study, in this case to the *Protection of State Information Bill*, *2010* to determine whether or not securitisation of information had occurred and, if so, the consequences of this securitised situation. This aim was informed by the necessity for democratic states to find an equilibrium between openness and secrecy, and to determine the extent to which South Africa succeeds in this. The primary research question was: *Does the Information Bill securitise information or not?* This question was informed by a series of secondary questions that are addressed at the conclusion of this chapter. The argument at the outset and in response to the main question was that the Bill partially securitised information without necessarily hindering the consolidation of democracy or seriously detracting from democratic norms regarding information access.

To understand the process of securitisation, Chapter Two offered the theoretical underpinnings of the paper. Securitisation Theory was at the core of the security paradigm used to answer the research question. Against the backdrop of a changed international arena at the end of the Cold War, Security Studies as a field of specialisation became prominent in IR. Under its scope the notion of non-military threats became prolific as the conceptualisation of security broadened and deepened to include alternative sectors other than the military domain as a source of threats – for example economic, environmental, societal, and other objects that deserved to be secured – namely the individual, the community and society. This questioning of the *status quo* gave impetus to CSS as a derivative of Security Studies, an approach that explored the origins of conceptualisations and issues in IR, in antithesis to more superficial problem-solving approaches.

Most notably CSS paid attention to the concept of security itself, questioning the attachment of a 'security' designation to some aspects of international relations. In this regard, proponents of CSS examined the process by which an issue is deemed a security issue by the ruling elite, concluding that it is this elite who expediently create this designation to contribute to their own agenda. Underpinning this is the idea that an issue positioned within a security setting affords the elite extraordinary power to address the issue. The elite are the securitising

© University of Pretoria

actors who ‘speak security’ in the form of a speech-act to represent the physical manifestation of the issue as security. Concomitant to this process, three necessary conditions were identified that complete the securitising move. The securitising actor must present an existential threat; must persuade the targeted audience of this existential threat; and must demonstrate the significance of historical context. Thus securitisation of an issue occurs.

In addition and at a conceptual-theoretical level, the notions of information and security and the information-security nexus were explored. This clarified the complexities of the concepts and their relation to each other in international relations and in the pursuit of national security. This concept-based framework for analysis was carried through to Chapter Three and incorporated into the examination of the historical context of the South African information-security landscape. As was determined, state information is not neutral but is politicised by its very nature and its existence in a state-centric paradigm. Viewed along a spectrum, concepts/ issues/objects start out as politicised, eventually becoming securitised with the completion of the securitising move to the point where they may be desecuritised in time. This state-driven securitisation was juxtaposed on the security-information spectrum with an analysis of the importance of information in the public-political domain, in the process providing an overview of the constitutional and legal context of information and security in South Africa.

It was into this context that the Information Bill itself was introduced as the case study, whereby its objectives and key provisions were discussed. The context of the creation and introduction of the Bill is significant and was addressed to explain how the Bill aims to contribute positively to the information-security landscape of the country. Subsequently the Bill was analysed in Chapter Four in terms of Securitisation Theory to determine whether information had been securitised, and whether this legislation was the catalyst for this securitisation process. Given the sensitivity and complexity of the information-security paradigm, the critique of the Bill offered a veritable contextualisation of how the legislation is perceived by its supporters and detractors. The Government supports the Bill as part of an enhanced information-security network and a necessity for efficient and effective intelligence services. The detractors bemoan the purported draconian and unconstitutional nature of the legislation. The discussion concluded tentatively that information had been partially securitised.

© University of Pretoria

As an evaluation of this analysis, the following key findings are presented: It was found that the prerequisites of a securitising move were evident to the extent that the Bill addressed an existential threat in the form of a weak and inconclusive information-security network. Therefore, the South African state and government was obligated to promote a relevant and suitable national security policy to pursue its national interests, which will be augmented by the aim and implementation of the Bill. The Government remained the authoritative agency to securitise issues and had been able to persuade the targeted audience (in this case the relevant state institutions such as Parliament) to support the legislation, in so far as the Bill has not been dismissed outright. However, civil society opponents of the Bill have not been completely persuaded of the expediency of the legislation, which contributed to the growing anti-government sentiment whereby the ruling party's legitimacy had reduced in the eyes of the general public. These two factors diminish the overall persuasion to complete the securitising move. The historical precedent was presented as an example of what Government must prevent (and not recreate); in South Africa's case a revival of apartheid-era thinking. However, the Government utilised the anti-apartheid sentiment to justify the aims of the Bill, arguing that its premise is to prevent the abuse of information and close loopholes in the information system that existed during the apartheid regime.

The evolving nature of threats to state-actors implores governments to manage new risks posed by emerging threats. Risk management requires continuous assessment to be effective, and provides for over-arching principles of practice to be applied to the information analysis process. Legislation forms the foundation of this practice. Within this rubric the periodic review of security legislation specifically, and the statutory framework of the intelligence and information landscape in general, is not uncommon but a prerequisite for an effective risk management strategy. This review of the legislation was overdue and perpetuated the vulnerability of the state. The all-encompassing nature of the legislation is also justified by the very nature of the operational environment, in that threats to national security are not definitive and static. Therefore, to enhance a proactive approach to national security, the legislation supporting the policies that guide operational strategies must be relevant when addressing security issues.

The SSA believed the proposed legislation would enhance the system of information dissemination and classification, and concurrently establish a system of security governance

© University of Pretoria

that is transparent and holds those in power to account. Given the current notion of national security, South Africa should benefit from a contemporary and customised information-security framework that forms the foundation of a proactive and effective intelligence service. By adopting 'modern' legislation on the protection of state information and retribution for its wrongful disclosure – exemplified by the Bill – the Government was able to propel the information-security landscape into the 21st century. Therefore the state would be better positioned to compete with actors in the international arena with regard to cyber security, espionage, information-peddling and information protection. Irrespective of the above, the consultation that informed the final version of the legislation through the legislative process and the public hearings was indicative of an inclusive democratic practice. This process positively contributed to democratic consolidation and remains true whether the Bill is assented to or not.

The promulgation of the Bill will epitomise a completion of the securitisation process of information. However, this development is not necessarily a negative manifestation of the information-security nexus in the country, with less pejorative consequences for the future of the South African democratic system than has been presented by the disparagers. Although securitisation tends to be viewed negatively, given the high degree of manipulation of extraordinary measures involved, it was shown that the Government had exercised constraint, at least in principle, with regard to its executive power. The only extraordinary measure in play had been the introduction of the Bill itself, in its extreme overhaul of the protection of state information. This approach in the legislation was critical to streamline South Africa' agenda in securing national interests and preventing national security from being threatened or compromised. In the Information Age, having a substantial legislative framework to combat existential threats to national security that could emerge from the exploitation of different forms of information, is an imperative to survival. This imperative vindicates the actions of the state to consolidate and improve the information-security agenda.

In light of this and as the country continues with efforts to embed democratic governance, democratic consolidation and progress rely on the interstices of transparency (as a prerequisite of a democratic nation) and secrecy (as a prerequisite to national security). The process that has unfolded as a result of the introduction of this piece of legislation demonstrated a vibrancy of civil society playing a vital, independent role in the democratic

© University of Pretoria

dispensation of the country, whereby the democratic institutions of South Africa are tested and found to be stable and secure. The degree of public skepticism towards actions of Government is warranted to keep the executive in check, as a way to minimise the exploitation of extraordinary measures in the name of national security.

Based on the research and findings, recommendations are made to guide further exploration in areas of policy and academia. As a point of departure, the information-security landscape of South Africa is pertinent to understand what legislation exists, how it operates and what loopholes require attention. A further exploration of the public-political and legal context is vital to appreciate the nuances of the legislative process and the decisions that inform executive decision-making with regard to policy. Of particular significance would be to examine the implementation of the legislation, given its likely and eventual promulgation, in terms of its efficacy and practice in regulating the information-security paradigm. An assessment of how the legislation interacts with the existing information-security laws is pertinent to the efficient and effective functioning of the information society.

In terms of contributing to a research agenda, an analysis of South Africa's information society after the Information Bill has had time to gain effect would improve an understanding of the consequences of the legislation on the information-security nexus. To link the study of theory and practice, it would be expedient to examine information-security as a concept in varying environments, to understand the dynamics that influence the role and power of information in practice. Thus a comparative study with other states in terms of their classification systems of state information, information landscapes in general, as well as their security law and information legislation, could be useful.

In conclusion, the secondary questions of the research problem are answered as follows: *How are information and (national) security related?* The relationship between information and security is not mutually exclusive, with a dependency and interrelatedness that has been perpetuated and intensified by the Information Age. States rely on information as intelligence, which is used to secure national interests; and likewise the information resources of a state need to be secure to prevent unwarranted and unwelcome disclosure. As a practical manifestation, the Bill is to secure the state's information resources and to contribute to an effective information-security relationship.

© University of Pretoria

What is the rationale of the Information Bill and how does it protect security-related information? Apart from removing the legacies of apartheid-era , the expansion of the security services and the expanded but coherent Government approach to information were seen as ways to reduce vulnerabilities, ultimately to combat threats to the state itself. Through more stringent regulation, these efforts of Government are to bring state and society to a more balanced understanding and practice of secrecy and democracy in the 21st century.

Does the Information Bill politicise, securitise and/or desecuritise information and who is responsible for this? Aligned with the information-security spectrum, information has traversed from politicisation to partial securitisation, with full securitisation imminent pending the pronouncement of the Bill into an Act. The Bill does partially securitise information, in that it constitutes a veritable speech-act, and the securitising agent was able to conclude the securitising move (with the presentation of an existential threat, the persuasion of the audience, and the historical significance). It is evident that the Bill has moved along the spectrum having been politicised with its formulation and introduction by the Government (the SSA in consultation with other state entities), through partial securitisation, to a point not excluding the possibility of desecuritisation given the uncertainty about its future status. However, as was argued, the issue of information is too sensitive and heightened at this stage to warrant desecuritisation. The promulgation of the Bill will result in completed securitisation, as this step will consolidate the speech-act and fulfil the felicity conditions of the securitising move. Although state and government were the primary securitisation agents, opposition parties, interest groups and civil society by default also played a role in this process.

What are the consequences of this development for South Africa's (national) security? The Bill (or a different version of similar legislation) is expected to be promulgated despite the time elapsed since its inception, given the state justification and state support of the Bill and the lengthy legislative process. However, the delay in passing the Bill could be construed as a deliberate hesitation on the part of the Government in light of the local political environment at present. But with eventual promulgation this securitisation should not be viewed pejoratively since it should also inspire confidence in the institutions involved in the process and in its contribution to the information-security sector. The mechanisms of the democratic state are operational and effective, highlighting an optimism with regard to governance.

© University of Pretoria

Is Securitisation Theory an appropriate theoretical framework to explore securitisation through an act or bill? Securitisation Theory proved to be an appropriate theoretical framework to explore securitisation occurrences in the Bill, as it unveils the practical manifestations of the process. This framework allowed for an empirical, qualitative study of the research problem. Notwithstanding its expediency, the theory must be applied conditionally, taking into consideration the dynamics of the situation. With regard to the Bill, Securitisation Theory was useful when the three conditions of the securitising move were used in conjunction with the speech-act concept; the speech-act as a securitisation formulation proved insufficient and superficial, in and of itself.

Based on the aforesaid and as a response to the main research question, *Does the Information Bill securitise information or not?*, the following: This study, by applying Securitisation Theory to the Information Bill, has determined that information has been partially securitised. Through this determination, whereby a contextualisation was proffered of the information-security nexus and an analysis was made of the securitisation process, the information society of South Africa is better understood. This also contributes to a prospective assessment of democratic progression in South Africa.

Twenty-two years into the democratic dispensation South Africa is at another turning point in its history, in the consolidation of democratic governance. The Information Bill – addressing remnants of the pre-1994 regime as part of a 'delayed' transition – does away with past legacies but also creates new problems. The world is in constant flux, with the progression of the Information Age and all its innovations and dynamics, furthermore creating uncertainty and insecurity. In light of this the Government had to reconsider its position in the international arena and re-evaluate its strategies to pursue its national interests and protect its national security. The Information Bill is a product of this reformation, as part of an expansion and rationalisation of the intelligence services, with the aim of enhancing South Africa's security posture, both at home and abroad. Consequently South Africa continues the pursuit of equilibrium between openness and secrecy, to achieve national security and secure the national interest.

Word count: 33737

© University of Pretoria

BIBLIOGRAPHY

Africa, S. 2009. ***Well-Kept Secrets: The Right of Access to Information and the South Africa Intelligence Services***. Midrand: Institute for Global Dialogue.

Africa, S. 2011. ***The Transformation of the South African Security Sector: Lessons and Challenges***. Policy Paper - No 33. Geneva: Geneva Centre for the Democratic Control of Armed Forces (DCAF).

Africa, S. 2012. The Policy Evolution of the South African Civilian Intelligence Services: 1994 to 2009 and Beyond. Monograph in ***Strategic Review for Southern Africa***, 34(1): 97-134.

Alker, H. 2005. Emancipation in the Critical Security Studies Project. In Booth, K (ed). ***Critical Security Studies and World Politics***. Boulder: Lynne Rienner.

Aradau, C. 2004. Security and the Democratic Scene: Desecuritization and Emancipation. ***Journal of International Relations and Development***, 7(4): 388-413.

Armistead, L (ed). 2004. ***Information Operations: Warfare and the Hard Reality of Soft Power***. Lincoln: Brassey's.

Austin, JL. 1962. How to Do Things with Words. In Urmson, JO and Sbisa, M (eds). ***How to Do Things with Words***. 2nd edition. Cambridge: Harvard University Press.

Ayoob, M. 1997. Defining Security: A Subaltern Realist Perspective. In Krause, K and Williams, MC (eds). ***Critical Security Studies.*** Minneapolis: University of Minnesota Press.

Balzacq, T. 2005. The Three Faces of Securitization: Political Agency, Audience and Context. ***European Journal of International Relations***, 11(2): 171-201.

Balzacq, T. 2011a. A Theory of Securitization: Origins, Core Assumptions, and Variants. In ***Securitization Theory: How Security Problems Emerge and Dissolve.*** Oxford: Routledge.

Balzacq, T (ed). 2011b. ***Securitization Theory: How Security Problems Emerge and Dissolve***. Oxford: Routledge.

© University of Pretoria

Barber, WE. 1978. National Security Policy. In Louw, MHH (ed). ***National Security: A Modern Approach***. Pretoria: Institute for Strategic Studies, University of Pretoria.

Bekker, K. 2004. The Contribution of the Entertainment and Media Industries. A Democratic South Africa: Three Perspectives on the Role of Culture and the Contribution of Entertainment and the Media. In World Economic Forum, ***South Africa at 10: Perspectives by Political, Business and Civil Leaders***. Cape Town: Human and Rousseau.

Bilgin, P. 2008. Critical Theory. In Williams, PD (ed). ***Security Studies: An Introduction***. Oxford: Routledge.

Bomford, A. 1999. Echelon spy network revealed. ***British Broadcasting Corporation (BBC)***. Internet: www.news.bbc.co.uk/2/hi/503224.stm Access: 17 July 2016.

Booth, K. 1991. Security and Emancipation. ***Review of International Relations***, 17(4): 313-326.

Booth, K (ed). 2005. ***Critical Security Studies and World Politics***. Boulder: Lynne Rienner.

Booth, K and Vale, P. 1995. Security in Southern Africa: After Apartheid, Beyond Realism, ***International Affairs***, 71(2): 285 -304.

Brink, A. 2010. A long way from Mandela's kitchen. ***New York Times***, 11 September 2010.

British Broadcasting Corporation (BBC). 2014. Edward Snowden: Leaks that exposed US spy programme. ***BBC***, 17 Janurary 2014. Internet: www.bbc.com/news/world-us-canada-23123964 Access 17 July 2016.

Bruneau, TC. 2008. Controlling Intelligence in New Democracies. In Johnson, LK and Wirtz, JJ (eds). ***Intelligence and National Security: The Secret World of Spies, An Anthology***. 2nd edition. New York: Oxford University Press.

Burns, YM. 1985. Freedom of the Press in South Africa. In Van Vuuren, DJ, Wiehahn, NE, Lombard, JA and Rhoodie, NJ (eds). ***South Africa: A Plural Society in Transition***. Durban: Butterworth.

© University of Pretoria

Buzan, B. 1989. ***People, States, and Fear: An Agenda for International Security Studies in the post-Cold War Era.*** Hemel Hempstead: Harvester Wheatsheaf.

Buzan, B. 1991. ***People, States, and Fear: An Agenda for International Security Studies in the post-Cold War Era***. 2nd edition. Hemel Hempstead: Harvester Wheatsheaf.

Buzan, B. 1998. Security in the Twenty-First Century. In Hughes, CW and Meng, LY (eds). 2011. ***Security Studies: A Reader***. Oxford: Routledge.

Buzan, B and Hansen, L. 2009. ***The Evolution of International Security Studies***. Cambridge: Cambridge University Press.

Buzan, B, Wæver, O and de Wilde, J. 1998. ***Security: A New Framework for Analysis***. Boulder: Lynne Rienner.

Currie, I. 2003. South Africa's Promotion of Access to Information Act. ***European Public Law***, 9(1): 59-72.

Currie, I and Klaaren, J. 2011. ***Evaluating the Information Bills: A Briefing Paper on the Protection of Information Bill***. Johannesburg: University of the Witwatersrand, on behalf of the Centre of Memory at the Nelson Mandela Foundation.

Darch, C and Underwood, PG. 2010. ***Freedom of Information and the Developing World: The Citizen, the States and Models of Openness.*** Oxford: Chandos Publishing.

Donnelly, L. 2010. Info Bill a 'danger to democracy', Parliament told. ***Mail & Guardian*** (Johannesburg), 23 July 2010. Internet: http://mg.co.za/article/2010-07-23-info-bill-a-danger-to-democracy-parliament-told Access: 15 April 2014.

Duvenage, PC. 2016. ***Cyber Counterintelligence***. Presentation by Mr P Duvenage (Senior Research Fellow). Academy of Computer Science and Software Engineering: University of Johannesburg. (used with the author's permission). Presentation based on: Duvenage, PC and Von Solms, SH. 2015. Cyber Counterintelligence: Back to the Future. ***Journal of Information Warfare***, 13(4): 42-56.

© University of Pretoria

Elbe, S. 2003. HIV/AIDS and the Security Sector in the Southern African Region. In Hentz, JJ, and Boas, M (eds). ***New and Critical Security and Regionalism: Beyond the Nation State.*** Hampshire: Ashgate.

Engelbrecht, L. 2011. National security strategy necessary – analysts. Internet: http://www.defenceweb.co.za/index.php?option=com_content&view=article&id=13124:feature-national-security-strategy-necessary--analysts-&catid=49:National%20Security&Itemid=115 Access: 16 April 2014.

Eriksson, J. 2001a. Introduction. In Eriksson, J (ed). ***Threat Politics: New Perspectives on Security, Risk and Crisis Management***. Aldershot: Ashgate.

Eriksson, J (ed). 2001b. ***Threat Politics: New Perspectives on Security, Risk and Crisis Management***. Aldershot: Ashgate.

Ferreira, E. 2012. State must go back to drawing board – Kasrils. ***Business Day Live***, 11 August 2012. Internet: http://www.bdlive.co.za/articles/2010/08/11/state-must-go-back-to-drawing-board---kasrils Access: 26 August 2015.

Fierke, KM. 2007. ***Critical Approaches to International Security***. Cambridge: Polity Press.

Friedman, S. 2013. Whose freedom? South Africa's Press, Middle-class Bias and the Threat of Control. In Wasserman, H (ed). ***Press Freedom in Africa: Comparative Perspectives***. Abingdon: Routledge.

Frisch, H. 2002. Explaining Third World Security Structures. ***Journal of Strategic Studies***, 25(3): 161-190.

Goldman, EO. 2004a. Introduction: Security in the Information Technology Age. In Goldman, EO (ed). ***National Security in the Information Age***. London: Frank Cass.

Goldman, EO (ed). 2004b. ***National Security in the Information Age.*** London: Frank Cass.

Goldman, EO. 2008. New Threats, New Identities and New Ways of War: The Sources of Change in National Security Doctrine. ***Journal of Strategic Studies***, 24(2): 43 – 76.

© University of Pretoria

Haggerty, KD and Ericson, R. 2006. ***The New Politics of Surveillance and Visibility.*** Toronto: University of Toronto Press.

Haggerty, KD and Samatas, M (eds). 2010. ***Surveillance and Democracy***. New York: Cavendish Publishing.

Hansen, L. 2000. The Little Mermaid's Silent Security Dilemma and the Absence of Gender in the Copenhagen School. ***Millennium: Journal of International Studies***, 29(2): 285-306.

Hartley, W. 2008. Time-pressed MPs shelve secrecy legislation. ***Business Day***. 16 October 2008. Internet: http://www.bdlive.co.za/articles/2008/10/16/time-pressed-mps-shelve-secrecy-legislation Access: 4 May 2014.

Heard, AH. 1987. The Press in South Africa: Twilight of Freedom? In Sethi, SP (ed). ***The South African Quagmire: In Search of a Peaceful Path to Democratic Pluralism***. Cambridge: Ballinger.

Hentz, JJ, and Boas, M (eds). 2003. ***New and Critical Security and Regionalism: Beyond the Nation State.*** Hampshire: Ashgate.

Holden, P and Plaut, M. 2012. ***Who Rules South Africa? Pulling the Strings in the Battle for Power***. Johannesburg: Jonathan Ball.

Holt, PM. 1995. ***Secret Intelligence and Public Policy: A Dilemma of Democracy***. Washington: CQ Press.

Hughes, CW and Meng, LY (eds). 2011. ***Security Studies: A Reader***. New York: Routledge.

Huysmans, J. 1998a. The Question of the Limit: Desecuritization and the Aesthetics of Horror in Political Realism. ***Millennium: Journal of International Studies***, 27(3): 569-589.

Huysmans, J. 1998b. Revisiting Copenhagen: Or, on the Creative Development of a Security Studies Agenda in Europe. ***European Journal of International Relations***, 4(4): 488-506.

Hynek, N and Chandler, D. 2013. No Emancipatory Alternative, No Critical Security Studies. ***Critical Studies on Security***, 1(1): 46-63.

© University of Pretoria

Johnson, LK and Wirtz, JJ (eds). 2008. ***Intelligence and National Security: The Secret World of Spies, An Anthology***. 2nd edition. New York: Oxford University Press.

Jones, AA. 1996. Information Security: Planning for the Deluge. In Schwartzstein, SJD (ed). ***The Information Revolution and National Security Info and National Security: Dimensions and Directions***. Washington D.C.: The Center for Strategic Studies and International Studies.

Kaldor, M. 2007. ***Human Security: Reflections on Globalisation and intervention***. Cambridge: Polity Press.

Kasrils, R. 2010. Defend Democracy; Don't Gag It. ***Pretoria News***, 20 October 2010.

Kelstrup, M and Williams, MC (eds). 2000. ***International Relations Theory and the Politics of European Integration***. London: Routledge.

Kirchner, EJ and Sperling, J (eds). 2010. ***National Security Cultures: Patterns of Global Governance***. Oxford: Routledge.

Kolodziej, EA. 2005. ***Security and International Relations***. Cambridge: Cambridge University Press.

Krause, K and Williams, MC (eds). 1997. ***Critical Security Studies.*** Minneapolis: University of Minnesota Press.

Lantis, JS. 2002. Strategic Culture and National Security Policy. ***International Studies Review***, 4: 87–113.

Levy, MA. 1995. Is the Environment a National Security Issue? ***International Security***, 20(2): 35-62.

Lipschutz, RD. 1995a. On Security. In Lipschutz, RD (ed). ***On Security***. New York: Columbia University Press.

Lipschutz, RD (ed). 1995b. ***On Security***. New York: Columbia University Press.

© University of Pretoria

Louw, MHH. 1978. The Nature of National Security in the Modern Age. In Louw, MHH (ed). ***National Security: A Modern Approach***. Pretoria: Institute for Strategic Studies, University of Pretoria.

Louw, MHH (ed). 1978. ***National Security: A Modern Approach***. Pretoria: Institute for Strategic Studies, University of Pretoria.

Lyon, D. 2003. ***Surveillance after September 11.*** Cambridge: Polity Press.

Lyotard, JL. 1984. ***The Postmodern Condition: A Report on Knowledge.*** Minneapolis: University of Minnesota Press.

Maduna, P. 2003. On the occasion of the adoption of the Promotion of Access to Information Act, 2000. Internet: http://www.justice.gov.za/legislation/regulations/r2003/2003_r887_gg25099-paia-descrip.pdf Access: 13 August 2015.

Mail and Guardian (Johannesburg). 2013. ***Editorial: Secrecy destroys accountability***, 15 November 2013. Internet: http://mg.co.za/article/2013-11-14-secrecy-destroys-accountability Access: 14 August 2015.

McDonald, D. 2011. The present is another country: A comment on the 2010 media freedom debate. ***Ecquid Novi: African Journalism Studies***, 32(2): 122-134.

McRae, R and Hubert, D (eds). 2001. ***Human Security and the New Diplomacy: Protecting People, Promoting Peace***. Montreal: McGill-Queen's University Press.

Mutimer, D. 1999. Beyond Strategy: Critical Thinking and the New Security Studies. In Snyder, CA. (ed). ***Contemporary Security and Strategy.*** Hampshire: Macmillan Press.

Ngcobo, S. 2013. Silence and secrecy: Let us shine a light on our secrets. ***Mail & Guardian*** (Johannesburg). Internet: http://mg.co.za/article/2013-11-21-let-us-shine-a-light-on-our-secrets Access: 17 March 2014.

Nye, JS (Jr). 1999. Redefining the National Interest. ***Foreign Affairs***, 78(4): 22-35.

© University of Pretoria

Nyirenda, A and Polaki, M. 2013. ***Workshop Report: National Security and the Right to Information Principles: Workshop Report***. Johannesburg: Open Society Initiative for Southern Africa.

Occupy Wall Street. 2011. Information on the website about the organisation. Internet: www.occupywallst.org Access: 13 March 2016.

O'Malley, P. 1991. The Heart of Hope. Black Consciousness Movement. Internet: https://www.nelsonmandela.org/omalley/index.php/site/q/03lv02424/04lv02730/05lv03188/06lv03193.htm Access: 14 July 2016.

Patman, RG (ed). 2006. ***Globalisation and Conflict: National Security in a 'New' Strategic Era***. Oxford: Routledge.

Peoples, C and Vaughan-Williams, N. 2010. ***Critical Security Studies: An Introduction.*** London: Routledge.

Ransom, HH. 2008. The Politicization of Intelligence. In Johnson, LK and Wirtz, JJ (eds). ***Intelligence and National Security: The Secret World of Spies, An Anthology***. 2nd edition. New York: Oxford University Press.

Republic of South Africa (RSA). 1994. ***White Paper on Intelligence, 1994***.
Internet: www.ssa.gov.za (PDF). Access: 22 February 2014.

Republic of South Africa (RSA). 1996. ***Minimum Information Security Standards (MISS)***. Internet: http://www.kzneducation.gov.za/LinkClick.aspx?fileticket=aDNwzVuiANQ%3D&
Access: 23 August 2014.

Republic of South Africa (RSA). 2010. ***Executive Summary of the Protection of State Information Bill.*** Internet: www.ssa.gov.za (PDF) Access: 18 February 2015.

Republic of South Africa (RSA) Act. 1957. ***Defence Act, 1957*** (Act 44 of 1957)

Republic of South Africa (RSA) Act. 1958. ***Police Act, 1958*** (Act 7 of 1958).

Republic of South Africa (RSA) Act. 1959. ***Prisons Act, 1959*** (Act 8 of 1959).

© University of Pretoria

Republic of South Africa (RSA). 1968. ***Armaments Development and Production Act, 1968*** (Act 57 of 1968).

Republic of South Africa (RSA) Act. 1970. ***National Supplies Procurement Act, 1970*** (Act 89 of 1970).

Republic of South Africa (RSA) Act. 1974. ***Publications Act, 1974*** (Act 42 of 1974).

Republic of South Africa (RSA) Act. 1977. ***Petroleum Products Act, 1977*** (Act 120 of 1977).

Republic of South Africa (RSA) Act. 1980. ***National Key Points Act, 1980*** (Act 102 of 1980).

Republic of South Africa (RSA). 1982a. ***Demonstrations in or Near Court Buildings Prohibition Act, 1982*** (Act 71 of 1982).

Republic of South Africa (RSA) Act. 1982b. ***Intimidation Act, 1982*** (Act 72 of 1982).

Republic of South Africa (RSA) Act. 1982c. ***Internal Security Act, 1982*** (Act 74 of 1982).

Republic of South Africa (RSA) Act. 1982d. ***Protection of Information Act, 1982*** (Act 84 of 1982).

Republic of South Africa (RSA) Act. 1993. ***Nuclear Energy Act, 1993*** (Act 131 of 1993).

Republic of South Africa (RSA) Act. 1994a. ***Intelligence Services Act, 1994*** (Act 39 of 1994).

Republic of South Africa (RSA) Act. 1994b. ***Public Services Act, 1994*** (Act 103 of 1994).

Republic of South Africa (RSA) Act. 1995. ***South African Police Services Act, 1995*** (Act 68 of 1995).

Republic of South Africa (RSA) Act. 1996a. ***Justice Laws Rationalisation Act, 1996*** (Act 18 of 1996).

Republic of South Africa (RSA) Act. 1996b. ***Constitution of the Republic of South Africa, 1996*** (Act 36 of 1996).

Republic of South Africa (RSA). 1996c. ***National Archives and Records Service of South Africa Act, 1996***. (Act 43 of 1996).

© University of Pretoria

Republic of South Africa (RSA) Act. 1997. ***Legal Deposit Act, 1997*** (Act 54 of 1997).

Republic of South Africa (RSA) Act. 2000a. ***Promotion of Access to Information Act, 2000*** (Act 2 of 2000).

Republic of South Africa (RSA) Act. 2000b. ***Promotion of Administrative Justice Act, 2000*** (Act 3 of 2000).

Republic of South Africa (RSA) Act. 2000c. ***Promotion of Equality and Unfair Discrimination, 2000*** (Act 4 of 2000).

Republic of South Africa (RSA) Act. 2000d. ***Protected Disclosures Act, 2000*** (Act 26 of 2000).

Republic of South Africa (RSA) Act. 2002a. ***Intelligence Services Act, 2002*** (Act 65 of 2002)

Republic of South Africa (RSA) Act. 2002b. ***Electronic Communications Security (Pty) Ltd Act, 2002*** (Act 68 of 2002).

Republic of South Africa (RSA) Act. 2003. ***General Intelligence Laws Amendment Act, 2003*** (Act 52 of 2003).

Republic of South Africa (RSA) Act. 2008. ***Companies Act, 2008*** (Act 71 of 2008).

Republic of South Africa (RSA) Act. 2013. ***Protection of Personal Information Act, 2013*** (Act 4 of 2013).

Republic of South Africa (RSA) Bill. 2010. ***The Protection of State Information Bill, 2010***. Internet: http://www.parliament.gov.za/content/b%206b%20%202010%20(protection%20of%20state%20information)~1.pdf Access: 12 February 2012.

Republic of South Africa (RSA) Bill. 2015. ***Cyber Crimes and Cyber Security Bill, 2015***.

Republic of South Africa (RSA), National Council of Provinces (NCOP) Ad Hoc Committee on Protection of State Information Bill. 2012. ***Protection of State Information Bill [B6B-2010]: continuation of deliberations.*** Chairperson: Mr R Tau (ANC, Northern Cape); Date of Meeting: 09 May 2012. Internet: https://pmg.org.za/committee-meeting/14330/ Access: 15 May 2015.

© University of Pretoria

Republic of South Africa (RSA), Parliamentary Monitoring Group (PMG). 2012a. ***Minister's and Department's briefing: Protection of State Information Bill [B6B-2010],*** Date of Meeting: 24 January 2012. Internet: https://pmg.org.za/committee-meeting/13871 Access: 26 August 2015.

Republic of South Africa (RSA), Parliamentary Monitoring Group (PMG). 2012b. Ad Hoc Committee on Protection of State Information Bill (NCOP). ***Protection of State Information Bill [B6B-2010]: Continuation of deliberations***. Date of Meeting: 09 May 2012.
Internet: https://pmg.org.za/committee-meeting/14330 Access: 26 August 2015.

Republic of South Africa (RSA), Parliamentary Monitoring Group (PMG). 2012c. Ad Hoc Committee on Protection of State Information Bill (NCOP). ***Protection of State Information Bill: Some ANC proposals.*** Date of Meeting: 29 August 2012.
Internet: https://pmg.org.za/committee-meeting/14741 Access: 26 August 2015.

Republic of South Africa (RSA), Parliamentary Monitoring Group (PMG). 2012d. Ad Hoc Committee on Protection of State Information Bill (NCOP). ***Protection of State Information Bill: Further deliberations on ANC proposals***. Date of Meeting: 11 September 2012.
Internet: https://pmg.org.za/committee-meeting/14848 Access: 26 August 2015.

Republic of South Africa (RSA), Parliamentary Monitoring Group (PMG). 2012e. Ad Hoc Committee on Protection of State Information Bill (NCOP). ***Protection of State Information Bill: public hearing Day 1.*** Date of Meeting: 27 March 2012.
Internet: https://pmg.org.za/committee-meeting/14163/ Access: 26 August 2015.

Republic of South Africa (RSA), Parliamentary Monitoring Group (PMG). 2014. ***Proceedings on Bills up to Act Status.*** Internet: https://pmg.org.za/page/current-bills-status Access: 30 January 2015.

Republic of South Africa (RSA), State Security Agency (SSA). 2010a. ***Media statement: Protection of Information Bill Debate***, 25 August 2010.
Internet: http://www.ssa.gov.za/Portals/0/SSA%20docs/Media%20Releases/2010/Statement%20on%20the%20debate%20on%20POIB_24%20August%202010.pdf Access: 16 April 2016.

© University of Pretoria

Republic of South Africa (RSA), State Security Agency (SSA). 2010b. ***State security response to the public hearings on the Protection of Information Bill, 2010: Building a Secure, Prosperous and Open Society***.
Internet: http://www.ssa.gov.za/Portals/0/SSA%20docs/Speeches/2010/Response%20to%20Public%20Hearings%20POIB_17%20September%202010.pdf Access: 25 September 2014.

Republic of South Africa (RSA), State Security Agency (SSA). 2011. ***Media release: Ministry welcomes progress on the Protection of State Information Bill***, 05 September 2011.
Internet: http://www.ssa.gov.za/Portals/0/SSA%20docs/Media%20Releases/2011/Ministry_notes_progress_on_Info_Bill_02_Sept11.pdf Access: 16 April 2016.

Republic of South Africa (RSA), State Security Agency (SSA). 2012. ***Media release: Ministry welcomes NCOP passing of the Protection of State Information Bill***, 30 November 2012.
Internet: http://www.ssa.gov.za/Portals/0/SSA%20docs/Media%20Releases/2012/Media%20Release%20Ministry%20Welcomes%20NCOP%20Passing%20of%20the%20Protection%20of%20State%20Information%20Bill%2030%20November%202012.pdf Access: 16 April 2016.

Republic of South Africa (RSA), State Security Agency (SSA). 2013. ***Media release: Ministry welcomes the passing of the Protection of State Information Bill***, 25 April 2013.
Internet:
http://www.ssa.gov.za/Portals/0/SSA%20docs/Media%20Releases/2013/Ministry%20welcomes%20passing%20of%20the%20bill.pdf Access: 16 April 2016

Right2Know (R2K). 2013. ***Honour Andre Brink: Scrap the Secrecy Bill!*** *Posted in Secrecy Bill, 9 February 2013.* Internet: http://www.r2k.org.za/2015/02/09/statement-honour-andre-brink-scrap-the-secrecy-bill/ Access: 5 October 2015.

Roberts, B. 1990. Human Rights and International Security. ***Washington Quarterly*****,** 13(1): 65-75.

Rosenau, J. 1980*.* ***The Study of Global Interdependence.*** London: Frances Pinter.

Schwartzstein, SJD (ed). 1996. ***The Information Revolution and National Security Info and National Security: Dimensions and Directions***. Washington D.C.: The Center for Strategic Studies and International Studies.

© University of Pretoria

Segar, S. 2012. ***Cwele rejects apartheid tag on 'spy bill',*** 25 February 2012. Internet: http://www.iol.co.za/news/politics/cwele-rejects-apatheid-tag-on-spy-bill-1242601 Access: 3 October 2015.

Sethi, SP (ed). 1982. ***The South African Quagmire: In Search of a Peaceful Path to Democratic Pluralism***. Cambridge: Ballinger.

Shaw, S. 2001. ***South Africa's Transition to Democracy: An African Success Story. A Resource Book on the Positive Changes of the Nineties***. Cape Town: Sandy Shaw.

Smith, S. 2006. The Concept of Security in a Globalizing World. In Patman, RG (ed). ***Globalisation and Conflict: National Security in a 'New' Strategic Era***. Oxford: Routledge.

Snyder, CA. 1999a. Contemporary Security and Strategy. In Snyder, CA (ed). ***Contemporary Security and Strategy***. Houndmills: Macmillan.

Snyder, CA (ed). 1999b. **Contemporary Security and Strategy**. Houndmills: Macmillan.

Snyder, CA. 2012a. Contemporary Security and Strategy. In Snyder, CA (ed). ***Contemporary Security and Strategy***. 3rd edition. Houndmills: Palgrave Macmillan.

Snyder, CA (ed). 2012b. ***Contemporary Security and Strategy***. 3rd edition. Houndmills: Palgrave Macmillan.

South African History Archive (SAHA). 2011. A Black Wednesday for Apartheid SA and a Black Tuesday for Democratic SA, 22 November 2011.
Internet: http://www.saha.org.za/news/2011/November/a_black_wednesday_for_apartheid_sa and_a_black_tuesday_for_democratic_sa.htm Access: 27 January 2015.

South Africa Press Association (SAPA). 2000. ***Press Release:*** 'Bill Will End Secrecy: Maduna', 25 January 2000.

Sparks, C. 2011. South African media in comparative perspective. ***Ecquid Novi: African Journalism Studies***, 32(2): 5-19.

Sullivan, P. 2004. The Media after 10 Years of Democracy. A Democratic South Africa: Three Perspectives on the Role of Culture and the Contribution of Entertainment and the Media. In

© University of Pretoria

World Economic Forum, ***South Africa at 10: Perspectives by Political, Business and Civil Leaders***. Cape Town: Human and Rousseau.

Suzman, H. 1991. The Erosion of Accountability. In Du Toit, A (ed). ***Towards Democracy: Building a Culture of Accountability in South Africa***. Mowbray: Institute for Democracy in South Africa (IDASA).

Terry, T, Croft, T, James, L and Morgan, PM. 1999. ***Security Studies Today***. Cambridge: Polity Press.

Thomas, C. 2004. What is Human Security? A Bridge between the Interconnected Challenges Confronting the World. ***Security Dialogue***, 35(3): 353-354.

Totten, MJ. 2014. Year Four: The Arab Spring Proved Everyone Wrong. ***World Affairs***, July/August. Internet: http://www.worldaffairsjournal.org/article/year-four-arab-spring-proved-everyone-wrong Access: 24 August 2014.

United Nations Development Programme (UNDP). 1994. Human Security Report. New York: Oxford University Press. Internet: http://hdr.undp.org/sites/default/files/reports/255/hdr_1994_en_complete_nostats.pdf Access: 14 April 2013.

Urmson, JO and Sbisa, M (eds). 1962. ***How to Do Things with Words***. 2nd edition. Cambridge: Harvard University Press.

Vale, P. 2003. ***Security and Politics in South Africa: The Regional Dimension***. Boulder: Lynne Rienner.

Van Vuuren, DJ, Wiehahn, NE, Lombard, JA and Rhoodie, NJ (eds). 1985. ***South Africa: A Plural Society in Transition***. Durban: Butterworth.

Wæver, O. 1995. Securitization and Desecuritization. In Lipschutz, RD (ed). ***On Security***. New York: Columbia University Press.

Wæver, O. 2000. The EU as a Security Actor: Reflections from a Pessimistic Constructivist on Post Sovereign Security Orders. In Kelstrup, M and Williams, MC (eds). ***International Relations Theory and the Politics of European Integration***. London: Routledge.

© University of Pretoria

Wæver, O. 2011. Politics, Security, Theory. ***Security Dialogue***, 42(4-5): 465-480.

Walt, SM. 1991. The Renaissance of Security Studies. ***International Studies Quarterly***, 35(2): 211-239.

Wasserman, H (ed). 2013. ***Press Freedom in Africa: Comparative perspectives***. Abingdon: Routledge.

Weiner, M. 1992. Security, Stability and International Migration. ***International Security***, 17(3): 91-126.

Williams, MC. 2003. Words, Images, Enemies: Securitization and International Politics. ***International Studies Quarterly***, 47: 511–531.

Williams, PD (ed). 2008. ***Security Studies: An Introduction.*** New York: Routledge.

Wolfers, A. 1952. 'National Security' as an Ambiguous Symbol. ***Political Science Quarterly***, 67(4): 481 – 502.

World Economic Forum. 2004. ***South Africa at 10: Perspectives by Political, Business and Civil Leaders***. Cape Town: Human and Rousseau.

Wyn Jones, R. 1999. ***Security, Strategy and Critical Theory.*** Boulder: Lynne Rienner.

Yin, J. 2013. Growing pains in the Development of a Free Press in Africa and Asia: A Comparative Analysis – South Africa and India. In Wasserman, H (ed). ***Press Freedom in Africa: Comparative perspectives***. Abingdon: Routledge.

Zapiro. 2011. Cartoon: Secrecy Bill in historic perspective - Government action on the press - Black Wednesday Remembered. ***The Times*** (Johannesburg) 20 October 2011.
Internet: www.zapiro.com Access: 27 January 2015.

Zelikow, P. 2003. The Transformation of National Security: Five Redefinitions. ***The National Interest***, Spring 2003: 17-28.

© University of Pretoria

APPENDICES

Appendix A: *Promotion of Access to Information Act, 2000* (Act 2 of 2000): Selected excerpts

- **The objectives of the Act** (Chapter 3 Section 9) are:

(a) to give effect to the constitutional right of access to-

(i) any information held by the State; and

(ii) any information that is held by another person and that is required for the exercise or protection of any rights;

(b) to give effect to that right-

(i) subject to justifiable limitations, including, but not limited to, limitations aimed at the reasonable protection of privacy, commercial confidentiality and effective, efficient and good governance; and

(ii) in a manner which balances that right with any other rights, including the rights in the Bill of Rights in Chapter 2 of the Constitution;

(c) to give effect to the constitutional obligations of the State of promoting a human rights culture and social justice, by including public bodies in the definition of 'requester', allowing them, amongst others, to access information from private bodies upon compliance with the four requirements in this Act, including an additional obligation for certain public bodies in certain instances to act in the public interest;

(d) to establish voluntary and mandatory mechanisms or procedures to give effect to that right in a manner which enables persons to obtain access to records of public and private bodies as swiftly, inexpensively and effortlessly as reasonably possible; and

(e) generally, to promote transparency, accountability and effective governance of all public and private bodies by, including, but not limited to, empowering and educating everyone-

(i) to understand their rights in terms of this Act in order to exercise their rights in relation to public and private bodies;

(ii) to understand the functions and operation of public bodies; and

(iii) to effectively scrutinise, and participate in, decision-making by public bodies that affects their rights.

© University of Pretoria

- ***Provisos* to deny a request for access to information that concerns the defence, security and international relations of South Africa** (Section 41 Sub-section 1-4) where such disclosure:

(a) could reasonably be expected to cause prejudice to-

(i) the defence of the Republic:

(ii) the security of the Republic: or

(iii) subject to subsection (3), the international relations of the Republic; or

(b) would reveal information-

(i) supplied in confidence by or on behalf of another State or an international organisation:

(ii) supplied by or on behalf of the Republic to another state or an international organisation in terms of an arrangement or international agreement, contemplated in section 231 of the Constitution, with that state or organisation which requires the information to be held in confidence; or

(iii) required to be held in confidence by an international agreement or customary international law contemplated in section 231 or 232, respectively of the Constitution.

(2) A record contemplated in subsection (I), without limiting the generality of that subsection, includes a record containing information-

(a) relating to military tactics or strategy or military exercises or operations undertaken in preparation of hostilities or in connection with the detection, prevention, suppression or curtailment of subversive or hostile activities;

(b) relating to the quantity, characteristics, capabilities, vulnerabilities or deployment of

(i) weapons or any other equipment used for the detection, prevention, suppression or curtailment of subversive or hostile activities; or

(ii) anything being designed, developed, produced or considered for use as weapons or such other equipment;

(c) relating to the characteristics, capabilities, vulnerabilities, performance, potential, deployment or functions of-

(i) any military force, unit or personnel; or

(ii) any body or person responsible for the detection, prevention, suppression or curtailment of subversive or hostile activities;

(d) held for the purpose of intelligence relating to-

© University of Pretoria

(i) the defence of the Republic;
(ii) the detection, prevention, suppression or curtailment of subversive or hostile activities; or
(iii) another state or an international organisation used by or on behalf of the Republic in the process of deliberation and consultation in the conduct of international affairs;
(e) on methods of, and scientific or technical equipment for, collecting, assessing or handling information referred to in paragraph (d);
(f) on the identity of a confidential source and any other source of information referred to in paragraph (d);
(g) on the positions adopted or to be adopted by the Republic, another state or an international organisation for the purpose of present or future international negotiations; or
(h) that constitutes diplomatic correspondence exchanged with another state or an international organisation or official correspondence exchanged with diplomatic missions or consular posts of the Republic.

- **The public interest clause** (Chapter 4 Section 46) stipulating a mandatory disclosure [of records] in the public interest if:

(a) the disclosure of the record would reveal evidence of-
(i) a substantial contravention of, or failure to comply with, the law; or
(ii) an imminent and serious public safety or environmental risk; and
(c) the public interest in the disclosure of the record clearly outweighs the harm contemplated in the provision in question.

Appendix B: *Protection of State Information Bill*, *2010*: Selected excerpts

- **Definition of concepts** (Chapter 1 Section 1):

'security' means to be protected against danger, loss or harm, and is a condition that results from the establishment and maintenance of protective measures that ensure a state of inviolability from hostile acts;

'national security' means 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

© University of Pretoria

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;

'State security matter' includes any matter which is dealt with by the Agency (i.e. a breach of security at a port of entry violent protests that disrupt regular practise) or which relates to the functions of the Agency or to the relationship existing between any person and the Agency;

'protected information' means State Information which requires protection against destruction, loss or unlawful disclosure;

'information security' means the safeguarding or protecting of information in whatever form and includes, but is not limited to—
(a) document security measures;
(b) physical security measures for the protection of information;
(c) information and communication technology security measures;
(d) personnel security measures;
(e) continuity planning;
(f) security screening;
(g) technical surveillance counter-measures;
(h) dealing with and reporting of information security breaches;
(i) investigations into information security breaches; and
(j) administration and organisation of the security function at organs of state to ensure that information is adequately protected;

'legitimate interest' means an interest that is consistent with the Constitution,
applicable law and the mandate of an institution or organ of state;

'information' means any facts, particulars or details of any kind, whether true or false, and contained in any form, whether material or not, including, but not limited to—

© University of Pretoria

(a) documents, records, data, communications and the like, whether in paper, electronic, digital, audio-visual format, DVD, microform C, microphone, microfilm and microfiche form or format or any other form or format; and

(b) conversations, opinions, intellectual knowledge, voice communications and the like not contained in material or physical form or format.

- **The objectives of the Bill** (Chapter 1 Section 2) are to:

2. (a) regulate the manner in which State information may be protected;

(b) promote transparency and accountability in governance while recognising that State information may be protected from disclosure in order to safeguard the national interest of the Republic;

(c) establish general principles in terms of which State information may be handled and protected in a constitutional democracy;

(d) provide for a thorough and methodical approach to the determination of which State information may be protected;

(e) provide a regulatory framework in terms of which protected information is safeguarded in terms of this Act;

(f) define the nature and categories of information that may be protected from destruction, loss or unlawful disclosure;

(g) provide for the classification and declassification of classified information;

(h) create a system for the review of the status of classified in formation by way of regular reviews and requests for review;

(i) regulate the accessibility of declassified information to the public;

(j) harmonise the implementation of this Act with the Promotion of Access to Information Act and the National Archives and Records Service of South Africa Act, 1996 (Act No. 43 of 1996c);

(k) establish a National Declassification Database of declassified information that will be made accessible to members of the public;

(l) criminalise espionage and activities hostile to the Republic and provide for certain other offences and penalties; and

(m) repeal the Protection of Information Act, 1982 (Act No. 84 of 1982).

© University of Pretoria

- **Principles of the Information Bill** (Chapter 2 Section 6):

6. (a) Unless restricted by law or by justifiable public or private considerations, State information should be available and accessible to all persons;

(b) information that is accessible to all is the basis of a transparent, open and democratic society;

(c) access to information is a basic human right and promotes human dignity, freedom and the achievement of equality;

(d) the free flow of information promotes openness, responsiveness, informed debate, accountability and good governance;

(e) the free flow of information can promote safety and security;

(f) accessible information builds knowledge and understanding and promotes creativity, education, research, the exchange of ideas and economic growth;

(g) some confidentiality and secrecy is, however, vital to save lives, to enhance and to protect the freedom and security of persons, to bring criminals to justice, to protect the national security and to engage in effective government and diplomacy;

(h) measures to protect State information should not infringe unduly on personal rights and liberties or make the rights and liberties of citizens unduly dependent on administrative decisions; and

(i) measures taken in terms of this Act must—

(i) have regard to the freedom of expression, the right of access to information and the other rights and freedoms enshrined in the Bill of Rights; and

(ii) be consistent with article 19 of the International Covenant on Civil and Political Rights and have regard to South Africa's international obligations;

(j) paragraphs (a) to (i) are subject to the security of the Republic, in that the national security of the Republic may not be compromised.

- **National interests of South Africa** (Chapter 5 Section 11 Part A):

11. (1) The national interest of the Republic includes, but is not limited to—

(a) all matters relating to the advancement of the public good; and

(b) all matters relating to the protection and preservation of all things owned or maintained for the public by the State.

© University of Pretoria

(2) The national interest is multi-faceted and includes—

(a) the survival and security of the State and the people of South Africa; and

(b) the pursuit of justice, democracy, economic growth, free trade, a stable monetary system and sound international relations.

(3) Matters in the national interest include—

(a) security from all forms of crime;

(b) protection against attacks or incursions on the Republic or acts of foreign interference;

(c) defence and security plans and operations;

(d) details of criminal investigations and police and law enforcement methods;

(e) significant political and economic relations with international organisations and foreign governments;

(f) economic, scientific or technological matters vital to the Republic's stability, security, integrity and development; and

(g) all matters that are subject to mandatory protection in terms of sections 34 to 42 of the Promotion of Access to Information Act, whether in classified form or not.

(4) The determination of what is in the national interest of the Republic must at all times be guided by the values referred to in section 1 of the Constitution.

- **Classification guidelines** (Chapter 6 Section 17 Part A):

17 (1) For the purposes of classification, classification decisions must be guided by section 21 and the following:

(a) Secrecy exists to protect the national interest;

(b) classification of information may not under any circumstances be used to—

(i) conceal an unlawful act or omission, incompetence, inefficiency or administrative error;

(ii) restrict access to information in order to limit scrutiny and thereby avoid criticism;

(iii) prevent embarrassment to a person, organisation, organ of state or agency;

(iv) unlawfully restrain or lessen competition; or

(v) prevent, delay or obstruct the release of information that does not require protection under this Act;

© University of Pretoria

(c) the classification of information is an exceptional measure and should be conducted strictly in accordance with sections 11 [National Interest of the Republic] and 15 [Classification levels].

Appendix C: *Protection of State Information Bill, 2010*: Classification levels

Classification criteria (Chapter 6 Section 15 Part A Sub-section 1-3):

15. (1) State information may be classified as "Confidential" if the information is [—(a)] sensitive information, the [unlawful] disclosure of which is likely or could reasonably be expected to cause demonstrable harm [may be harmful] to the security or national [interest] security of the Republic or could reasonably be expected to prejudice the Republic in its international relations;

[(b) [commercial information] the disclosure of which may cause financial clients, competitors, contractors and suppliers.]

(2) State information may be classified as "Secret" if the information is—

(a) sensitive information, the disclosure of which is likely or could reasonably be expected to cause serious demonstrable harm to [endanger] the security or national [interest] security of the Republic or likely or could reasonably be expected to jeopardise the international relations of the Republic; or

[(b) commercial information, the disclosure of which may cause serious financial loss to an entity;]

(c) personal information, the disclosure of which [may] is likely or could reasonably be expected to endanger the physical security of a person.

(3) State information may be classified as "Top Secret" if the information is—

(a) sensitive information, the disclosure of which [may] is likely or could reasonably be expected to cause serious or irreparable harm to the national [interest] security of the Republic or [may] is likely or reasonably be expected to cause other states to sever diplomatic relations with the Republic;

[(b) commercial information, the disclosure of which may—

(i) have disastrous results with regard to the future existence of an entity; or

© University of Pretoria

(ii) cause serious and irreparable harm to the security or interests of the state; (d) personal information the disclosure of which [may] is likely or could reasonably be expected to endanger the life of the individual concerned.

- **Request for status review of classified information** (Chapter 7 Section 23)

23. (1) A request for the declassification of classified information may be submitted to the head of an organ of state by an interested non-governmental party or person.
(2) Such a request must be in furtherance of a genuine research interest or a legitimate public interest.

Appendix D: Zapiro cartoon

A cartoon by Zapiro, the prominent South African satirical cartoonist, depicting the dominant media sentiments at the time when the Bill received more media attention. This cartoon was related to the 'Black Tuesday' event, as a recall to the Black Wednesday event of the 1970s, when the BCM and aligned activists were banned.

(Zapiro 2011)

© University of Pretoria