THE SECURITISATION OF CYBERSPACE IN SOUTH AFRICA: THE TENSION BETWEEN NATIONAL SECURITY AND CIVIL LIBERTIES

By

Edwin Papie Hlase

Student Number: 96195577

A mini-dissertation submitted in partial fulfilment of the requirements for the degree

Master of Security Studies (MSS),

Department of Political Sciences,

Faculty of Humanities, University of Pretoria

Supervisor: Mr R. D. Henwood

March 2018

UNIVERSITY OF PRETORIA

FACULTY OF HUMANITIES

RESEARCH PROPOSAL & ETHICS COMMITTEE

DECLARATION

Full name: Edwin Papie Hlase ____

Student Number: 96195577____

Degree/Qualification: Master of Security Studies_____________________

Title of thesis/dissertation/mini-dissertation:
The Securitisation of Cyberspace in South Africa: The Tension between National Security and Civil Liberties

I declare that this thesis / dissertation / mini-dissertation is my own original work. Where secondary material is used, this has been carefully acknowledged and referenced in accordance with university requirements.

I understand what plagiarism is and am aware of university policy and implications in this regard.

____________________ 28 March 2018

SIGNATURE **DATE**

ABSTRACT

The concepts of national security and civil liberties have had a conflictual relationship throughout the history of human societies. Most societies have always strived to create a form of government that will maximise the security of individuals within the society while allowing each member to pursue their goals without encroaching on the rights and lives of others. This tense relationship between the two concepts came to be heightened by modern developments such as technology, mass migration and transnational terrorism. In particular, the development of cyberspace as technology advanced in the 20th century had a profound impact on the concepts of national security and civil liberties across the global political landscape, as states' critical information infrastructures and private businesses have increasingly come to rely on cyber systems. Cyberspace, particularly with the arrival of the Internet in the late 1980s, created a virtual space for all members of society to interact and conduct social, political and business activities within and across borders. While this has had a positive impact in terms of economic and other opportunities for most people, it has also provided an innovative way for criminals and other actors to conduct illegal activities, with potential destructive consequences on businesses and state institutions as cyberspace proved to be plagued by security vulnerabilities. The overall response by most states to the potential national security threats posed by cyberspace has been the securitisation of the cyberspace domain, which has come to have negative implications on citizens' civil liberties. Since 2010, South Africa has also gradually been implementing and drafting cybersecurity policies that have followed the typical securitisation trajectory.

This study analyses the securitisation of cyberspace in South Africa. The research will contextualise the concepts of national security and civil liberties in relation to cybersecurity. The study will also examine the development of cybersecurity in South Africa and how it has impacted on the civil liberties of citizens and the country's national security. In highlighting the various cyberattacks and consequences suffered in the country, this study will analyse the cyber-securitisation processes in South Africa, how it has affected civil liberties, how national security and civil liberties in South Africa can be balanced through cybersecurity, and whether securitisation of cyberspace in South Africa is necessary or not.

ACKNOWLEDGEMENTS

First and foremost, I thank the Omnipresent, Everlasting and Almighty God, without whom I could do and would be nothing.

I sincerely thank my supervisor at the Department of Political Sciences, Mr Ronald Henwood, whose expert guidance, motivation and assertiveness helped me towards the right direction, finding the most relevant sources and to build up my argument. Mr Henwood's contribution in completing this dissertation is truly appreciated.

A special thanks to my parents, Richard Hlase and Hunadi Hlase, my brother Joshua Hlase, my sister, Mmabatho Hlase, and my beloved niece, Mahlaku Hlase. I am deeply grateful for the support and encouragement throughout the time of conducting this study. This study would not have been possible without the support of my family.

TABLE OF CONTENTS

CHAPTER 1: RESEARCH OVERVIEW

ABBREVIATIONS/ ACRONYMS

ANC	African National Congress
CAC	Cybercrimes and cybersecurity Bill
CCDCE	Cooperative Cyber Defense Center of Excellence
CNII	Critical national information infrastructure
CSIR	Council for Scientific and Industrial Research
EIS	Electronic information systems
GDP	Gross Domestic Product
ECTA	Electronic Communications and Transactions Act
ECSPs	Electronic Communications Service Providers
IEC	International Electrotechnical Commission
ICT	Information Communications Technology
IoT	Internet of Things
IR	International Relations
ISO	International Organisation for Standardization
ISPs	Internet Service Providers
ITU	International Telecommunication Union
NATO	North Atlantic Treaty Organisation
NCPF	National Cyber Security Policy Framework
PPI	Protection of Personal Information
PSI	Protection of State Information
RICA	Regulation of Interception of Communications and Provision of Communication-related information Act

Stats SA	Statistics South Africa
SSA	State Security Agency
UNHRC	United Nations Human Rights Commission
UN	United Nations
UNODC	United Nations Office on Drugs and Crime
US	United States
WWW	World Wide Web

CHAPTER 1: RESEARCH OVERVIEW

1.1. IDENTIFICATION OF THE RESEARCH THEME

The tension between the concepts of security and liberty can be found throughout the recorded history of human life. Societies have always grappled with constructing a form of government that will maximise the security of every individual member of the society while allowing each member to pursue happiness without endangering the rights and lives of fellow members. The tension between the modern concepts of national security and civil liberties has its roots in the formation of the Westphalian state– modern states with physical boundaries. National security hardliners have consistently argued that civil liberties are political conveniences for enjoyment in times of peace (Posner, 2001: 46; Baker, 2003: 549). Therefore, these should not constitute restraining benchmarks for governments in times of national security crises (Baker, 2003: 549). On the other hand, advocates of liberal ideals maintain that "it is particularly in times of crisis that the liberal democratic state must adhere strictly to its defining principles" (Cole & Dempsey, 2002: 13). Accordingly, civil liberties will be futile if they can easily be supressed by the authorities acting under some orders to contain a certain emergency.

The 20th and 21st centuries saw revolutionary advances in social and political life that have had a greater influence on the tension between security and liberty. Technological advances in communications and transportation in particular improved nations' abilities to interact; to conduct political, economic and social relations in ways that negated the physical boundaries of the Westphalian state. However, such advances have also made it easier for states, individuals and organisations to engage in unethical and harmful activities; ranging from crime, terrorism, espionage to warfare. Consequently, these security challenges have been met by state responses which have varied according to political systems. In liberal democratic states, responses to these developments that have challenged national security in new ways had to be tailored in accordance with the founding liberal democratic principles, particularly civil liberty and transparency in government.

Amongst the technological developments of the 20th and 21st centuries emerged electronic information systems (EIS) – interconnected and interdependent hardware and software that include computers, computer networks, digital data and other related equipment – that have generally become known as ‘cyberspace’. Within cyberspace, lies what is considered “one of the most important and powerful creations in all of human history”: the Internet (Mohammed & Ahmed, 2017: 127). Though there’s a conceptual distinction between the two terms, the Internet and cyberspace have become synonymous terms in everyday language. The Internet is recognised as one of the greatest inventions that has greatly improved human life. It has created a transnational horizontal platform for information sharing among ordinary citizens of different countries. Ordinary people across borders are now able to share information and ideas without the government’s involvement. This development has caused historical political turbulences in some autocratic regimes, such as Tunisia, Egypt and Syria, which depended on information control and propaganda to keep the citizenry in control.

However, cyberspace has also created a virtual reality that facilitates various malicious activities that carry potentially dangerous and devastating real-life effects. Accordingly, individuals have suffered theft of their monies, large corporations have been robbed massive amounts of money across the world, and nations’ military systems have been infiltrated by enemy agents; all through the domain of cyberspace. These have added new dimensions to national security and created new state and societal adversaries marked by terms such as cybercrime, cyberterrorism, cyberespionage and cyberwarfare.

South Africa is one of the African countries which has been greatly influenced by the rise of cyberspace, particularly the Internet. Since the early 1990s as it emerged from a difficult past, cyberspace contributed to the development of a fairly sophisticated Information and Communications Technology (ICT) sector in the country that has become a keystone of its economy and a fundamental aspect of national strategic policy. As such, South Africa has become increasingly reliant on ICT for business, social and political activities. Moreover, this sector holds the promise for economic and social development, job creation, and provides a space for innovative explorations. However, as in other ICT-driven countries, the cyber-environment in South Africa has also ushered in new challenges to the country’s citizens, businesses and the government. Large and small corporations, government entities and millions of individuals in the country have already suffered attacks through cyberspace; some of which, as will be explained later in this paper, have reached South Africa's highest levels of political power, resulting in manipulation and loss of top state secrets and economic damages that have amounted to billions of rands on an annual basis. Furthermore, such infiltrations have exposed the dreaded possibility that, if enemy agents can breach the country's highest security features and manipulate highly classified data, it is then highly likely that they can cause devastating destruction on the country's critical national information infrastructure (CNII) that rely on the effective functioning of EIS or cyberspace. For instance, it means that adversaries can break into the country's national defence computer systems and sabotage radar or missile launching systems, leaving the country vulnerable to invasion or attacks by other states or non-state actors. Other examples are that enemy actors can hack into air traffic control systems at major airports; or break into the national energy grid and shut down the country's power supply; or breach water supply systems and sabotage the distribution of water. Such scenarios could have devastating impacts on the country's national and economic security if they were to materialise.

However, there is scepticism about the likelihood of such scenarios becoming a reality in South Africa. Some critics have argued that such scenarios are wilfully propagated into mainstream media and politics by the government in order to justify repressive policies and to maintain control on society. However, and perhaps most importantly, if cyberspace then contains potentially catastrophic threats to South Africa's national security, what measures must be put in place to curb the threats, bearing in mind that the country is a constitutional democracy. In this way, debates on national security and civil liberties have intensified as civil freedoms as well as national security threats have expanded to the internet. As Finkelstein *et al* (2017: 293) noted, "Policymakers are faced with the delicate task of increasing the security of the nation without imposing an undue burden on the public". Cyberspace has thus created a paradoxical phenomenon– a platform for human development, yet a source of national security threats.

South Africa, like most countries, have followed the typical securitisation trajectory in order to address rising and constantly changing threats to national security emanating from cyberspace. As a result, the government has been confronted by significant criticisms from civil society groups for its approach to cybersecurity. Therefore, this study will provide an explanatory research on the securitisation of cyberspace in South

Africa and how national security and civil liberties in the country have been impacted by this process.

1.3. STUDY OBJECTIVES

First, the purpose of this study is to analyse how the concepts of national security and civil liberties have been understood throughout early and modern political societies. Secondly, this study aims to track the development of cyberspace and how it has evolved from simply being an advancement in communications technology to becoming a human rights need and, most importantly, a key national security priority across nation-states of the world, with some negative implications on civil liberties.

This will help to identify the reasons behind processes of change in national security dynamics, as well as, to assess the impacts of such changes on existing norms related to civil freedoms. To this degree, the main aim is to contextualise and provide a deeper understanding on the basis and rationale of the securitisation of cyberspace in South Africa, in order to establish whether the country's approach to cybersecurity is warranted or not; as well as to examine how to mitigate on the undesired consequences of securitisation.

1.4. FORMULATION AND DEMARCATION OF THE RESEARCH PROBLEM

The fundamental research problem that this study focuses on is whether threats emanating from cyberspace pose real national security threats to South Africa, and, therefore, whether the country's securitisation approach to cybersecurity is necessary or not. The significance of this research problem is that South Africa is a constitutional democratic state and its approach to cybersecurity has met intense criticisms for its potential to become a licence for the government to violate constitutionally protected civil liberties of citizens. In order to seek a thorough understanding of South Africa's dilemma, this study analyses the following issues:

- The meaning of the concepts of national security and civil liberties, and the nexus between the two concepts
- The development of cyberspace and its impact on both national security and civil liberties

- How cybersecurity has consequently and rapidly developed to become a strategic national security priority across the world

These will provide a broader picture on the meaning of national security and civil liberties, as well as how the rise of cyberspace has come to influence citizens' freedoms, which, in turn, had implications on states' national security.

By understanding the meanings of national security and civil liberties, this study will demonstrate that the two concepts have been and continue to be intertwined and essential for human progress. However, it will also be shown that an expansion of liberty can lead to a weakening of security, and vice versa. With the rise of cyberspace, particularly the Internet, individuals, organisations and governments across the world can participate in economic, social and political activities within a virtual space that have real life effects. Accordingly, this has had positive and negative effects. The positives include the fact that cyberspace has expanded civil freedoms such as access to information, freedom of speech and expression, as well as presenting some entrepreneurial opportunities. On the other hand, the cyber environment has also enabled criminals to infiltrate and manipulate confidential data held in the EIS of governments and businesses; sabotaging programmes and stealing large sums of money. To this end, it has become a common assumption that a "world cyberwar" may be looming. In this way, the process of securitisation of cyberspace will be put within the global context. This study will then analyse the South African securitisation process focusing on the following issues:

- The development of cyberspace in South Africa
- How the cyber-revolution impacted on South Africa
- Attempts by the South African government to alleviate the dangers of cyberspace
- The question of the whether cyberspace poses a real national security danger to South Africa: are the threats deliberately exaggerated by the government to restrict civil liberties and impose tyrannical control over the masses, or are the threats real?
- Lastly, whether national security measures in cyberspace can be reconciled with citizens' civil liberties

This study focuses on the rise of cyberspace in South Africa and how it has impacted on citizens' civil liberties and the country's national security during the period 2000 to

2017, though certain references in the 1990s will be covered. Between 2000 and 2017, cyber-activity grew rapidly in the country, and it is also the time in which South Africa experienced increasing cyberattacks against businesses, individuals and the government. Moreover, during this period, particularly in the last seven years, the South African government began implementing and proposing cybersecurity policies that have been framed within the securitisation paradigm.

1.5. LITERATURE REVIEW

In light of the study objectives and demarcation of the research problem, the first section of this literature review analyses explanations of national security and civil liberties in both classical and contemporary political philosophy. The second section will examine perspectives on cyberspace in the literature, and how the cyber domain influences civil freedoms as well as national security, including in South Africa.

1.5.1. National security versus civil liberties

The subject of national security and civil liberties can be traced to classical political philosophy, found in the works of early philosophers such as John Locke (1690), Thomas Hobbes (1651), and William Blackstone (1803), among others. A convergent viewpoint found in classical political thought is that individuals in a state of nature are entitled to natural liberty– the natural freedom that individuals enjoy before the establishment of civil laws and a political government. However, such unrestrained freedom cannot be effectively exercised and is itself a threat to life as anyone is free to act according to their own wishes, whether moral or immoral (Locke, 1690b: 6) . Therefore, it is exactly the main reason individuals opted for organised politically governed societies that provide limited liberties (civil liberties) and security by virtue of being a member of the collective (Blackstone, [1803] 1969: 251; Cartwright & Condé, 2000: 26; Skaaning, 2006: 4). From this perspective, the liberties of individuals are thus subject to laws of the society, and addressing particular situations that threaten the very existence of the collective may have temporary negative implications on the liberties of members of the society. In this way, every individual can exercise their limited liberties in return for a relatively secure existence. This is where the idea of national security– the protection and preservation of a nation and its core interests– becomes apparent.

Although the concept of national security can be traced to ancient societies by characteristics of its meaning, national security as a political concept emerged in the 20th century with a particular meaning revolving around the protection of a nation and its core interests within a particular bordered geographic territory (Fjäder, 2014: 117; Goldman 2001:43; Neocleous, 2006: 363). While the concept has been shadowed by ambiguity (Wolfers, 1951), political realism has produced a domineering standpoint on the meaning of national security that posits it as the paramount national interest that prevails above all other interests (Waltz, 1979: 126; Fjäder, 2014: 116-117). National security is about survival of the nation and all other interests and objectives of the nation come second and must be in harmony with national security. In other words, when the very existence of the nation is under threat from particular developments or entities, exceptional measures are put in place to address the threat in order to preserve the nation. When the national security threat has been contained, then other national interests can be pursued in accordance with the national security objectives. This perspective continues to be the dominant approach to national and foreign policy-making across the world.

The tension between national security and civil liberties in modern politics attained prominence in the aftermath of the 2001 September 11 (9/11) terrorist attacks in the United States (US), which ushered in the "war on terror" and "securitisation of domestic life" (Baker, 2003: 548). Accordingly, as Baker (2003:548) noted, this restored 'wartime' views in modern societies that "civil liberties are generally categorized as luxury items, like silk stockings during World War II, that divert valuable resources from the war effort". George (2005: 219-220) observed that, "once the period of mourning came to a close, the question arose how life would ever return to normal…we also cannot afford to ignore the dangers of the current environment and pretend that the malevolence of our enemies cannot exploit the very openness of our open society to further their evil ends". Lopach & Luckowski (2006: 246) also noted that, "the world finds itself confronted by an enemy that is not defined by borders or boundaries". Thus, the crucial question for intellectuals and policymakers concerns how governments effectively balance the provision of civil rights and liberties with the appropriate level of national security measures in times of crises.

Warshawsky (2013: 95) argued that "though civil liberties have not always existed in their current form, and are not universally accepted, there has, in most cases, been recognition of the fact that citizens sacrifice some degree of their freedom when there is a threat present". This is an inevitable trade-off that many scholars and policymakers seem to acknowledge (Buzan *et al*.1998: 24; Fjäder, 2014: 117; Goldman, 2001:43). In line with this perspective, Lowe (2016: 654) indicated that, "national security and individual liberty are mutually inclusive concepts, as the state has a responsibility to protect an individual's personal liberty, but equally important the state must also protect its population from terrorist attacks".

The dominant perspective across the literature is that compromises between national security and civil liberties are often inevitable. In particular, when national security is under threat all other interests of the nation may be put on hold to ensure the survival of the nation.

1.5.2. Cybersecurity, national security and civil liberties

The technological advances and information digitisation of the 20th century that produced the cyber domain has had one of the most profound impacts on modern societies. Today cyberspace has become both a human rights essential and a strategic national security concept of states (Alexander & Shore, 2016; Geers, 2011: 4; Liff, 2012: 401; UNHRC, 2016). Cyberspace, particularly as a result of the Internet, provides a means that enables easy communications across nations as well as a cost-effective business and political platform. However, it is also an environment in which individuals, businesses and governments often engage in conflictual interactions. Cobb (1999:146) argued that, "the conflicts involving cyberspace are the most serious national security threats facing nations since the development of nuclear weapons in the 1940s". Geers (2011:12) noted that, "today, cyber-attacks can target political leadership, military systems, and average citizens anywhere in the world, with the added benefit of attacker anonymity". Dunn-Cavelty (2013: 105) also noted that "the cybersecurity discourse is about more than one threat form: ranging from computer viruses and other malicious software to cybercrime activity to the categories of cyber-terror and cyberwar".

The events on 9/11 highlighted the significance of information technology on security, "to questions of digital infrastructure protection, surveillance, cyberterrorism, and the internet as a networked platform for communication across and against states" (Latham 2003:1; Hansen & Nissenbaum, 2009: 1155-1156). Thus, the link between national security and cyberspace has become an undeniable fact with economic and political consequences (Dunn-Cavelty, 2013: 105). Dunn-Cavelty (2013: 106) argued that only a broad understanding of cyber-security as discursive practice by a multitude of state and non-state actors reveals the variety of choices available to political actors at all times and enables us to show what the consequences of such choices are.

The literature demonstrate that the domain of cyberspace has added new dimensions and complexity to national and global security. Research on the double sided effects that the Internet has manifested into the social, economic and political landscapes of South Africa appears limited. Nevertheless, Dlamini (2012: 1) noted that, “Increased bandwidth and proliferation of mobile phones with access to the Internet in South Africa imply increased access to the internet by the South African population”. On the other hand, “such massive increases in access to the internet increases vulnerabilities to cybercrime and attacks and threatens the national security” (Dlamini, 2012: 1). Grobler, van Vuuren & Zaaiman (2013: 32) point out that “South Africa at present does not have a coordinated approach in dealing with Cybercrime and does not have a comprehensive Cyber defence strategy in place”.

In summary, the literature shows that the meaning of national security and civil liberties evolved as individuals in a state of nature gradually moved to becoming members of political societies comprising civil laws and rights. In this, members of the society sacrifice some of their freedoms in exchange for protection by the force of the collective.

However, the tension between national security and civil liberties in relation to the domain of cyberspace has not been studied extensively, particularly in South Africa.

1.6. RESEARCH METHODOLOGY

This research adopts an explanatory, qualitative approach and will be a literature-based study relying on secondary, and some primary, resources, such as books, journals, newspapers, research publications, the Internet, government Acts and publications. A qualitative approach is suitable for the purpose of this study; in order to illuminate the contexts and to critically analyse the meanings and links between the concepts of national security, civil liberties and cybersecurity.

Besides limitations such as time and lack of resources, this study does not require field research. The nature of the topic and research question lend themselves well to a literature-based design because substantial studies have been conducted on the subject of national security and civil liberties. Likewise, there are equally sufficient scholarly works on cybersecurity. Therefore, this study is well positioned to extract valuable information from these resources to analyse, critically engage and provide meaningful explanations on the dynamics between national security and civil liberties, and to evaluate the basis and rationale of the South African government's approach to cybersecurity.

This study will be designed around a *traditional review design*, with particular application of a *critical conceptual review*, to analyse how concepts such as national security, civil liberties and cyberspace, are explained in the literature, and also how such concepts have been understood in relation to other security issues. This will provide insight on whether or not such meanings can be equally applied in the context of this study's research problem, and help to illuminate whether the South African government's threat perception and approach to cybersecurity are realistic or not.

1.7. RESEARCH DESIGN

CHAPTER 1: RESEARCH OVERVIEW

Chapter one introduces the research theme and identifies and contextualises the research problem of this study, namely the evolution of the meanings of national security and civil liberties and how cybersecurity has come to be a vital aspect in the contemporary shape of the two concepts. Secondly, the objectives of this study will be explained. Thirdly, a literature review will be outlined in order to provide classical and contemporary understandings of national security and civil liberties, as well as perspectives on cybersecurity. Lastly, this chapter explains the research methodology and design.

CHAPTER 2: NATIONAL SECURITY AND CIVIL LIBERTIES

Chapter two will provide an analysis of the relationship between the concepts of national security and civil liberties. The Copenhagen School's theory of securitisation will first be explained in order to clarify processes of securitisation. The chapter will then examine the definitions of national security and civil liberties in early and modern political philosophy. This will help highlight the reasons behind the evolution of the two concepts as individuals moved from the state of nature to politically governed societies, which themselves also grapple with evolving security challenges that continue to impact on accepted social and political norms.

CHAPTER 3: CYBERSPACE AND ITS IMPACT ON NATIONAL SECURITY AND CIVIL LIBERTIES

Chapter three analyses the development of cyberspace and how it has influenced modern societies. This will commence with examining the meaning of cyberspace and how it has risen to become a key component of modern societies, with both positive outcomes and negative consequences such as cybercrime and cyberterrorism. How cybersecurity consequently evolved to become a national security priority across the world will then be analysed. Lastly, this chapter will explore the impact of cybersecurity as a national security priority, and the tension between national security and civil liberties.

CHAPTER 4: THE SECURITISATION OF CYBERSPACE IN SOUTH AFRICA

Chapter four analyses the process of securitisation of cyberspace in South Africa. This will first explore the historical development of cyberspace in South Africa, and how the cyber domain has positively and negatively impacted on socio-political and economic activities in the country. This will lead to scrutinising attempts by the South African government to tackle the national security threats emanating from cyberspace, which have faced criticisms for being framed within the securitisation paradigm and thereby threatening civil liberties. Lastly, this chapter will critically tackle the question of whether cyber-threats pose real national security dangers in South Africa, and what should be the acceptable legal framework in order to balance national security and civil liberties.

CHAPTER 5: CONCLUSION

The last chapter will summarise the study and highlight the main findings. This will be followed by a discussion on the relevance and structure of the study. In conclusion, the main argument will be emphasised, with recommendations and areas for future research.

CHAPTER 2: NATIONAL SECURITY AND CIVIL LIBERTIES

2.1. INTRODUCTION

In this chapter, the relationship between the concepts of national security and civil liberties will be explored. First, the theory of securitisation will be explained in order to understand the central features of securitisation. Secondly, the meaning of national security will be analysed, beginning from its traditional conception to its contemporary meaning. Thirdly, the chapter will delve into the definitions of the concept of civil liberties. Like security, the concept of liberty has its roots in classical political philosophy which require to be examined in order to have an enriched understanding of civil liberties in modern politics. Thirdly, an analysis of the tense relationship between national security and civil liberties will be outlined.

In conclusion, it will be shown that civil liberties and national security are not antithetical concepts. Rather, they are mutually inclusive and reinforcing. However, since any expansion on any one of them is a potential weakening of the other, a trade-off, as the literature review showed, is often inevitable.

2.2. SECURITISATION THEORY

To understand the securitisation of cyberspace, it is important to understand the central argument of *securitisation theory*. It is through securitisation that a non-security issue becomes an issue of security. In simple terms, securitisation refers to a process in which the authorities declare a particular issue to be an existential threat to the nation in order to implement exceptional measures to address the issue.

Assuming a constructivist ontological standpoint, securitisation theory conceptualises security as a process underlined by the intersubjective formation of an existential threat to a particular referent object with sufficient saliency that it somehow effects political action (Buzan et al., 1998: 25). The concept of securitisation was introduced to the field of International Relations (IR) by the Copenhagen School in the mid-1990s, following a research agenda on security dynamics in Europe (Buzan et al., 1990; Wæver et al., 1993). It was further developed into a fully-fledged theoretical and analytic framework by Buzan et al (1998). Initially, the emphasis was on ‘speech act’, in which the act of verbally positioning a particular issue as an existential threat to a particular ‘referent object’ (that which has to be protected) itself amounted to securitisation. Then the role of audiences or constituencies was later recognised as an important factor in supporting speech acts and was thus incorporated into the theory (Buzan et al., 1998: 26–33). Accordingly, speech acts or ‘securitising moves’ sought the consent of the audience it is presented to for securitisation to occur.

The fundamental argument of securitisation theory is that security is an illocutionary act, in which the act of speaking or saying ‘security’ has the power to create ‘a new social order’ (Balzacq, 2005: 171; Stritzel, 2007: 361; Wæver, 2004: 13). As Wæver (2004: 13) puts it, ‘It is by labelling something a security issue that it becomes one’. This act of identifying an existential threat upon a particular referent object, an actor (usually a political leader) announces and rationalises the need for exceptional measures to ensure the survival of the referent object. If the relevant audience accept it, it will be followed by the removal of the issue from the realm of ‘normal politics’ into the sphere of ‘crises politics’, and then the implementation of exceptional measures in responding to the perceived security crisis. In this way, the issue can swiftly be addressed without having to undergo the normal, at times, lengthy policy-making processes.

To avoid undue processes, securitisation comprises three steps: First, an existential threat and a referent object have to be identified; secondly, consent of the relevant audience and subsequent politicisation of the issue; and lastly, the suspension of normal day-to-day activities (Buzan et al. 1998: 6). The fundamental point, as Buzan et al. (1998: 24) put it, is that “If we do not tackle this problem, everything else will be irrelevant (because we will not be here or will not be free to deal with it in our own way)”. Securitisation is therefore motivated by the fear that if extraordinary measures are not immediately implemented to address the issue, the consequences may debilitate or destroy the referent object. An important point to highlight for the purposes of this study is that, the implementation of exceptional measures to contain threats consequently becomes a subject of contestation between the authorities and the public as some civil liberties can be temporarily or even permanently revoked.

However, the Copenhagen thinkers oppose securitisation processes. They argued that “security should be seen as a negative, as a failure to deal with issues of normal politics” (Buzan et al. 1998: 29). As a result, they proposed desecuritisation– the removal of issues out of crisis mode and into normal politics wherein they can be addressed through normal policy-making processes.

Having clarified what securitisation is, the next section will discuss the meaning of national security from its traditional conceptions to post-Cold War era perspectives.

2.3. DEFINING NATIONAL SECURITY

The concept of national security has largely been expressed in narrow terms, usually considered to simply mean the preservation of the territorial and sovereign integrity of a nation-state as well as its core political and cultural values, particularly against external military threats, and, to a lesser extent, internal threats (Ullman, 1983: 129; Chandra & Bhonsle, 2015: 337; Goldman, 2001: 43; Fjäder, 2014: 117). Accordingly, because such threats are commonly associated with the use or threat to use force, national security is considered to pivot primarily on the state’s ability or inability to pacify threats and to influence or coerce certain actors to act in accordance with the state’s core national interests. However, the meaning of national security has not always been clear. Arnold Wolfers (1952: 481) argued that the concept of national security “need to be scrutinized with particular care”, as it “may not mean the same thing to different people; while appearing to offer guidance and a basis for a broad consensus they may be permitting everyone to label whatever policy he favours with an attractive but possibly deceptive name”. Wolfers, however, declared that “it would be an exaggeration to claim that the symbol of national security is a stimulus for semantic confusion, though closer analysis will show that if used without specifications it leaves room for more confusion than sound political counsel” (1952: 483).

2.2.1. The traditional concept of national security

The concept of national security has been a subject of debate in the field of IR and security studies due to its ambiguity as a result of the contested nature of the term ‘security’ itself. The concept of security attracted political thinkers in the aftermath of the two World Wars and rose to prominence during the Cold War. However, a clear and comprehensive definition remained elusive (Haftendorn, 1991: 15; McSweeney, 1999:1; Schultze, 1973: 529-530). “For how is security to be achieved? Who is to be secured, against which dangers? And, more importantly, what actually happens when we ‘speak’ security?” (Von Boemcken & Schetter, 2016: 01); persisted to be questions to which scholars seemingly never reach consensus on. Wolfers (1952: 484) observed that, “the term ‘security’ covers a range of goals so wide that highly divergent policies can be interpreted as policies of security”. Baldwin (1997:09) claimed that the problem with security is that it has not “received the serious [conceptual] attention accorded to other concepts such as justice and equality”. Nevertheless, security in its traditional conception generally referred to the protection of acquired values, such as life, society, territory, and so on (Baldwin, 1997: 13; Bourne, 2014: 1; Wolfers, 1952: 484).

Baldwin (1997:21) noted that the realist school of thought, influenced by early thinkers such as Thomas Hobbes and Niccollo Machiavelli, “devoted remarkably little attention to explaining what security means”. However, political realism became the dominant perspective on the subject of security. Prominent neo/realists such as Kenneth Waltz and Hans Morgenthau viewed security as the paramount national interest of the state because the anarchic nature of the international environment poses existential threats to the state. Morgenthau (1952: 973) argued that, “The survival of a political unit, such as a nation, in its identity is the irreducible minimum, the necessary element of its interests vis-a-vis other units”. Waltz (1979: 126) upheld this argument when he observed that, “In anarchy, security is the highest end. Only if survival is assured can states seek such other goals as tranquillity, profit, and power”. In this way, the state was the primary actor as both the referent object and the provider of security.

The realist concept of security was thus aptly reflected in the concept of national security, which is “above all maintaining security within a geographically defined territory in order to protect the survival of the state against both external and internal threats” (Fjäder, 2014: 117; Goldman 2001:43). Similar to ‘security’, however, the concept of national security became a subject of debate and contestation. Neocleous (2006: 363) traces the first usage of the term ‘national security’ to the Cold War era when the United States replaced its Council of Common Defense with the National Security Act and the National Security Council. According to Neocleous, this signified a paradigm shift from the narrow and militarist concept of ‘defence’ to a seemingly more extensive notion of security. However, the meaning of national security at this time stemmed from the same line of political thought whose point of departure was that the state must be entrusted with "the absolute monopoly upon the legitimate use of physical force and that security is the core responsibility of a nation-state" (Fjäder, 2014: 116-117).

The concept of national security has therefore been founded on the realist paradigm according to which nation-states compete for survival and power within an environment devoid of a central authority. In this context, states depend on their military capabilities and economic power to safeguard their interests. Again, this narrow conception of national security was propagated into mainstream IR and global politics by realists and became the dominant perspective, particularly in the aftermath of World War II and during the Cold War. The prevailing argument was that the utopianism of liberalism led states to naivety as they failed to appreciate the unforgiving and brutality of the anarchic international system.

2.2.2. The meaning of national security in the post-Cold War era

The global nuclear threat of the Cold War coupled with the horrific scenes of World War I and II spurred a need to start thinking about how to avoid wars rather than how to fight them. As a result, by time the Soviet Union collapsed and the Cold War ended in 1989, a new conception of security had emerged among European scholars. The "broadening" of security encompassed not just the military but also non-military issues such as mass migration, environmental degradation, economic issues, famine, organised crime, as issues of security; and the "deepening" of security emphasised also on the security of multiple actors as referent objects rather than the state only (Krause & Williams, 1996: 230). Arguments in these developments were that the old concept of security was too narrow and, therefore, required to be broadened and deepened in order to cover contemporary and non-military security concerns (Krause & Williams, 1996: 229; Smith, 1999: 77; Ullman, 1983: 129). As a result, influential new approaches to security such as human security and environmental security emerged.

Thus, as the concept of security was redefined, so was national security. It was no longer simply about militarily defending the nation and the state against external threats. Rather, issues such as global mass migration, environmental degradation, transnational organised crime and terrorism, came to be acknowledged as national security threats of the 21st century. For example, the 2001 September 11 (9/11) terrorist attacks at the heart of the US' economy and its military headquarters sent shockwaves across the world. It demonstrated that a non-state actor can inflict catastrophic destruction even on 'the world's most powerful state', therefore, terrorism was now a major national security threat. Nevertheless, despite the "new thinking" and the rise of significant non-state actors, the sovereign state remained the only actor with the capacity to provide security for its nation and enable the nation to pursue its core interests. No other actor can provide security for citizens of a certain state without its permission. Therefore, the state ultimately remained the central referent object in world politics, and across mainstream and 'new' theoretical approaches in IR and security studies.

As a result, the concept of national security even in the post-Cold War era remains fundamentally state-centric. This is a point made by Buzan (2009, as cited by Fjäder, 2014: 117) in that, "regardless of the perceived diminishing role of the state in international relations, the state remains the chief provider of security because it is the only societal structure having both the authority to define what represents a security threat as well as the power to act".

Krause (2009, as cited by Fjäder, 2014: 117) argues that the securitisation of traditionally non-security issues has in fact led to the expansion of the role of the state. In this way, the state manages to retain its privilege in regulating the area of security. Securitisation theory has had a significant impact on the meaning of national security. While being part of the 'new thinking' that contributed to the redefinition of security, the securitisation framework has in fact highlighted the hegemony of the state in global politics. Securitisation depends on the capabilities of the securitising actor to construct a threat. For example, climate change may be declared as a critical threat to the world by international organisations. However, it is only the states, if they agree, that have the power to securitise environmental issues in their own territories. Therefore, national security is still fundamentally about the preservation of a nation-state and its core interests. As Goldman (2001:43) noted, "There tends to be little dispute over the nature of core national interests: physical security, economic prosperity, and preservation of national values, institutions, and political autonomy". In other words, the main objective is securing the territory in which the nation can exist and pursue its vital goals.

As the meaning of national security has been clarified, the following section will discuss the meaning of civil liberties.

2.3. DEFINING CIVIL LIBERTIES

Before attempting to define the concept of civil liberty, it is necessary to briefly clarify the meaning of liberty. The term liberty is derived from the Latin word *libertas*, a derivative of *liber*, which means ‘free’ (Encyclopædia Britannica. 2017). Thus, liberty indicates the idea of freedom or "a state of being free". In fact, it is not uncommon to come across people using the terms ‘freedom’ and ‘liberty’ interchangeably in daily discussions. According to the Human Rights Dictionary (as cited by Cartwright & Condé, 2000 : 145), liberty is "The quality or state of being free; the power to do as one pleases; the positive enjoyment of various social, political, or economic rights or privileges; freedom from arbitrary or despotic control; and freedom to be subject to and follow the rule of law”. Therefore, liberty primarily refers to the freedom to rationally pursue one’s wishes within the confines of entrenched social values and restraints.

In political theory, contemporary arguments about liberty were influenced by Isaiah Berlin’s classical *Two Concepts of Liberty*, republished in 1969 in the book *Four Essays on Liberty*. Despite fierce criticism, Berlin's conception of liberty remained one of the most influential in political theory (Coser, 2014: 41). Berlin argued that liberty comprises a negative as well as a positive aspect. Accordingly, negative liberty refers to “the area within which the subject–a person or group of persons–is or should be left to do or be what he is able to do or be, without interference by other persons” (Berlin, 1969: 122-123). In simple terms, negative liberty is the freedom from unjustified interference, coercion, or restraint. For Berlin, positive liberty is used to determine “the source of control or interference that can determine someone to do, or be, one thing rather than another” (Berlin, 1969: 131-134). Put simply, positive liberty means self-determination, that is, freedom to act or do according to one’s will, as opposed to freedom from some interference.

2.3.1. Natural liberty

Classical writers such as William Blackstone, John Locke, Thomas Hobbes, Jean-Jacques Rousseau, among others, conceptualised liberty with their point of departure as ‘natural liberty’– the natural freedoms enjoyed by humans in a state of nature. Natural liberty was understood as the power to act as one thinks fit, without any constraint or control, unless by the law of nature (Blackstone, [1803] 1969: 125; Hobbes, 1651:129; Locke, 1690b: 4). According to Locke (1690a: 222), it is the “power to think or not to think, to move or not to move, according to the preference or direction of one’s own mind”. In this way, the classical definition captures both the positive (a power to act) and negative (without any restraint) aspects pointed out by Berlin. Natural liberty therefore is not simply the absence of restraints, but ‘a state of ability’– the ability to act according to how one sees fit.

The negative dimension of natural liberty– the power to act without any restraint–was a major focus for classical thinkers as it represents “a state of perfect freedom… within the bounds of the law of nature” (Locke: 1690b: 4). The law of nature was understood as “a general rule that is discovered through reason, which affirms human self-preservation and condemns acts destructive to human life” (Hobbes, 1651: 88). However, the law of nature comprised no effective means to forbid individuals from violating the natural liberties and rights of others; it is subject to the individual’s ability to restrain themselves or physical inability to act in a certain manner rather than a matter of external constraint. Thus, Hobbes (1651:78) contended that the state of nature “is worst of all, continuall feare, and danger of violent death; and the life of man, solitary, poore, nasty, bruitish, and short”. In this way, natural liberty means that the only thing restraining the individual to do whatever they wish is their will or physical inability. Most classical writers tended to agree that such unrestrained freedom was a recipe for potential mayhem and brutality in human life (Heyman, 1992: 84). When liberty is understood as the absence of any restraint against the individual’s wishes, not only does it become a licence but it is also irrational, as what is liberty for one individual could effectively be a restraint for another (Blackstone, [1803] 1969:125).

Thus, though liberty is a prerequisite for human progress, it cannot be unconditional. It has to be subjected to reason and particular conditions, as unrestrained liberty effectively becomes ‘survival of the fittest’, and thus a breeding ground for anarchy and savagery. Consequently, a convergent perspective among early thinkers was that "Liberty is to be free from restraint and violence from others which cannot be where there is no Law"; because, "where there is no Law, there is no Freedom” (Locke, 1690b: 25).

2.3.2. Civil Liberty

Realising that unrestrained liberty is a formula for chaos and potential barbarism, individuals therefore enter into political societies in order to have security and liberty within the confines of the society's established laws, and to gain the additional benefits of a mutual existence. In this way, they compromise a certain degree of their natural liberty, but as a collective, they attain something more important: civil liberty– the liberty that is due to every individual member of the society.

In this context, civil liberty can be referred to as the right to act and pursue one's own goals and objectives according to how one thinks fit within the confines of authorised social restraints. It is the right for one's conduct within a society to be subjected only to laws and not to be arbitrarily violated in any way, whether by the law itself or other entities (Skaaning, 2006: 04). Depending on the political system, civil liberties are freedoms of individuals in their capacity as members of a society. They are liberties which individuals could not effectively secure and exercise in a state of nature. Lowi & Ginsberg (2000: 75) defined civil liberties as "Protections of citizens from improper government action". Cartwright & Condé (2000: 26) defined them as, "legal guarantees established by the governed of a democratic society and are assurances that the basic freedom of the individual will not be curtailed or reduced by the government". Such freedoms, as classical thinkers had already contended, include "the right not to be arrested, detained, put to death or maltreated in any way; and the right of everyone to: express their opinion, choose their profession, dispose of property, come and go without permission, to associate with other individuals and to process the religion which they prefer. Finally, it also included the exercise of some influence on the administration of government" (Constant, [1816]1988: 311). The latter statement points to the right of citizens to investigate or criticise the actions of the government, which has to do with access to information and freedom of expression.

While most explanations of civil liberties seem to focus on freedom from external restraints, particularly from the state, civil liberties of an individual can also be violated by non-state actors, such as other individuals, groups or organisations. Thus, the conception of civil liberties also encompasses the protection of one's basic liberties from arbitrary interference by such actors. To this degree, Heyman (1992) distinguished between the private and public dimensions of civil liberty. Accordingly, the private dimension is about “the individual's freedom in relation to other individuals in society”, while “the individual's liberty in relation to the state constitutes public civil liberty” (Heyman, 1992: 84-85). The private dimension requires that the protection of civil liberties of an individual be enforced by the state, and thus becomes a less complicated process as the state acts as the adjudicator between conflicting non-state actors. As Blackstone ([1803] 1969: 251) argued, "the law, which restrains a man from doing mischief to his fellow-citizens, though it diminishes the natural, increases the civil liberty of mankind". On the other hand, when individuals’ freedoms are threatened by the state itself– the public dimension– it becomes a complex process which requires the interpretation of law such that the state has to act against itself. From this perspective, "civil liberty, rightly understood, consists in protecting the rights of individuals by the united force of society” (Blackstone, [1803] 1969: 251), not just by the state.

Another important element is *political liberty*, without which, civil liberties could not have been fully secured in modern societies. Heyman (994: 86) defines political liberty as “the power of the community to govern itself, and that of citizens to participate in self-government”. The community's power in this regard is subject to the law, which simultaneously wields and curtails state power in order to protect the “civil liberty of mankind" against unjustified encroachments from both the state and non-state actors. In simple terms, political liberty refers to the right of a sovereign nation to determine its own law on how to effectively protect the nation and the freedoms of individuals.

The aspect of protection in the conception of political and civil liberty sheds light in two ways. First, as unrestrained freedom is a formula for social mayhem, it is through the law that freedom can actually be accomplished. The element of protection forces an actor within the society to allow other actors to pursue their goals. Secondly, individuals are entitled to demand to be protected by society. In this way, civil liberty refers to enjoying one's freedom within the framework of the law, while considering and allowing other individuals to realise theirs as well. The state can interfere in the affairs of citizens only in cases in which activities of individuals threaten a common interest, and the state acts only to protect that interest. This way of thinking highlight the point that civil liberties, unlike fundamental human rights, are not absolute or unconditional, but are dependent upon terms and conditions instituted for the well-being of the entire society. However, such terms and conditions are never permanent or fixed, they always vary depending on the context and issues under which the society grapples with, particularly issues of security.

Lastly, it is important to note that liberty is a fundamental term and objective of both classic and modern political liberalism, which has championed concepts such as liberal and constitutional democracy, rule of law and justice. Thus, for civil liberties to be properly realised, freedom-loving societies have commonly followed the liberal-constitutional democratic path of government. Such a system of government has consisted of the following core characteristics: a constitutional and democratic form of government; constitutionally protected human rights and civil liberties; a separation of powers between the legislative, executive and judicial branches of government; the rule of law; and media freedom. Furthermore, in addition to a multiparty system of competition for political power, liberal democratic societies have entrenched the existence of organised and independent civil society groups to promote vigilance on the activities of the state.

As the meanings of both national security and civil liberties have been clarified, the next section will analyse the tension between the two concepts.

2.4. THE TENSION BETWEEN LIBERTY AND SECURITY

“Freedom for the wolves has often meant death to the sheep.” (Berlin, 1969: xlv)

The above quote highlights the predicament that frequently comes to play between the concepts of liberty and security. Liberty and security are essential concepts of human life, of which a society deprived any of them is effectively an oppressed one. However, the relationship between the two concepts throughout the history of political philosophy has often been conflictual, as the expansion of one is the potential weakening of the other. Thus, the issue has been how to frame the law in a way that would permit the two concepts to be mutually inclusive, rather than a zero-sum game.

Locke’s (1690b: 6) influential writings pointed out that, individuals in the state of nature have two natural rights: “the right to ensure their survival as well as the right to punish those who threaten their survival”. However, the state of nature is only governed by the unenforceable ‘law of nature’. Thus, while the state of nature is a ‘state of liberty’ and ‘not a state of license’ (Locke, 1690b: 6), it is too unstable for individuals to realise their goals and aspirations. Therefore, individuals abandoned the state of nature in favour of political societies specifically for ‘the mutual preservation of their lives, liberties, and estates” (Locke, 1690b: 11).

The interconnection between liberty and security was further delved into by other philosophers of the enlightenment era and afterwards, including Rousseau. Though Rousseau remarked that ‘man is born free, and everywhere he is in chains’ (Gourevitch, 1997: 41), he was actually advocating for a civil government framed around the interests of its citizens, rather than an anarchic state of nature. For Rousseau, the government was to have exclusive monopoly on the legitimate use of violence in order to restore order and security. However, such power must be controlled by the citizenry and not be under the sole discretion of the ruling elite (Gourevitch, 1997: 41), lest the saying that “power corrupts, and absolute power corrupts absolutely” may come to materialise.

In this way, liberty has thus been perceived as an important factor for stability and security in societies, and a legitimising factor for governments. History has proven that most states that have severely oppressed the liberties of their people have typically come down crashing as people tend to rebel against despotic rulers. Nevertheless, it has also been recognised that, for individuals to fully realise liberty and personal security, a certain degree of liberty itself is bound to be compromised, and allow a partial government to interpret and enforce the law. Such a government must, however, be accountable to the people themselves, not the rulers (Constant, [1816]1988: 311; Locke, 1690b: 65; Gourevitch, 1997: 41).

Thus, despite the high emphasis on liberty and human rights, liberal constitutional democracies, which came to be seen as the ideal system of government in contemporary world politics, upheld the view recognised by both realists and liberals that the state has to have exclusive right to use force in order to maintain security and the rule of law (Michaelsen, 2006: 4). Though government power in this regard is limited by constitutional terms that forbids an undue burden on citizens, the dispute has always been on how much state power must be permitted or limited, and to what degree are civil liberties to be curtailed in order to ensure a satisfactory framework for government power and civil life. As Ullman (1983:130) noted that, “what should we be willing to give up in order to obtain more security? How do we assess the trade-offs between security and other values? The question is apposite because, of all the "goods" a state can provide, none is more fundamental than security”. Such a caveat was pointed out earlier by Locke (1690b: 66) in his observation:

> *“for since... the lawmaking power... is usually too numerous and too slow for the dispatch requisite to execution; and because it is impossible to foresee, and so by laws to provide for all accidents and necessities… therefore there is a latitude left to the executive power, to do many things of choice which the laws do not prescribe”.*

National security is therefore primarily about the protection of the core interests of the nation-state, particularly the preservation of territorial and sovereign integrity of the nation-state in order to secure the lives of citizens and their core political and cultural interests. Consequently, national security, whichever way it is looked at, is essentially about survival. It can hardly be contested that security is fundamentally about life and death, or at least a sensible existence, and, therefore, that the conditions of life depend on the presence of life itself. As a result, liberty and democracy as conditions of life are consequential and derivative as they depend on the existence of life. This is exactly why individuals had to abandon the lawless state of nature, because the perpetual potential for barbarism to ensue meant that no individual was actually safe or free from arbitrary interference or coercion. In this way, protecting the primary national interest of the state, which is preserving the nation-state, permit members of society to enjoy and exercise their core political and cultural interests, such as liberty and the pursuit of happiness. Failure to preserve the nation-state or let it be debilitated would deprive citizens of both their security and liberty.

Therefore, a certain degree of freedom is compromised by belonging to a political society, though a fixed or permanent level of this comprise can never be reached. Moreover, a further degree of civil freedom is sacrificed when an existential threat to the nation becomes identifiable, particularly in the instance that the nation will be destroyed or suffer immensely if the threat is not attended to. An obvious example would be if another state or group make attempts to overthrow the government of South Africa. In such a case, it will be an identifiable national security crisis in which securitisation will ensue and civil liberties will significantly be curtailed in order to swiftly deal with the security crisis.

Warshawsky (2013: 95) details the US's history of sacrificing civil liberties in favour of national security: From President John Adams' use of "the potential threat of a war with France" in 1798; throughout the First and Second World Wars in which stringent measures were put in place to monitor information flows, such as the Espionage Act of 1917; the Cold War 'red scares' that led to the US government basically spying on its own citizens; to the aftermath of the 9/11 terrorist attacks that brought the 'War on Terror'. The US, according to Warshawsky, is not the only constitutional democratic state that has a history of restricting civil liberties in the name of national security. Others such as Britain, France, and Australia, particularly in the aftermath of 9/11, have followed suit.

The tension between national security and civil liberties in the 21st century has risen to significantly higher proportions as borders between states seem to fade away and actors on the international stage proliferate as a result of technological advancements and mass migration. It is thus important to consider that these developments significantly influence the underlying forces between national security and civil liberties, particularly the rise of violent international terrorism that aims to perpetrate mass killings and cause international panic. A significant factor here is also the rise of Internet usage in which 'the web' has become a crucial tool for terrorists for communication and executing their plans as well as recruiting members to their networks and spreading their propaganda and fear throughout the world. Hence, it is plausible that technologically capable terrorists may seek to use the Internet for not merely just communication, but for more serious issues such as hacking and sabotaging CNII of states.

Thus, as Warshawsky (2013: 95) notes, "a significant attention has led to a re-evaluation of security measures, and it seems that in order to address the changing shape of the threat, a more intrusive approach may be needed". This has become a common national security approach for almost all states, even liberal-constitutional democracies, as they deal with evolving challenges such as terrorism and pervasive Internet connectivity. It all comes down to the preservation of the state, and then all else will follow, which has unavoidably resulted in the encroachment on some civil liberties. In this way, national security and civil liberties are fundamental concepts that constitutional democracies hold dear, but security prevails above everything else.

2.6. CONCLUSION

This chapter analysed the meanings of national security and civil liberties and explored the relationship between these concepts. The concept of national security evolved overtime as the traditional, state-centric conception was perceived to be obsolete to make sense of contemporary issues of security. However, even with ‘the new security’, the state-centrism of the traditional security persisted within the redefinition of security as the state remains the primary actor as both the referent object and the provider of security. As a result, national security remains the sole responsibility as well as the main objective of the state.

Civil liberty is a liberal democratic concept that emerged with the recognition that unrestrained liberty was in fact detrimental to security. Therefore, individuals had more chances of realising their liberty and security in political societies consisting of a government authorised with the power to use force in order to safeguard the common interest. Meaning that liberty became regulated and subject to terms and conditions that depend on variable contexts and issues that can influence the common interest, particularly issues that threaten national security. Civil liberties and national security are therefore mutually inclusive and inseparable. It is only through preserving the existence of the nation-state that its citizens will be able to realise their liberties.

CHAPTER 3: CYBERSPACE AND ITS IMPACT ON NATIONAL SECURITY AND CIVIL LIBERTIES

3.1. INTRODUCTION

This chapter analyses the concept of cyberspace and how it has impacted on socio-political relations and security. Firstly, the chapter will examine the meaning of cyberspace, a term often used interchangeably with the 'Internet'. The second section will explain the impact of cyberspace on modern societies. This will include an analysis of the rise of security issues such as cybercrime, cyberterrorism, cyberespionage and cyberwarfare. Thirdly, the chapter will examine how cybersecurity consequently became a national security priority across the world. The fourth section will then explore the impact of cybersecurity on the debate concerning the tension between national security and civil liberties.

The aim is to trace the evolution of cyberspace; to probe the security threats that has accompanied its benefits; and, in recognition that it has come to be an indispensable component of the modern economy and social practices, to understand its rightful place in the democratic political dispensation in which security and liberty cannot be treated as mutually exclusive concepts. In conclusion, the argument advanced in this chapter is that cyberspace has indeed added new dynamics to civil liberties as well as in national security and, therefore, adjustments between the concepts of national security and civil liberties are unavoidable.

3.2. EXPLAINING CYBERSPACE

The concept of cyberspace lacks a shared and comprehensive definition at the academic level, and different governments and organisations use different definitions (Mayer *et al*, 2013:07; Ottis & Lorents, 2010: 02). According to Kramer *et al* (2009: 1), the term cyberspace contains at least 28 different definitions. The United Nations' (UN) International Telecommunication Union (ITU) defines cyberspace as "systems and services connected either directly or indirectly to the Internet, telecommunications and computer networks" (ITU, 2011: 5). The International Organisation for Standardization

(ISO)[1] and the International Electrotechnical Commission (IEC) explain the term as "a complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form" (ISO/IEC 27032: 2012). While Kuehl (2009: 29) explained it as “a domain characterised by the use of electronics and the electromagnetic spectrum to store, modify and exchange information via networked information systems and physical infrastructures”. Mayer *et al* (2014: 01) recently attempted to provide a more comprehensive definition, elaborating that cyberspace is “a global and dynamic domain (subject to constant change) characterised by the combined use of electrons and electromagnetic spectrum, whose purpose is to create, store, modify, exchange, share and extract, use, eliminate information and disrupt physical resources”. In this way, cyberspace can be defined as “the virtual space – including the Internet, and other computer-communications infrastructure – that is entirely composed of computers, algorithms, computer networks, and data” (Kenney, 2015: 112).

The term “cyberspace” was first used in the 1960s in the visual arts under the moniker *Atelier Cyberspace* by Susanne Ussing and Carsten Hoff (Lillemose & Kryger, 2015). Under this term, Ussing and Hoff came up with a series of depictions which they called “sensory spaces”, which had little to do with computers or technology. Their aim was to create virtual mediations between machines and people that can have physical effects and could help to close space (Lillemose & Kryger, 2015). Atelier Cyberspace was conceptualised before the existence of the Internet and when computers were predominantly inaccessible to the masses. The term cyberspace was popularised in the 1980s by fiction novelist, William Gibson. Gibson (1984: 67) defined cyberspace as “a consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts... A graphic representation of data abstracted from the banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the nonspace of the mind, clusters and constellations of data. Like city lights, receding”. In 1991, Sir Tim Berners-Lee’s invention– the World Wide Web (www)– went live to the world and became

[1] The organisation is called the International Organization for Standardization but it is abbreviated ISO.

accessible to the public, and the word cyberspace came to be primarily associated with online or Internet activities ever since.

While cyberspace is commonly used interchangeably with the Internet, the term refers to entities and activities that exist mainly within the communication system itself, in such a way that a website or a blog, for instance, exist in cyberspace. From this perspective, activities occurring on the Internet are not taking place in the physical sites of participants or web servers, but in cyberspace (Mayer et al, 2014: 01-02). The domain of cyberspace also comprises outside Internet systems such as, radio, intranet, various telecommunication networks, fixed and mobile phones, and satellite communication systems. Thus, it is unsurprising that cybercriminals, such as the phone ‘phreakers’ of the 1950s and 60s in the United States (US), existed prior to the existence of the Internet, as the concept of cyberspace is more expansive than that of the Internet (Hoscheidt & Eichner, 2014: 447).

Today, cyberspace support a range of other internet applications such as smartphone mobile apps (WhatsApp and snapchat, for example), PlayStation games and navigation systems. The world is now also witnessing the phenomenon of the so-called Internet of Things (IoT) – a concept that “refers to the use of intelligently connected devices and systems to leverage data gathered by embedded sensors and actuators in machines and other physical objects” (GSMA, 2014: 1). Other than the typical computers and smartphones, IoT connected devices include cars, home appliances and wearable devices such as watches and heart monitors. Mohammed & Ahmed (2017: 126), note that “IoT-enabled things will share information about the condition of things and the surrounding environment with people, software systems and other machines”. The IoT is expected to spread rapidly in the foreseeable future, “with IoT-enabled devices reaching more than 24 billion on Earth by 2020, about four devices for every person on earth connected to cyberspace” (Business Insider Intelligence, 2016). The IoT will provide the means for devices to communicate amongst each other with various information and effect ‘smart action’ through artificial intelligence (Mohammed & Ahmed, 2017: 128; Jaffe, 2014). It is projected that this will create the means for ‘smart cities’ with intelligent energy grids, transportation systems, waste management and monitoring systems; smart healthcare systems, and smart homes that effectively utilise energy and water (Jaffe, 2014; Business Insider Intelligence, 2016; Mohammed & Ahmed, 2017: 128).

Similar to the anarchic international system in the real world, a crucial feature of cyberspace is that it lacks a central authoritative body to enforce law and order (Mayer *et al*, 2014: 9). The lack of enforcement though does not mean that cyberspace lacks the aspect of power, nor that power is distributed and spread evenly across numerous unknown channels, individuals, groups or governments. Participants in cyberspace operate in completely different contexts and have significantly different capacities and means of power. Whereas in the real world power can be measured or observed at least to a certain extent, the same cannot be said with the hierarchies of power in cyberspace. States in economically weaker positions, such as North Korea, have demonstrated some of the most sophisticated cyber capabilities that have influenced the actions of the world's leading superpowers. For example, North Korean hackers are said to have only been stopped by a spelling mistake from stealing $1 billion from the New York Federal Reserve in 2016, while the global "Wanna cry" ransomware that briefly crippled Britain's National Health Service in 2016 was also traced to North Korea (Naughton, 2017; Sanger, Kirkpatrick & Perlroth, 2017).

The following section will provide an analysis of how cyberspace has impacted on the socio-political and economic life of modern societies.

3.3. THE INFLUENCE OF CYBERSPCAE ON MODERN SOCIETIES

3.3.1. The socio-political and economic influence of cyberspace

Particularly due to the Internet, cyberspace has literally connected individuals and nations across the world through more than two billion users in approximately 200 countries. In 1996 the first survey of Internet users counted about 40 million users; by 2015, that number had risen to 3.4 billion and continues to rise (ITU, 2015). The cyber domain has established a permanent base in the structures of academic institutions, businesses, and government sectors in numerous countries; connecting individuals, influential academics, business leaders, political leaders, governments, organisations and different groups across borders, all with different agendas. As a result, modern life has become easier and more convenient due the communication, information sharing, research and innovative capabilities made available by cyber technology. It has become easier to communicate with anyone in any part of the world at any time without having to leave one’s room, as long as the sender and receiver of information both have access to the Internet.

With the advent of the World Wide Web and electronic mail (email), cyberspace has enabled people to communicate with as little time and effort as possible. It is now incomprehensible for any organisation, business, government and even many individuals in modern societies to function without email. The convenience of e-mail has allowed organisations and multinational corporations to cost-effectively broaden and connect with their stakeholders in different parts of the world. Social media platforms such as Facebook and Twitter and video calling applications such as Skype are some of the latest innovations added to the cyber domain which have enabled real time communication, anywhere, any time. Such instantaneous and live communication capabilities has enabled people in different parts of the world to form friendships wherein thoughts and foreign cultures are explored.

Thus, not only has cyberspace been a great leap in human progress in terms of communication and information dissemination, but it has also provided everyone with the platform and opportunity to explore their business, learning and artistic capabilities – to venture into the unknown and test their limits. This has resulted in the domain of cyberspace becoming a constantly evolving arena that seem to provide new opportunities and abilities on a daily basis, as different people from different parts of the world seek opportunities and come up with various ideas to contribute to making life easier for Internet users.

As information or knowledge is a vital component of modern societies, cyberspace has become a virtual treasure trove of information. Whether you seek information on trivial topics such as cooking lessons, home renovations, to more challenging endeavours such as starting a business, academic research, to the darker side of life such as how to commit suicide or the perfect murder or any topic one can think of; it is all available on the Internet. Internet search engines such as Google and video applications such as YouTube have made it possible for anyone to upload information on the Internet such that anyone can find information on almost any topic available in the world. As a result, cyberspace has now become more pervasive than television and radio. It has become an industry on its own that has created powerful multinational corporations, millions of jobs and business opportunities, and influential billionaires such as Larry

Page and Mark Zuckerberg. Internet access has provided instant access to an unlimited and constantly evolving supply of information and numerous opportunities. Access to the Internet has even been declared as a fundamental human right by the United Nations Human Rights Commission (Alexander & Shore, 2016; UNHRC, 2016).

Perhaps the most powerful manifestation of the cyber information revolution is how it has transformed socio-political relations in today's world. Today's information is no longer disseminated exclusively from a small ruling elite to the masses, and with little to no interactivity. Information is now also transmitted globally from within the masses to the masses themselves, multichannel and with high interactivity. By removing the elites and large corporations on the control of the flow of information, horizontal information sharing systems have been established which have added a new dimension on social and political practices.

In autocratic regimes, cyberspace has presented new challenges to the authorities which have often manifested in enthusiastic, mobilised resistance movements that have resulted in social and political uprisings. One of the most profound examples of the influence of Internet communication in the 21st century is the events that came be known as the 'Arab Springs' or Arab Revolutions that began in 2009. It was through the use of social media that people in Tunisia, Egypt, Libya and other Arab states communicated and mobilised popular uprisings that saw the toppling of some of the oldest dictatorships in the world and the brutal killing of Muamar Gadhafi. Consequently, the freedom to communicate with anyone and potentially influence the thoughts and actions of others became a powerful weapon at the disposal of relatively powerless masses. In this way, "online and particularly wireless communication has helped social movements pose more of a challenge to state power" (Castells, 2014).

However, as the popularity of cyberspace grew, another side of it has also been increasingly influencing social, business and political relations across states. This will be explained in the following section.

3.3.1. The rise of cyber threats

a) Cybercrime

The term "cybercrime" also lacks a single definition and has been used to refer to a range of offences that include conventional computer crimes, as well as network crimes (ITU, 2012: 11). As a result of the variety of such crimes, it has been difficult to construct a single criterion that encompasses all acts listed in different international and regional legal approaches dealing with the phenomena of cybercrime, whilst excluding conventional computer crimes perpetrated only through the use of hardware, such as forging documents (ITU, 2012: 11). McQuade (2011: 2) notes that cybercrime is "a broad construct for many emerging sorts of abuse and crime enabled by ICT. While Hoscheidt & Eichner (2014: 454) point out that the definition of cybercrime remains a national sovereign decision and "a field of international cooperation". As a result, for purposes of this study, cybercrime will be defined here as any illegal activity committed by means of, or in relation to, EIS for self-gain or simply inflicting harm on the holder of the information. It is important to note that this definition excludes illegal actions that are intended for political objectives, as such could cover acts of terrorism and espionage.

Cybercrime developed over significantly longer periods of time to become the security issue that it is today. The first digital computers such as the Electronic Numerical Integrator and Computer (ENIAC), Binary Automatic Computer (BINAC) and the Universal Automatic Computer (UNIVAC) and other related machinery were less prone to security breaches (Shinder 2002: 51). These devices were standalone systems, gigantic and extremely costly for the average person, and only those in the science community had knowledge about computers. As Shinder (2002: 50) noted, "working with early systems required the ability to communicate in the 1s and 0s of binary calculation that computers understood, and it was a privilege of few". The opportunities for cybercrime became available with the introduction of the Programmed Data Processor (PDP-1) in the 1960s, which was rented out to organisations and individuals. As the machine became used by different individuals for different purposes, programs and data stored in it became vulnerable to manipulation, and thus the first possibilities for security breaches became apparent (Hoscheidt & Eichner, 2014: 454).

Cybercrime rapidly grew as the use of computers became popular, easier and more affordable. When the idea of moving data from one computer to another through computer networks was finally realised in the 1970s, data stored in computers also became more vulnerable, and it did not take long for some people to start exploring ways to exploit it for their own selfish gains (Shinder 2002, 54). The first hackers came out of the Massachusetts Institute of Technology (MIT) in the 1960s sometime after the Institute received its own PDP-1 (Pitts, 2017: 4; Hoscheidt & Eichner, 2014: 447). At first, hacking during this period was associated with intellect and was used for purposes of exploring and enjoyment. Hacking became associated with malicious activity when the “radical yippies” and “phone phreakers” in the 1970s began exploiting cyberspace for selfish motives (Shinder, 2002: 52; Pitts, 2017: 4). The availability of personal computers afforded the average person with the opportunity to purchase their own computer and, in their own private spaces, learn computer programming and other skills associated with computing. As the popularity of computers accelerated and the wider public increasingly gained access to them, the need to further develop the capacity of computer processors and to simplify the sharing of different databases led to the development of a broader network of computers (Shinder, 2002: 54), attracting more inquisitive minds and opening up space for further manipulation of digital information.

The 1980s saw the first major wave of cybercrime as the use of email grew faster and more people were attracted to its convenience (Castells, 2014). Email permitted the ability to distribute computer malwares and phishing scams to millions of people, companies and governments in their inboxes. It was during this period that the first cybercriminal, Ian Murphy, was arrested and convicted in 1981 for a cybercrime of hacking into the American Telephone and Telegraph Company (AT&T) network and manipulating the company’s internal clock system for his own personal gains (Hoscheidt & Eichner, 2014: 450). Nevertheless, security was not a major concern at the time as scientists and computer engineers were more fascinated by what digital information and computer networks could do than protecting them.

The first case of a major security threat that caught the attention of computer scientists and law makers was in 1988 when the self-replicating ‘Morris worm’– developed by Robert Morris Jr., a graduate student at Cornell University– was released into the US government’s computer network (Hoscheidt & Eichner, 2014: 450; LeVPN, 2017). The worm became uncontrollable and quickly spread and infected thousands of computers throughout the United States, and eventually led to a shutdown of a large portion of the Internet. By 1990, the first large-scale case of ‘ransomware’ was reported, in which a malware was used to infect computers in the health industry and held computer data hostage for $500 (LeVPN, 2017). With the advancement of web browsers, malwares and viruses that started appearing in the 1990s became more vicious and increasingly threatening. Cybercriminals began exploring the idea of stealing business secrets stored on companies' computer mainframes and confidential information of individuals, such as banking details and passwords.

A cybercrime incident that greatly raised the stakes was the release of the "Melissa worm" in 1999, by computer programmer, David Smith, using a hacked America Online (AOL) account with the intention of taking over email accounts and sending out mass-mailings promising Internet users access to porn websites (Hoscheidt & Eichner, 2014: 450). Within hours, the virus had spread far and wide through email, replicating itself and infecting thousands of computers belonging to individuals, businesses and government agencies across the world (LeVPN, 2017). While the Melissa worm did not devastate the Internet, it received a great deal of media attention and was a security wake-up call for businesses and governments. Since then, several large corporations and organisations, such as Microsoft, Amazon, The New York Times and UNICEF, had suffered cyber-attacks by criminals seeking to steal valuable data and funds.

The 2000s witnessed large-scale cybercrime cases such as the release of the 'ILOVEYOU' virus, 'Code Red' virus, 'SQL Slammer' and countless others that infected hundreds of millions of computers across the world and caused massive monetary damages in recovery and removing these viruses (LeVPN, 2017. With the advent of social media, there has been a surge of people putting some of their most personal details on profile databases, thereby creating a pool of personal information of millions of people online for cybercriminals to exploit. Powerful multinational corporations such as Sony, JP Morgan Chase (the largest bank in the US), Yahoo! and eBay have recently fallen victims to large-scale hacks that have seen customers' most confidential details being infiltrated by cybercriminals, resulting in billions of dollars in monetary losses for both companies and customers (Armerding, 2017).

The latest trend of cybercrime is increasingly becoming an organised and globalised criminal industry estimated to be in the hundreds of billions of dollars annually (LeVPN, 2017; Morag, 2014: 5). Organised cybercriminal rings are now using highly sophisticated equipment and methods targeting any entity with a presence on the Internet, whether its individuals, governments or businesses. According to a report by the United Nations Office on Drugs and Crime (UNODC, 2013: 39- 42), around 80%

of major cybercrimes in the 21st century are perpetrated by sophisticated criminal syndicates engaging in extremely organised operations. In fact, these syndicates have established operations that resemble normal organisations and businesses in that they maintain a hierarchical organisational structure and a consistent work schedule to coordinate and execute their attacks. Such developments have further complicated efforts to come to a common definition of cybercrime as such organised syndicates and states such as China and Russia have allegedly been colluding or sponsoring criminal groups to sabotage and steal business and government secrets from foreign companies and other states (Banks, 2017: 515-516).

Thus, the distinction between cybercrime and other concepts such as cyberterrorism, cyberespionage and cyberwarfare has often been blurred.

b) Cyberterrorism

The meaning of “cyber-terrorism” has become fairly clear in security discourse during the 21st century as cybersecurity and terrorism developed to become ubiquitous concepts. Cyberterrorism is commonly understood to refer to the use of computers and computer networks for terrorist purposes, typically marked by political or ideological motivations (Heickerö, 2014; Weimann, 2005: 130). Unlike cybercrime, cyberterrorism is fundamentally intended to cause mass destruction and deaths in order to make purposive political or ideological statements.

Due to the inherent benefit of anonymity that comes with cyberspace, cyberterrorism is arguably an appealing alternative for contemporary terrorists. It also contains the potential to inflict large-scale destruction and mass hysteria. The threat posed by cyberterrorism has been a sensational subject that have caught the attention of the ICT industry, security experts, mainstream media and the modern society at large. As Weimann (2005: 130) noted, influential news agencies such as CNN and BBC, politicians, and analysts in diverse fields have propagated a scenario in which sophisticated cyberterrorists hack into computer mainframes that control national energy grids, national defence systems, air traffic control systems or dams, thereby manipulating or crashing these systems in such a way that millions of lives and the security of the state itself would be at stake. Such a situation is arguably probable as cyberterrorists can be anyone motivated by the same political and ideological objectives of conventional terrorists but seeking anonymity to evade arrest and prosecution. As Heickerö (2014: 555) points out, “cyber terrorists are not suicide bombers, nor is media attention an end in itself; on the contrary, they usually try to hide what they are doing online as far as possible”.

As most CNII in modern societies have become essentially dependent upon EIS, the threat posed by cyberterrorism has become a national security concern for most states. Cybercriminals mainly motivated by speedy financial gains have demonstrated the ability to break into EIS and manipulate sensitive information of businesses, individuals, and governments. In the same logic, technologically capable terrorists can hack into the EIS of governments and businesses in ICT-dependent countries with the intention to destroy or incapacitate CNII such as military defence systems, transport systems, or financial systems. The more technologically advanced a country is, the more vulnerable its CNII is to cyberterrorism. To this degree, concerns about the threat posed by cyberterrorism are merited. However, some of the fears and scenarios popularised in the media and even in movies may be too exaggerated, but not impossible.

Banks (2017: 517) notes that terrorists groups such as the Islamic State (ISIS) have “demonstrated a sophisticated understanding of methods for shielding their communications from electronic surveillance by intelligence agencies”. This indicates the technological capabilities of terrorist organisations, and the likelihood that they could be planning to use cyberspace to orchestrate terror activities.

Such developments have led to a divergence of cybersecurity legal frameworks among different states, with others, particularly non-democratic states, opting for stricter government control on communications networks and curtailing certain liberties and rights and blocking access to some Western websites. These has also led to a race in cyber-capability build-up among states competing for military superiority as allegations of cyberespionage and cyberwarfare have become widespread in current world affairs. The following section focuses on the issues of cyberespionage and cyberwarfare.

c) Cyberespionage and cyberwarfare

By 2000, cybersecurity had already evolved from simply being a technical discipline to a national strategic concept as cyberspace came to theoretically pose some of the most feared national security threats (Deibert & Rohozinski, 2010b: 16; Geers, 2011:

9). Kosenkov (2016: 1) pointed out that, “Cyberspace is the first fully artificial space (no matter within or outside of the information environment) which, alongside land, sea, air, and space is considered to be a domain pursued for military superiority”. ICT advancements have offered states the opportunity to innovate and utilise their capabilities to achieve their goals in much more powerful and previously unseen ways. On the other hand, the extremely interconnected nature of EIS has made protecting confidential information an exceedingly difficult task, while making it easier for data transfer and storage. Thus, using satellite technology and fast internet connectivity, a state or anyone with the technical know-how and the necessary resources can spy on another state thousands of kilometres away and even take pictures, or sabotage CNII and wreak costly and even deadly havoc. Such scenarios have brought forth the concepts of cyberespionage and cyberwarfare.

The manual published by the North Atlantic Treaty Organisation’s (NATO) Cooperative Cyber Defense Center of Excellence (CCDCE) in Tallinn, Estonia in 2013, defines cyberespionage as “an act undertaken clandestinely or under false pretenses that uses cyber capabilities to gather (or attempt to gather) information with the intention of communicating it to the opposing party” (Schmitt, 2013:193). In this way, cyberespionage refers to activities executed through EIS that are intended to gain access to sensitive information and secrets without the knowledge or consent of a rival information owner (individuals, corporations, states, and so on) in order to acquire a strategic advantage over them.

Just like traditional espionage, the main objective in cyberespionage is to acquire crucial information about the capabilities and intentions of rivals, or, in the case of industrial or economic espionage, to steal intellectual property or to gain access to proprietary trade secrets to understand a rival company’s business strategy (Morag, 2014: 3). A notable example is claims by Google in 2010 that China, in order to keep up with rival global technological advancements and domestic economic demands, stole source codes from Google to spy and infiltrate information systems of foreign companies (Banks, 2017: 514-515). In the same year, the Christian Science Monitor reported that persistent cyberespionage against big American oil companies such as Exxon Mobil and Marathon Oil had uncovered substantial amounts of detailed data about global oil discoveries, which rival companies could exploit. The theft was traced to a single site in China (Brenner, 2014: 2). Brenner (2014: 4) points out that the distinction between economic and other kinds of espionage for the Chinese and Russians is an ideological construction, convenient only to the West, as all forms of espionage are conducted in the name of the national interest.

While economic espionage have accelerated and may be a cause for concern in the Internet age, Brenner (2014: 1) indicates that states have in fact been conducting economic espionage against each other long before the internet came to exist, and will continue to seek more stealthier methods to do so. In this way, economic espionage does not pose such a critical security threat to the state. Rather, it is state to state cyberespionage that poses a greater threat to the nation, which sometimes blurs the distinction between cyberespionage and cyberwarfare as any information security breach in one state perpetrated by another can be regarded as cyberattacks or acts of war. The concept of cyberwarfare contains no widely accepted definition as yet (Robinson, Jones & Janicke, 2015: 12). However, it generally refers to activities conducted through EIS by one state against CNII of another state in order to cause harm or significant disruption (Andress & Winterfeld, 2011: 2; Liff, 2012: 403-404; Shakarian, Shakarian & Ruef, 2013: 2; Theohary & Rollins, 2015: 4).

State to state cyberespionage involves activities of one state coordinated through cyber systems to infiltrate or steal the state secrets of another. This can be sensitive information such as military secrets, public services information or national economic strategies. Several scholars have indicated that acts of cyber espionage are far more pervasive, and the leading nations that are conducting cyber espionage campaigns on a global scale are China, Russia and the US (Carr, 2010: 4; Rubenstein, 2014: 2; Theohary & Rollins, 2015: 4).

Providing clear definitions and distinctions between terms such as cybercrime, cyberespionage and cyberwarfare was not the main aim of this section. The aim has been to highlight the fact that EIS have become the cornerstone of today's economies, thereby, making it easier for actors with sinister motives to attack these systems and manipulate, steal or sabotage them, wreaking social and economic havoc and even threatening lives and national security. Such cyberattacks have occurred in several states including Brazil (2005 & 2007), Estonia (2007), Iran (2010), and Ukraine (2015) (Armerding, 2017; Brunst, 2010: 52; Chuipka, 2016: 39; Farwell & Rohozinski, 2011: 23; Gomez, 2016: 42; Kenney, 2015: 111). Kosenkov (2015: 7) argues that, "In the worst case scenario, the maximum application of cyber capabilities could supersede effects of all kinds of modern weapon, due to the potential impact on weapon systems and the strategic destructive influence on society".

It is therefore not surprising that cybersecurity has become a national security priority for most states in the 21st century, especially for states that continue to look to technological advancements and innovation to advance their national interests. The prioritisation of cybersecurity by states will be explored in the following section

3.4. CYBERSECURITY: THE SECURITISATION OF CYBERSPACE

As with other 'cyber' concepts, cybersecurity contains different definitions. Craigen, Diakun-Thibault & Purse (2014: 13-17) examined various existing definitions and proposed that "Cybersecurity is the organization and collection of resources, processes, and structures used to protect cyberspace and cyberspace-enabled systems from occurrences that misalign de jure from de facto property rights". The ITU defines cybersecurity as "the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets" (ITU, 2018). A similar definition is also provided by Schatz, Bashroush & Wall (2017: 66). Essentially, cybersecurity is about protecting the cyber-environment against intentional and unintentional malicious cyber activities. To varying degrees in terms of capabilities of states, cybersecurity at national levels has largely translated into securitisation of cyberspace.

Among its numerous features, the domain of cyberspace has added new dynamics to the age-old tensions between security and liberty. Advancements in ICTs have benefitted humanity in that the freedoms of individuals to communicate, associate and express themselves have been immensely expanded. However, as demonstrated in chapter two, the expansion of freedom usually sees the weakening of security. The development of cyberspace overtime also expanded the vulnerabilities of participants, while lowering the ability to detect and locate users with sinister intents. It has provided innovative means for criminals and terrorists to commit various crimes or attacks against individuals, corporations or states, which have resulted in serious data breaches and caused economic damages and potential national security threats.

Attempts by states to counter against such risks have ultimately resulted in a global trend of securitisation of the cyberspace domain (Deibert & Rohozinski, 2010b: 19). Securitisation efforts at a global scale against cyberspace can be traced to the 1990s American politics and mainstream media which frequently featured terms such as "electronic Pearl Harbors" and "weapons of mass disruption" (Nissenbaum, 2005:67). These conjured looming catastrophic attacks against the West waiting to be carried out through cyberspace (Bendrath 2003:50-3; Nissenbaum, 2005:67; Yould; 2003:84-8). The 9/11 terrorist attacks in the US further heightened these fears and spurred the attention given to EIS and security, as lawmakers and the ICT industry realised that the openness and convenience of cyberspace could easily become an effective tool for terrorist organisations seeking technological methods to commit mass destructions and killings in the highly cyber-dependent countries of the West.

NATO also played a major role in the global securitisation of cyberspace. In 2007, Estonia suffered substantial cyberattacks, allegedly by Russian agents, which resulted in a vast disruption of some of its key government and financial services. After assisting Estonia to contain the threat, NATO declared the protection of EIS as a key component of its mandate (Hansen & Nissenbaum, 2009: 1156). This move cemented cyberspace at a global level to be a national security priority of the world's developed nations. Thus, developing nations were bound to follow suit.

Some of the most prominent cyberattacks of the 21st century which have vindicated the securitisation trajectory include the "Stuxnet" cyber-sabotage of Iran's nuclear programme in 2010, and the recent cyberattacks against the US' democratic processes in 2016 and 2017. In the latter case, if true, it means that the election of the US' current president was effectively influenced by outside forces. These have demonstrated that rivals located anywhere in the world can infiltrate, manipulate and sabotage crucial EIS of a particular government or organisation without physically leaving their locations or sending any form of conventional weapon.

Deibert & Rohozinski (2010a: 49) argued that, the securitisation of cyberspace has been driven primarily by a "defensive" agenda—to protect against adverse intrusions on state secrets and CNII and to allow security forces to monitor and address cyber threats more effectively. Others argue that securitisation of cyberspace is necessary because EIS are riddled with security vulnerabilities that conducting a spectacular attack on CNII is relatively easy, making cyberwar inevitable (Liff, 2012: 402; McGraw, 2013:109-110).

As a result, global powers such as the US, China and Russia, have already established dedicated cyber-defence and even cyberwarfare command centres (Carr, 2010: 2-3; Deibert & Rohozinski, 2010a: 49; Geers, 2011: 12). Cyber-surveillance – mass or targeted surveillance, which include “monitoring, interception, collection, analysis, use, preservation and retention of, interference with, or access to information that includes, reflects, or arises from a person or community’s communications in the past, present or future” (Necessary & Proportionate, 2014: 04) – has also become a necessary national intelligence and strategic tool for most states (Lowe, 2016: 654). Cyber-surveillance can yield vital information with regard to cyber-activities that may threaten the state’s national security and other core interests.

Thus, as the concept of ‘security dilemma’ has demonstrated, these factors have necessitated other states to adjust their capabilities in order to counter against growing threats, or risk being left behind and vulnerable to various cyberattacks by criminals, terrorists and adversarial states. It is also important to highlight the fact that national cybersecurity measures are less costly as compared to traditional national security measures such as conventional weapons development and intelligence gathering. However, the consequences of neglecting cybersecurity could potentially be greater than the threat of conventional warfare as modern life continues to move towards the direction of fully-integrated and interdependent information systems across all sector of society.

On the other hand, the trend of securitisation of the cyber domain has also had an influence on the security-vs-liberty tension. This will be analysed in the following section.

3.5. CYBERSECURITY AND THE TENSION BETWEEN SECURITY AND LIBERTY

Throughout modern history, freedom of expression, movement, privacy and access to information have been crucial components in humanity’s efforts to build civilised societies. Such liberties are fundamental elements of the conception of human rights and freedom in general, which practically all democratic nation-states have translated into their constitutions. The ability of people to hold and communicate their thoughts, or to be precise, the freedom to do so, could essentially serve as a benchmark for human progress. While the difficult task of clarifying limitations of freedom for purposes of collective security and public order is an equally crucial and indispensable component of efforts to find acceptable security policies– a continuous struggle to find a balance between individual liberty and national security.

Although cyberspace in the 'Internet age' has not particularly altered this basic pattern of principles, it has fundamentally transformed its form. The Internet has propelled the abilities and freedoms of individuals to communicate and access information into a whole new dimension. It has seen the enlargement of communication coverages and dissemination of information that allow the flourishment of most of the behaviour and activities you can find in the real world– social, business, education, entertainment, crime, and so on. Cyberspace has also drastically altered conventional means of measuring quantity and weighing content quality and created uncertainties in many social practices.

The benefits and disadvantages of cyberspace have been discussed earlier. It is important to point out that cyberspace is a public platform but not similar to the physical realm wherein basic freedoms can all be exercised. For example, you cannot have the right or freedom of movement in cyberspace that can either be allowed or denied. Once you enter the cyberspace domain, you do so voluntarily and it is arguably similar to leaving your private space (home) and going into a public place wherein you meet people or do business and so on. A public place and a private home are two distinct spaces which cannot be treated equally by the law. Also, an individual in a public place is not entitled by law the same liberties and rights that his private home affords them. Therefore, the government has the duty to secure a public space to ensure the liberties and security of people in such a way that it cannot do so in the private homes of individuals.

From this perspective, cyberspace is a sort of public platform upon which the government has the responsibility to make efforts to ensure security, for voluntary participants to exercise their liberties with minimal security concerns. As mentioned in chapter two, for society to realise liberty, the domain in which they conduct activities – whether its land, sea, air or cyberspace– has to be secured first.

3.6. CONCLUSION

This chapter explained the concept of cyberspace, the positive and negative impact it has had on modern societies, and how it affected the tension between security and liberty. Cyberspace refers to the artificial global domain that enables activities through interconnected and interdependent EIS. Cyberspace has become a crucial component of contemporary human life. However, on the one hand, it has extended individual freedoms and created a horizontal, transnational information sharing network that has allowed the global masses to communicate among themselves; a development that has seen the fall of some repressive regimes and continues to be a threat to existing ones as people across borders influence each other's opinions and challenge political authority.

On the other hand, the rise of cyberspace has also seen a rise in malicious cyber activity. Criminals have taken advantage of the convenience and openness of cyberspace to break into EIS of businesses and governments to commit various crimes. States as well have apparently used cyberspace to spy, infiltrate and sabotage other states or colluded with groups to infiltrate other states and foreign businesses. Terrorist organisations with the necessary resources and technical skills can also exploit cyberspace to carry out their depraved objectives. As a result, cybersecurity has become a core feature of the national security and military strategic frameworks of most, if not all, states.

Furthermore, cyberspace is not similar to private homes in which individuals have the liberty to behave in ways they cannot do in public spaces. The domain of cyberspace is a public space that requires to be secured in order for individuals to exercise their freedoms and pursue their goals, and for organisations and governments to conduct their operations with minimal security fears. Ultimately, this means that in cyberspace certain liberties such as privacy cannot be accorded to individuals in the same way as in a private home.

CHAPTER 4: THE SECURITISATION OF CYBERSPACE IN SOUTH AFRICA

4.1. INTRODUCTION

The global development of cyberspace, its impact on modern societies, and how policymakers around the world have securitised cyberspace in attempts to counter the undesirable effects of cyberspace have been explained. In this chapter, these aspects will be critically analysed within the South African context. First, the meaning of national security and civil liberties in South Africa will be explained. Secondly, a historical development of cyberspace in South Africa will be outlined, tracing how the country eventually became part of the global 'information revolution'. Thirdly, an analysis of how the cyber-revolution impacted on South Africa will be provided. As in other cyber-influenced countries, the rise of cyberspace in South Africa carried positive socio-economic gains and negative developments with potentially destructive consequences. Fourthly, this chapter will explore attempts by the South African government to tackle cyber threats, which have faced criticisms for framing these policies within the securitisation paradigm and threatening civil liberties.

The question of whether cyberspace poses a real national security danger to the country will also be probed: are the threats wilfully sensationalised by the government in order to curtail civil liberties and impose despotic control over the masses, or are the threats real? Lastly, this chapter will outline an argument on how national cyber security measures can be reconciled with citizens' civil liberties. In conclusion, the argument advanced in this study is that cyberspace contains serious national security threats, and, therefore, securitisation of this domain is necessary. However, national security measures of such do not necessarily have to lead to harmful effects if appropriate checks and balances are put in place.

4.1. THE MEANING OF NATIONAL SECURITY AND CIVIL LIBERTIES IN SOUTH AFRICA

The 1994 transition to liberal democratic rule in South Africa saw the new political leadership of the country dismantling the traditional state-centric security paradigm adopted by the previous apartheid regime, which, at the expense of human rights of a black majority, was primarily designed to secure the interests of a white minority through the state. While the country was emerging from a gloomy past characterised by gross human rights violations, the rest of the world had also just survived the threat of a nuclear war that persisted throughout the Cold War and came to an end with the collapse of the Soviet Union in 1989. Throughout the Cold War, the national security paradigm followed by the two superpowers (US and Soviet Union), and which had a major influence on the national security of other major and middle powers around the world, was rooted in political realism. Thus, as the threat of war subsided and the new 'broadened and deepened' concept of security came to be the norm in post-Cold War global politics, the new South Africa led by human rights champion, Nelson Mandela, was arguably obligated to subscribe to the new security approach.

The 'new' security had in fact already been under development as a government policy approach prior to the African National Congress' (ANC) takeover of political power in 1994, particularly in the defence, police and intelligence areas (Seegers, 2010: 272). The ANC's commitment to a broadened concept of security was outlined in a document titled *Ready to govern: ANC policy guidelines for a democratic South Africa* (ANC, 1992) which was developed in its 1992 conference. According to the ANC:

> *"National and regional security should not be restricted to military, police and intelligence matters, but as having political, economic, social and environmental dimensions. Underdevelopment, poverty, lack of democratic participation and the abuse of human rights are regarded as grave threats to the security of people. Since they invariably give rise to conflict between individuals, communities and countries, they threaten the security of states as well [...] National security and personal security shall be sought primarily through efforts to meet the social, political, economic and cultural needs of the people"-(ANC, 1992)*

Subsequently, in the 1994 *White Paper on Intelligence*, a section entitled "Towards a new national security doctrine" cemented the new security in the government's broader security policy approach. It specified that the "mission of the South African intelligence community' includes: safeguarding the Constitution; upholding fundamental rights; promoting security, stability, co-operation and development in South and Southern Africa; achieving national prosperity and making a contribution to global human priorities; and contributing to South Africa's ability to face foreign threats and to compete internationally" (RSA, 1994). Subsequent security related policies and strategies came to maintain the broad security agenda (Seegers, 2010: 272).

The post-Cold war concept of security was ultimately reflected in South Africa's 1996 Constitution, which embedded the new security into the country's law. The Constitution pronounced four "principles that govern national security in the republic"; most notably, that "National security must reflect the resolve of South Africans, as individuals and as a nation, to live as equals, to live in peace and harmony, to be free from fear and want and to seek a better life"; and that "National security must be pursued in compliance with the law, including international law" (RSA, 1996: 198). Furthermore, the Constitution had also entrenched fundamental human rights through the Bill of Rights (chapter 2) as a "cornerstone of democracy in South Africa", which "enshrines the rights of all people in our country and affirms the democratic values of human dignity, equality and freedom" (RSA, 1996: 7).

The Bill of Rights explicitly pronounce "non-derogable" rights such as "the right to life, not to be tortured, not to be forced into slavery, human dignity, freedom and security of the person". Such rights are absolute and cannot be compromised under any circumstance. In this way, other rights and civil liberties such as privacy, freedom of expression/ association/ movement, among others, are thus subject to the possibility of derogation or partial suppression under exceptional circumstances, particularly, in cases of national security emergencies.

Therefore, individuals in South Africa are constitutionally guaranteed freedom from arbitrary interference or coercion from government, and to act according to their will within the confines of law. However, as advances in societies often comes with new threats, state powers to ensure national security require some adjustments in order to effectively address new security challenges.

The following section will explain the development of cyberspace in South Africa.

4.2. THE DEVELOPMENT AND RISE OF CYBERSPACE IN SOUTH AFRICA

In 1965, several universities in South Africa were among the first public institutions to acquire computers in the country. According to Mike Lawrie, a former computer engineer at Rhodes University considered to be the 'father' of the Internet in South Africa, Rhodes University in 1981 installed a Control Data Cyber model 825 computer which was equipped with a cyber operating system called the NOS (Network

Operating System). This computer was an excellent calculator with a flexible network processing unit that controlled data communications (Lawrie, 1997: 6).

Encouraged by technological developments in Europe and North America, in 1985 Lawrie and his team at Rhodes embarked on a computer network project to link together Rhodes' computer systems with those of the Universities of Witwatersrand, Pretoria and Potchefstroom, as well as the Council for Scientific and Industrial Research (CSIR). They succeeded, but the network was small and not of great use. Nonetheless, the fact that it existed and had connected different autonomous institutions was of great significance in the academic community (Lawrie, 1997: 7; TechCentral, 2016). Inspired by this development, the CSIR in 1987 spearheaded a similar project called the UNINET, which aimed to create a wider network that would virtually connect South African universities. Around the same time, Lawrie and his team were working on establishing the first internet network in South Africa. The team finally built their own gateway through a network called the Fidonet, through which they managed to have Rhodes University receive its first IP number in 1988. In 1989, the CSIR' project UNINET was successfully completed, allowing the Rhodes gateway to work as a carrier for e-mail (Lawrie, 1997: 10-14; TechCentral, 2016).

After international sanctions against apartheid South Africa were lifted in 1991, Lawrie secured a sign in on TCP/IP protocols at the University of Delaware, opening an internet gateway between South Africa and the US (Lawrie, 1997: 18; TechCentral, 2016). This was followed by the registration of the ZA domain– the country's own Internet domain. An internet network linking South Africa with other countries was now available, however, access to the network at the time was limited to the government, academic and research institutions. It was in 1993 when the World Wide Web (www) was already established that the Internet became available to the public in South Africa. However, the development of the Internet in early 1990s-South Africa took off at a slow pace, as Naudé (1999: 58) puts it, "While South Africa tried to erase the remains of apartheid in every sphere of life, the rest of the world 'quietly' moved into the information age".

Nevertheless, the emergence of commercial Internet service providers (ISPs) in 1993 as well provided means for private businesses and citizens to access the Internet. By 1997, the state-owned Telkom and private companies such as MWeb had attracted a significant number of Internet subscribers. But Internet access was still very costly and mostly available in universities and work places. There was an estimated 600 000 South African users in July 1997 (Van Niekerk, as cited by Naudé, 1999: 59). However, that number had risen to one million by the end of 1998, a 67% increase in just 18 months, and nearly all the large business corporations and various smaller companies and organisations had established a presence on the World Wide Web (Naudé, 1999: 59).

A cyber game-changer in South Africa was when broadband Internet was introduced in 2002, and particularly when wireless broadband arrived in 2004. This was at the same time when cellphone ownership and usage was significantly on the rise. By 2006, South Africans could access the Internet on portable laptop computers as well as on pocket-size cellphones that could be taken almost anywhere. Since then, other online activities that have become popular in technologically advanced societies, such as online shopping, banking, gaming, dating and, lately, social networking, have been on the rise in the country. By 2010, "the number of South African Internet users passed the 5-million mark for the first time", reaching over 10% of the country's population (World Wide Worx, 2010). The Internet upsurge continued from 2010 onwards, with the number of users in 2016 at 21 million, an almost 40% penetration of the population of South Africa (World Wide Worx, 2017).

Currently, South Africa along with the rest of the world is in the midst of the Internet of Things (IoT) phenomenon (discussed in chapter 3), though to a lesser extent compared to developed countries. IoT in the country is also expected to become widespread in the coming years, a development which will continue to have significant effects on its socio-political and economic landscapes. The influence of cyberspace in South Africa will be analysed in the following section.

4.3. THE EFFECTS OF INCREASING CYBER ACTIVITY IN SOUTH AFRICA

4.3.1. The economic and socio-political effect

Since the mid-1990s, cyberspace in South Africa contributed to the development of a fairly sophisticated ICT sector in South Africa; comprising a national fixed-line operator; five mobile service providers, and hundreds of electronic communications service providers (ECSPs). Some of these companies have grown to become large multibillion rand corporations that contribute significantly to the country's GDP and employment.

As in other ICT-driven economies, private and public activities and transactions in South Africa are increasingly being conducted through ICT platforms. The ICT sector has contributed immensely to economic growth, and continues to hold the prospects for better economic performance and job creation for South Africa. According to Statistics South Africa (Stats SA, 2017), the ICT sector in South Africa is now larger than the agriculture industry, which is by far the most sophisticated and advanced on the continent and one of the largest sources of employment in the country. But in 2014, agriculture contributed 2.4% to economic production, while the ICT sector was slightly higher at 2.7% (Stats SA, 2017).

Though South Africa is yet to tap into the full potential of the 'information revolution', Internet usage in the country has been increasing at an accelerated rate, helping to catch up with comparable developing middle income countries (Salahuddin & Gow, 2016: 1142). Reaching more than 40% of its population, South Africa has one of the highest Internet population penetration on the African continent, which provides a favourable platform for further infrastructure investments, job creation and economic growth. In turn, increased Internet usage has accelerated the sharing of ideas and information and enhanced competition and entrepreneurial innovations, "thereby further facilitating macroeconomic growth" (Salahuddin & Gow, 2016: 1142). Furthermore, it has also enhanced the government's capacity to provide services to society, as well as citizens' capacity to interact with or mobilise against the government. The '#Fees Must Fall' protests by students in 2016, the countrywide '#SaveSA' protests and the '#ZumaMustFall' protests against former President Jacob Zuma provide vivid examples of how the Internet has become an effective tool for political mobilisation for citizens.

However, while increasing cyber activity in South Africa has had such a significant positive effect, the country has also been increasingly starting to heavily rely on ICT platforms for various economic, social and political activities. On the other hand, a parallel, menacing side of cyberspace with potential catastrophic effects has equally been on the rise in the country. This is discussed in the following section.

4.3.2. The rise of cyber-attacks in South Africa

a) Cybercrime

As the popularity of the Internet was rapidly gaining momentum in the 1990s, other users demonstrated that cyberspace in South Africa can be used for malevolent purposes. In 1998, computer systems at Telkom were hacked by a 15-year-old boy. The boy had apparently breached the security features at the company to an extent that he was in a position to sabotage the systems or transfer large sums of money from the company's accounts. Nevertheless, the boy did not cause any damage or manipulate any data. He was tracked and eventually arrested on 22 October 1998 (Van Heerden, Von Solms & Mooi, 2016: 4-5). But it was a concerning cyber-security breach.

In the early 2000s when the ICT sector in the country was slowly catching up with global Internet trends, cybercriminals too were upping the ante. In 2003, a hacker stole R530 000 from ABSA's Internet banking clients. The cyber-criminal had accessed the clients' online banking profiles by sending out spyware-infested emails which then exposed the users' confidential banking details. It took several days for ABSA to detect the breach, let alone establish how the hacker operated (Van Heerden, Von Solms & Mooi, 2016: 16). The hacker, however, did not penetrate ABSA's security systems, but defrauded the bank's clients on their home computers to gain access to their bank accounts. The case was the first incident that indicated that civilian Internet users in South Africa were now unsafe in cyberspace.

In 2006, cybercriminals hacked into 10 bank accounts belonging to First National Bank, Standard Bank and ABSA clients and stole almost R1 million (Oiaga, 2006). After hacking into the personal and business accounts of the clients, the hackers transferred R979 671 into both mobile and fixed-line prepaid accounts.

The largest online heist of the time was attempted in 2010 when hackers almost stole R150 million from the South African LandBank–South Africa's agricultural finance house, also known as The Land and Agricultural Development Bank of South Africa (Van Heerden, Von Solms & Mooi, 2016: 16). The attackers hacked into Land Bank systems and retrieved passwords, and then encoded for funds to be transferred to several ABSA bank accounts of some newly-established businesses. The attempted heist was intercepted on Christmas Eve after ABSA employees noticed a sudden surge of suspicious transfers from Land Bank accounts, and froze them (Potgieter, 2011). The attempted cyber-robbery was foiled and most of the stolen money was recovered. It was one of the most sophisticated cybercrimes in South Africa, which highlighted advances and the determination of criminal syndicates, and a glimpse into the likely future of crime in South Africa.

On New Year's day of 2012, another state-owned national financial services provider, PostBank, was attacked by cybercriminals. Reported as "the first major cybercrime of 2012" in the world (Jacobsson-Purewal, 2012), hackers this time managed to steal R42 million from the bank. An employee at the bank and member of the criminal gang used a key-logger on the bank's computer systems to obtain confidential information which the criminals used to create a virtual branch of Postbank (Jacobs, 2013). The money was then transferred into multiple fraudulent bank accounts, through which large sums of money were withdrawn by mules from ATMs across three provinces (Jacobs, 2013). The case was eventually solved, and four suspects were ultimately arrested and sentenced. However, cybercrime cases were on the rise and proving to be a major concern in the country.

Burger (2013), indicated that a study by Wolfpack Information Risk reported that "the three sectors hardest hit by cybercrime in South Africa were government, banking and telecommunications". These sectors were estimated to have lost R2.6bn between January 2011 and August 2012 (Burger, 2013). Van Niekerk (2017), chronicles some of the largest cyber-attacks in South Africa which have cost the economy billions of rands annually (Sutherland, 2015; Van Niekerk, 2017: 115, 119-120). Accordingly, cyber incidents in 2014 are reported to have cost the South African economy a staggering R50 billion (Van Niekerk, 2017: 115)

Cyber-attacks have also increasingly been perpetrated from South Africa by criminal syndicates in the country towards different organisations, citizens and governments in other countries. This was evidenced in 2014 by the dismantling of a global cybercrime syndicate with a base in South Africa during a specialised operation jointly conducted by Interpol and South African and American elite law enforcement agents (Monama, 2014; U.S. Mission South Africa, 2014). A total number of twenty individuals were arrested in Canada, the United States and South Africa, of which 12 of the criminals were stationed in South Africa. According to a US Embassy publication, the syndicate inflicted a loss of millions of US dollars on the US federal government and its citizens (U.S. Mission South Africa, 2014). Such criminal syndicates are most likely still operating in South Africa.

b) Cyber-sabotage and Cyberespionage

Politically motivated cyber-attacks have also become prevalent in South Africa. This can in fact be traced back to 1994 when the country was undergoing the political transition. During the country's first democratic national elections in 1994, South Africa's electoral system was infiltrated by a suspected right-wing hacker. The unknown attacker had illegally accessed the Election Commission's computer systems and manipulated votes in favour of three right-wing parties against the ANC. But international observers detected the criminal acts, leading to the suspension of the electronic counting process. Votes were then counted manually, which delayed the announcement of the results by two days (Leyden, 2010; Plaut, 2010). The hack caused significant disruption but ultimately had no effect on the final results of the elections. However, it had potential devastating consequences in case the attacker's aim was, and succeeded, to influence the results of the elections in favour of a white party. The continuation of a minority white rule after the elections may have plunged the country down a path of civil war and destruction. Thus, the hacker could have done great harm simply by using a computer.

Cyber-sabotage demonstrated to be a looming threat to the government in 1999 when Stats SA's official web page was hacked and defaced by a group calling themselves "B1nary Outlawz". The group was apparently on a campaign trail against Telkom's 'monopoly' in the telecommunications sector (Van Heerden, Von Solms & Mooi, 2016: 5). The significance of the Stats SA hack was that it had the potential to inflict reputational damage on state institutions and harm on the country's image and economy. The Stats SA's official website provides statistics on the country's population, crime, consumer price index and GDP figures, to name just a few. Manipulation of the information can influence investors and, therefore, effect economic implications.

Infiltration of government EIS in South Africa remains to be a major concern. In February 2016, the Government Communications and Information Services (GCIS) database was hacked by "hactivist" group "Anonymous", leaking names, phone numbers, email addresses and passwords of approximately 1500 government employees (Arvinth, 2016; IOL, 2016). The Department of Water Affairs was also hacked by the same group, resulting in the leak of sensitive data including also usernames, passwords, full names, identity numbers, financial data and details of government projects (Arvinth, 2016; IOL, 2016). Again, in August the same year, the same group hacked the state-owned and government arms supplier, Armscor, allegedly accessing data that included financial records of the company and confidential information which can be used to log in to the Armscor system as supplier or manager (Abbas, 2016; Defenceweb, 2016a).

Cyberespionage in South Africa has also become a reality. In 2013, MacAskill *et al* (2013) reported in the British newspaper, The Guardian, that the British Government Communications Headquarters (GCHQ) has been conducting "a sustained campaign to penetrate South African computers, and gained access to the network of their foreign ministry; and retrieved documents including briefings for South African delegates to G20 and G8 meetings in 2009". Again in 2015, the paper together with the Qatar-based Al Jazeera news agency, revealed the 'the leaked Spy Cables'. The leaked cables were mainly acquired from communications between South Africa's State Security Agency (SSA) and other intelligence agencies during the period of 2006 to 2014.

The leaking of the cables revealed a number of security weaknesses within the South African government and intelligence services (Van Heerden, Von Solms & Mooi, 2016: 16). In fact, the "South African government and security agencies have left secrets exposed at every level and foreign spies have access to all areas of government" (Jordan, 2015a). 140 foreign spies working in South Africa were revealed to have hacked into South African government information systems to steal top-secret military plans and blueprints. Accordingly, one of the government's computers was infected with eight malware applications, "leaving military secrets exposed" (Jordan, 2015a). To this degree, South Africa suffered "the theft of Rooivalk Helicopter Blueprints" (Jordan, 2015a), as well as the "theft of 'Mokopa' anti-tank missile technology and other intellectual property at several state-owned enterprises" by Israeli intelligence operatives (Gillham, Hosken & Smillie, 2015; Jordan, 2015b). The South African-made Rooivalk helicopter "is recognised as one of the best combat helicopters in the world"

(Jordan, 2015a), and the theft of such intellectual property held at the highest security levels of the country can be regarded as a serious attack.

c) Cyberwarfare

According to Beza Belaney (2013), “South Africa may not feel it is at cyber war, but its adversaries have set up online and offline shops, and have declared co-ordinated and sophisticated cyber assaults on its people, government and financial institutions”. While Belaney’s scenario may sound ‘hyperventilated’ and typical of the ‘cyber Pearl Harbours’ narrated in the US, the 2015 Spy Cable leaks somehow vindicate him.

A secret security assessment by South African intelligence in the leaked cables identified "serious deficiencies in the security integrity" of the government’s information systems, with "far-reaching strategic implications" (Jordan, 2015a). Accordingly, the cables document several information security failures, including a scam by unknown agents to register bogus workers at South Africa’s Ministry of Foreign Affairs, and the theft of pilot exam papers from the Civil Aviation Authority (Jordan, 2015a). Moreover, the theft of the Rooivalk blue prints and missile technology from the government’s top national defence systems indicate a sophisticated and high-level attack on South Africa’s national security apparatus, and it is justifiable if it is declared as an act of war. In this case, cyberwar

Definitions of cyber-attacks are still debated and clear criteria for determining whether a cyberattack is criminal, terrorism, espionage, or an act of war-cyberwar– are yet to be established (Andress & Winterfeld, 2011: 2; Liff, 2012: 403-404; Shakarian, Shakarian & Ruef, 2013: 2; Theohary & Rollins, 2015: 4). However, what is certain is that cyber-attacks against individuals, businesses and governments do occur, and therefore implementing measures to curb the threats is a necessity. The following section analyses South Africa’s attempts to address the rising cyber-threats.

4.4. SOUTH AFRICA’S RESPONSE TO “THE CYBER THREAT”

4.4.1. The legal framework

When cyber-activity in South Africa rose to higher levels in the 2000s, the South African government enacted the Electronic Communications and Transactions Act

(ECTA) in 2002; "to facilitate and regulate electronic communications and transaction; and to prevent abuse of information systems" (ECTA, 2002: 2). The ECTA contains only three acts classified as cybercrimes: "unauthorised access to, interception of or interference with data; computer-related extortion, fraud and forgery; and attempting and assisting others to commit the above offences" (ECTA, 2002:72-74).

In the same year, the government passed the Regulation of Interception of Communications and Provision of Communication-related information Act (RICA); to provide the legal means in regulating the interception and monitoring of electronic communications. With the exception of security-related emergencies, RICA prohibits the interception and monitoring of direct and indirect communications by any person or entity who is not party to the communication (RICA, 2002: 15-20). Under RICA, every SIM card used on any communications device must be registered by its holder to their ECSPs. Also, all ECSPs have "the duty to obtain and retain particular details from their customers" and to assist the state with investigations when required. The Act further prohibits the establishment of any communications network that does not have the capability to be intercepted. RICA, however, came into effect in 2011, against the backdrop of advances in communications technology and a rise in more sophisticated cybercrimes.

Prior to RICA coming to effect, The Protection of Personal Information (PPI) Bill was passed by government in 2009, and the infamous Protection of State Information Bill (aka "the Secrecy Bill") was tabled in parliament in 2010. The PPI introduced new laws intended to protect the personal information of individuals (Grobler, Van Vuuren, & Zaaiman, 2013: 35). The 'Secrecy Bill', on the other hand, was meant to replace the Protection of Information Act of 1982, and to 'protect' State information. It allowed the government to classify any information deemed necessary for the protection of the national interest. Thus, the Bill met extreme criticism from all sectors across South Africa, and has possibly been shelved.

As cyber-attacks were becoming more sophisticated and reports of a looming cyberwar were widespread across the world (Branigan, 2010; The Economist, 2010), the South African government announced that it has approved the National Cyber Security Policy Framework (NCPF) in March 2012. The Framework was spearheaded by the Department of State Security and the Department of Communications. After remaining classified for three years, the NCPF was published in October 2015. In this document, the South African government highlight that “Cyberspace comes with new types of challenges to the governments of the world and it therefore introduces a further dimension to National Security” (SSA, 2015: 10). Amongst its key objectives, the NCPF (SSA, 2015: 6-15) aims to:

- Centralise coordination of Cybersecurity activities […], and address national security imperatives;
- Strengthen intelligence collection, investigation, prosecution and judicial processes, to prevent and address cybercrime, cyber espionage, cyber terrorism, cyber warfare and other cyber ills;
- Ensure the protection of national critical information infrastructure;

An important point outlined in the NCPF is that “Traditional investigative methods are ineffective in addressing the detection, prevention, combating and investigation of cybercrime” (SSA, 2015: 6-7). However, the framework “recognises the need to balance, on the one hand, the risks associated with the use of information systems and, on the other hand, the indispensability of extensive and free use of information technology to the functioning of open and modern societies” (SSA, 2015: 11). In this way, it is acknowledged that enhancing measures to address cyber-threats may affect civil freedoms, which themselves have to be protected.

Additionally, in 2016 The Denel Tactical Cyber Command Centre (DTC[3]) was announced at the Africa Aerospace and Defence exhibition at the behest of the Department of Defence (DefenceWeb, 2016). The Defence department further announced it is in the process of developing a National Cyber Warfare Strategy and Implementation Plan, with plans to establish a Cyber Command Centre Headquarters (Martin, 2017). Though progress on these is yet to be seen.

4.4.2. The Cybercrimes and Cybersecurity Bill

The latest legislative attempt by the South African government to address the increasing cyber-threats is the Cybercrimes and Cybersecurity bill (CAC), published in December 2015 for public comment. The CAC developed on the ECTA and added various other cyber offences. The Bill was intended to consolidate the country’s cybercrime laws and improve the capacity of law enforcement agencies and the judiciary in solving cybercrimes. The voluminous 128-page document covered more than 20 new cyber offences, which include (Duffy, 2016; RSA, 2015: 10–36):

- Illegal access (to a computer device, electronic communications network, critical database, and so on);
- Illegal interception of data (on a computer device, electronic communications network, critical database, and so on);
- Dissemination of data or messages which advocate, promote or incite hate, discrimination or violence;
- Cyber-related offences concerning terrorist activity such as espionage, illegal access to restricted data, as well as extortion.

The CAC criminalised the 'intentional', legal or illegal, access to and reporting on leaked classified state information. Moreover, it assigned crucial powers to the government's security cluster, and imposed compliance from the private sector. Of particular significance and concern under the CAC was that the Minister of State Security can declare any information infrastructure– "any data storage medium, computer device, database, computer network, electronic communications network, electronic communications infrastructure or any part thereof or any building, structure, facility, system or equipment associated therewith or part or portion thereof "(RSA, 2015: 107) – as CNII (RSA, 2015: 104). Thus, any public or privately owned information infrastructure deemed to be "of such a strategic nature that any interference with them" may, for example, "cause any major economic loss…or create a public emergency situation" (RSA, 2015: 104), can be declared as critical by the Minister of State Security. Evidently, this clause has potential to become a licence for corrupt officials to classify information that implicates them in wrong doing.

The CAC expanded RICA's terms regarding communications interception. Accordingly, any "appropriately qualified, fit and proper person" with or without a warrant operating under the supervision of the security cluster can issue directions for interception of data without notifying users (RSA, 2015:38-50). Additionally, the CAC specified for the creation of several new institutions falling under the Departments of State Security and Defence to counter cyber-threats, which included a Cyber Response Committee and a Cyber Command Centre.

Securitisation is evident in the moving of powers to regulate electronic communications from the Department of Communications to the security cluster, particularly the Departments of State Security and Defence. Furthermore, law enforcement agencies can– "having regard to the urgency of the case or the existence of exceptional circumstances"– investigate, search, access and seize any cyber-related data, network, hardware or software with verbally granted search warrants or even without search warrants (RSA, 2015: 42-44). This clause as well could provide an opportunity for corrupt officials to abuse the relevant processes and state institutions.

The CAC was confronted by intense criticism from the media, academics and, mostly, civil society organisations, with the Right To Know (R2K) campaign in the forefront. Major concerns raised revolved around the Bill's potential encroachments and violations on access to information and privacy rights, which are enshrined in the 1996 Constitution. This is a key challenge as constitutional democratic governments have to balance the need to protect the country with the freedoms of citizens.

The 2015 CAC failed public scrutiny and a shortened 88-page revised version was tabled in Parliament on 21 February 2017. The 2017 CAC removed some clauses and offences from the 2015 draft which were deemed to have potentially severe unintended consequences, and created several new offences, including disseminating "malicious communications" (RSA, 2017: 13):

- Data message which is harmful– "which is inherently false in nature and is aimed at causing mental, psychological, physical or economic harm" (such as cyberbullying or 'fake news').
- Distribution of data messages of intimate pictures without consent from involved persons (such as 'revenge porn')

The offence of "computer-related espionage" which rendered journalists and whistle-blowers in possession or reporting of classified state material liable to criminal prosecution was also removed. However, the draft Bill maintains the crucial legislative and regulatory powers assigned to the security cluster over cyber activity in South Africa. "Having regard to the urgency of the case or the existence of exceptional circumstances", law enforcement agencies are still empowered with the extensive investigation, search and seizure powers covered in the 2015 Draft Bill. ECSPs and financial services providers are still obliged not only to assist in the investigation but also to report cases of cybercrime (RSA, 2017: 20-21).

The several state structures to be established for the purpose of dealing with cybercrimes which were proposed in the 2015 Draft Bill are reduced to two (RSA, 2017: 77-78): a 24/7 Point of Contact "to ensure the provision of immediate expedited assistance"; a Cyber Response Committee "as the overseeing body to implement the cyber initiative of the Republic".

The 2017 CAC Bill remains divisive but on track to be concluded. Chances are that this may happen in 2018 or 2019. Civil society groups have raised concerns about the security cluster, particularly the State Security Agency, being in control of cybersecurity (Gerber, 2017; Hunter, 2017). Such concerns are warranted because the CAC may well afford intelligence operatives to work under 'classified assignments' while arbitrarily violating citizens' civil freedoms. Critics argue that the Bill is a threat to freedom of speech, access to information and privacy. It is indisputable that a legal framework is necessary to combat and prosecute cybercrimes in South Africa. However, the question is, how much amendment is required to make it acceptable and effective? And most importantly, does cyberspace hold a real national security threat to the country? The following section attempts to answer the latter question.

4.5. IS THE "CYBER-THREAT" A REAL NATIONAL SECURITY THREAT TO SOUTH AFRICA?

In 2013, South African Centre for Information Security CEO, Beza Belayneh, referred to cybercrime in South Africa as a national crisis, and called on the government to make it a national security concern (Duncan, 2013). Belayneh elaborated that "Network hacking, mass target phishing, persistent cyber criminality and the illegal release and posting of classified information on the internet were all hot topics in recent news headlines. These are topics that the government, citizens and the military must take seriously and treat as a crisis and a digital disaster in the making" (Belayneh, 2013). While Grobler, Vuuren & Zaaiman (2013: 35) asserted that "cyberterrorists have the capability to shut down South Africa's national power grid".

Cisco South Africa's Managing Director, Cathy Smith, indicated that "cybercrime is currently the fourth most reported economic crime in South Africa", costing the local economy as much as billions of rands annually (Cisco, 2017). Fichardt (2015) noted that "South Africa is starting to feel the heat from attackers across the globe". Furthermore, the US Federal Bureau of Investigation (FBI) has ranked South Africa sixth and seventh on its cybercrime predator list (Kilian, 2017), meaning that, the country itself is becoming a threat to other countries.

South Africa is also reported to have the "third highest number of cybercrime victims in the world", and "losing about R2.2 billion a year to cyber-attacks" (IOL, 2017; Vincente, 2016). Basie von Solms, director of the University of Johannesburg's cyber security centre, echoed Belaney's claims that "South Africa faces a national crisis in terms of cyber security" (Cyanre, 2016).

While current cyber-attacks appear to have reached 'critical' levels, scepticism still abounds about the likelihood of real and devastating cyberattacks on South Africa's information infrastructures. For instance, an extract from a submission on the 2015 CAC bill by Research ICT Africa– an institution that conducts research on effective cybersecurity policies and regulations across the African continent– read (RICTA. 2015:3):

> *Currently, the only empirical evidence on cyber-threats is provided by commercial organisations involved in internet and computer-related security which may have a commercial interest in creating alarmism among the citizenry. Despite the increasing attention cyber security is getting in security politics, it seems that cyber incidents are causing minor and occasionally major inconveniences. Research ICT Africa is concerned that potential cyber-threats identified by Governments aligned with the US War on Terrorism, have become the main reason why the South African government is imposing draconian restrictions and regulations although the current status of cyber-threats and cyber-crime has not been properly measured and assessed.*

Such a standpoint indicate complete mistrust and cynicism towards the government's cybersecurity approach. For a research institution, it also indicates bias and a dismissive approach towards the numerous expert and media reports (as discussed in section 4.3.2 in this chapter) about the billions of rands that cyber-attacks have cost the SA economy, not to mention the Spy Cable leaks that exposed national security flaws and theft of top secret military data from the South African government. On the same note, the R2K campaign, which has been at the forefront of activism against the CAC, published a paper in 2016 titled: *The Surveillance State: Communications surveillance and privacy in South Africa*. Interestingly, the paper mentions the 2015 Spy Cable leaks, but only report about “a secret agreement” between SA and Zimbabwe intelligence agencies to exchange information about “rogue NGOs” and to “identify and profile subversive media” (R2K, 2016: 13). The paper does not mention anything about exposure of national security failings and theft of sensitive military data revealed in the leaks.

The argument in this study is that cyber-attacks are real in South Africa, and the dangers they pose to the government, organisations and individuals have potential devastating effects. While life-threatening cyber-related cases have not been documented in South Africa, it would be irresponsible to conclude that the country is immune to an incident of that magnitude. Cyberspace has become a national strategic environment, and any participant in it who does not put appropriate measures in place to protect their information systems remain vulnerable to infiltration and sabotage. In an environment wherein confidential state secrets, intellectual property and banking accounts can be infiltrated and manipulated by criminals, securitisation may be unavoidable. What is required is a legal framework and government structures with proper checks and balances to attempt a reasonable balance between national security and civil liberties (this is discussed in the following section). Then, the country can grapple with another issue that is itself a threat to cybersecurity in South Africa: the lack of cyber experts, which is not covered in this study.

4.6. NATIONAL SECURITY VERSUS CIVIL LIBERTIES: STRIKING A BALANCE WITH CYBERSECURITY

The need for effective cybersecurity is of paramount importance for modern societies. The moment a country puts in place infrastructure for cyber-connectivity, a host of opportunities become apparent for organisations, individuals and the government. This is a much glorified part of the cyberspace as individuals are now presented with seemingly infinite opportunities for communication, learning, entertainment, entrepreneurship, and so on. This side of cyberspace often overshadows the other side of it, which entails challenges such as cybercrime, cyberterrorism, cyberespionage and the threat of cyberwar.

Cybersecurity measures to address such challenges are therefore crucial in today's cyber-reliant governments and economies. However, the implementation of these measures presents challenges, particularly for constitutional democratic countries such as South Africa. Overemphasising security can have adverse effects on citizens' freedom of choice pertaining to how they gain access, who they interact with, and what they do in cyberspace. Also, an excessively securitised cyberspace can suppress a nation's entrepreneurial potential, thereby denying individuals of certain economic opportunities and growth possibilities for the country's economy. A typical example is the US, whose' cyber environment has produced multinational Internet-based corporations such as Google, Facebook and Amazon, which have contributed billions of dollars to the country's GDP and created numerous direct and indirect jobs in the US. If the country's cyber-policy was too restrictive, it may have discouraged such entrepreneurial innovations.

Equally important, overemphasising cyber liberty can result in critical national security risks. It must be acknowledged that without a vigorous level of security the benefits provided by an expanded liberty as a result of the Internet will amount to nothing, if not mayhem and suffering caused by various cybercrimes. Cyberspace can only be beneficial to society if it is both free and secure. However, as explained in Chapter 2, liberty and security are fundamental human life concepts, but the expansion of one can weaken the other. In other words, a trade-off between the two concepts is mostly inevitable, as modern life progresses. This applies to all areas of political and commercial activity, including cyberspace. Government interventions to ensure security are therefore crucial, even though the same interventions carry potential intrusions on civil liberties. This is an unavoidable trade-off.

In South Africa, the freedom to legally access, investigate and use information, as well as to pursue economic opportunities in the cyber environment is, or must always be, part of our fundamental constitutional rights. Thus, the country in this regard is confronted by two challenges for the cyber domain: ensuring security, and keeping security subject to liberty; as the 1996 Constitution declares that ""National security must reflect the resolve of South Africans". The complex challenge is therefore to construct appropriate and effective checks and balances in the legal system and government structures in order to, on the one hand, improve cybersecurity and, on the other, minimise intrusions into civil liberties.

Cyber-surveillance, as mentioned in chapter 3, is an important aspect for national intelligence and strategic purposes and can produce crucial information with regard to national security threats that could emanate from cyberspace. However, gathering information on actors suspected of sinister motives often means that information on many other citizens is collected as well. In a constitutional democratic state, such a trade-off does not automatically lead to harmful effects if appropriate checks and balances are put in place in order to ensure transparency.

It is important to highlight that cyber-threats are constantly changing as technology advances; the IoT phenomenon provide a clear example. As more electronic devices are being or expected to be combined intelligently into cyberspace, hackers will eventually find loopholes to break into various publicly and privately-owned information infrastructures. Therefore, restraining the government's capacity to collect data could be a serious national security and strategic risk. Cyber-surveillance should rather be as transparent as possible, as outlined in the *International Principles on the Application of Human Rights to Communications Surveillance* (Necessary & Proportionate, 2014). The R2K's 2016 publication refers to this document, acknowledging that "Individuals should be notified of a decision authorising communications surveillance with enough time and information to enable them to challenge the decision or seek other remedies and should have access to the materials presented in support of the application for authorisation" (R2K, 2016: 19; Necessary & Proportionate, 2014: 9). However, R2K fails to highlight the exceptions to user-notification outlined in "The Principles"; which include that notifications to users can be 'delayed' provided that "Notification would seriously jeopardize the purpose for which the Communications Surveillance is authorised, or there is an imminent risk of danger to human life". Note that the 'purpose for surveillance' could at times be related to sensitive classified state information, which may not be disclosed at all. These are fundamental issues that complicate efforts to find a balance between security and liberty. However, security always comes first, because the environment has to be secured first, so that liberties can be exercised with reasonable limitations and compromises.

Therefore, this study finds that the securitisation of cyberspace in South Africa is necessary. Rather than focusing on the input level– how data is gathered– , although it is important, key checks and balances should be implemented at the output level – how the data is stored, interpreted, and used by the government and other institutions.

4.7. CONCLUSION

This chapter explained the nature of national security and civil liberties in South Africa. Accordingly, since 1994 the country had become a constitutional democracy subscribing to the new national security approach. Thus, the state is supposed to protect civil liberties and create and maintain an environment conducive for freedom. At the same time, the state's actions must be kept in check, lest it overly impinge on the liberties of citizens. However, such processes are dependent upon security issues that can influence survival of the nation.

This chapter also demonstrated that the rise of cyberspace in South Africa has had both positive and negative results. Cyberspace has had a positive impact on the country's economic growth and carries further prospects for economic development and job creation. The benefits, however, are at times overemphasised, leading to a neglect on the various threats that cyberspace comes with. Some of these threats continue to cost the economy billions of rands annually. Other threats have reached the highest echelons of the national security machinery of the country– sabotage of the government's official communications channels and even infiltration of top secret national defence data by foreign agents. It would be reckless to not acknowledge that these are critical national security threats.

As argued, measures such as cyber-surveillance are therefore necessary to deal with the constantly changing cyber-threats. However, overemphasising security is just as detrimental for a constitutional democratic country. Civil liberties are fundamental tenets of democratic South Africa. Any measures to counter national security threats have to strictly consider individual civil liberties and rights. However, as demonstrated, certain civil liberties are bound to be curtailed in efforts to ensure security. Even 'The Principles' regarding communications surveillance encompass 'exceptions' that permit the curtailment of certain civil liberties. Therefore, considering the threats, securitisation of cyberspace in South Africa is necessary, and intrusions to civil liberties such as privacy and access to information in exceptional cases are inevitable. Greater emphasis should rather be placed on implementing effective checks on how data gathered though cyber-surveillance is processed by the government, in order to combat arbitrary violations of civil liberties.

CHAPTER 5: CONCLUSION

5.1. INTRODUCTION

This concluding chapter will summarise the research and the main argument of this study. This study analysed the classical and contemporary meanings of national security and civil liberties in order to clarify the relationship between the two concepts. The study also probed the concept of cyberspace and how it has influenced both civil liberty and national security, which many states have responded to with a securitisation approach. From this context, the study analysed the securitisation of cyberspace in South Africa to find out if the process in the country is a necessity or not.

52. THE RELEVANCE AND STRUCTURE OF THE RESEARCH

The main purpose of this study was to establish whether South Africa's securitisation approach to cyberspace is necessary. The relevance of this study is that cybersecurity has become a fundamental national security concept due to cyberspace's inherent security vulnerabilities which adversaries can exploit to, in the worst case scenario, infiltrate and sabotage CNII. However, a major issue in constitutional democracies such as South Africa is that securitisation of cyberspace threatens fundamental civil liberties, which has hindered efforts by government to address rising cyber-threats. This study aimed to increase understanding and knowledge on cyberspace's influence on civil liberty and national security, which has been under-researched in the context of South Africa. To accomplish this objective, this study ensued in the following structure:

Chapter one outlined the research theme and problem, objectives, review of the literature and the methodology which the study adopted.

Chapter two explained the securitisation theory in order to clarify securitising processes. The chapter then analysed the traditional and contemporary meanings of national security, tracing the shift from a state-centric, militarist perspective to a broadened and deepened definition that also recognises non-military security threats. This chapter also delved into the definition of civil liberty, which also traces its roots to classical political philosophy. Civil liberties found in democratic societies emerged from the development of modern political societies as individuals gradually moved from the state of nature to organised politically governed societies of the modern world, in which individuals could be accorded security as well as limited liberties designed for a common interest. Moreover, the chapter established that civil liberties were found to be unavoidably subject to potential further curtailment in the face of an identifiable national security threat.

Chapter three analysed the development of the concept of cyberspace. The cyberspace domain emerged with the rise of computers, computer networks and communications technology from the 1960s onwards, reaching a revolutionary breakthrough with the invention of the Internet in the late 1980s. Cyberspace increasingly became a cornerstone of modern economies due to the ease and convenience it has embedded in communications, economic transactions and socio-political activities between individuals, organisations and states all across the world. The cyberspace domain has however also simplified means for criminals to attack private and public EIS that rely on effective cyber systems. This has led to a cyber-securitisation trend across the world as states realise that the cyber domain can be used by their enemies to infiltrate and sabotage their CNII. This was demonstrated in analysing cybercrime, cyberterrorism, cyberespionage and cyberwarfare, including some cases that have exacerbated national security fears around the world. Consequently, cybersecurity has even become a military strategic concept.

Chapter four focused on securitisation of cyberspace in South Africa. The chapter showed that South Africa is a constitutional democratic state which its national security approach is based on the post-Cold War ‘new security’ concept. This chapter also demonstrated how the rise of cyberspace produced positive socio-economic gains, as well as cybercrimes and other malicious cyber activities that have resulted in massive economic damages and threatened national security. In analysing attempts by the South African government to address cyber-threats, key legislative attempts to tackle the threats were found to be hindered by criticisms from civil society groups arguing that the latest proposed cyber laws is an attempt by government to control citizens by limiting access to information and keeping everyone under cyber-surveillance. The study found that this argument is biased and does not seriously take into account the potential catastrophic nature of cyber-threats. Thus, this chapter offered an argument on how to strike a balance between national security and civil liberties with cybersecurity.

Chapter five summarised the research and emphasised the key findings and main arguments of the study, and the relevance and structure of the research. This chapter also proposes recommendations and possible areas for further research.

5.3. CONCLUSION AND RECOMMENDATIONS

While national security is the main objective of the state, civil liberties are a key component of democratic South Africa's socio-political processes. According to the constitution, measures for national security in South Africa have to strictly take into account constitutionally enshrined rights and liberties of citizens. On the same note, national security has proven to override all other objectives of states, particularly when a national security threat becomes identifiable. This has become evident with the rise of cyberspace and cybersecurity in global politics. The benefits of the cyber domain, particularly the Internet, are indisputable and immeasurable. Likewise, the threats to national security have also become distinct and critical. South Africa has been identified among the countries in the world that suffer the most cyberattacks, resulting in massive financial damages against citizens, businesses and the government. Not only this but some cyberattacks in the country have infiltrated and manipulated national defence systems– a development that is undeniably a national security threat, whichever way it is perceived. Additionally, it is also accepted that terrorist organisations with the technical abilities and necessary resources could exploit the openness and convenience of cyberspace to attack CNII of states with the intention to cause destruction and deaths. Therefore, the argument that cyberspace poses national security threats is irrefutably accurate.

As mentioned in chapter 4, the domain of cyberspace is susceptible to constant changes as technology advances. Likewise, cyber threats are also in a mode of continuous evolution: new threats are constantly on the horizon. Therefore, it would be a grave national security and strategic risk to restrict government's powers pertaining to addressing cyber-threats. This study finds that cyber-surveillance upon users is one of the most important tool for law enforcement agencies to gather information in which users and cyber activities that threaten national security could be detected. It is acknowledged that there has been cases of intelligence incompetency and abuse by government officials for corrupt objectives on the subject of surveillance (Jordan, 2015a; Saba, 2017; Brümmer, 2015; R2K, 2017). As a result, the mentioning of surveillance may invoke suspicions due the lack of trust that has thereof developed between the government and the public. Also, there is no guarantee that the regulatory powers of cyberspace under the SSA as stipulated in the proposed CAC will not be abused by officials to arbitrarily encroach on citizens' civil liberties.

Notwithstanding, this study comes to the conclusion that the securitisation of cyberspace in South Africa is necessary. The lack of thorough cyber laws in South Africa is one among several impediments to effective cybersecurity, but it is the most important. Without a precise legal framework that properly defines illegal cyber activities and how law enforcement agencies should act, issues of cybersecurity cannot be effectively addressed, even if the country develops the necessary cyber-defence technology and skills. The CAC Bill needs to be concluded as soon as possible in order for the country to have a clear comprehensive legal framework to address cyber threats. Furthermore, this study finds that the more intrusive securitisation approach provisioned in the CAC pertaining to surveillance of cyber activities may be the only option available for governments in order to effectively deal with cyber threats. Arguments against this approach fail to take into cognisance the fact that the cyber domain is arguably akin to a public platform in which the state has the responsibility to ensure security for participants to pursue their objectives. When activities in a public platform produce major national security threats as shown in this study, such a platform need to be scrutinised and monitored in order to discern activities and participants that threaten national security. Moreover, although cases of cyberattacks that have resulted in significant loss of lives and mass destruction of property have not been evidenced yet, it would be irresponsible to conclude that they will never occur.

Intrusive measures such as cyber-surveillance, searches and seizures of articles without warrants by government may not necessarily lead to harmful effects in a constitutional democratic state such as South Africa. As mentioned in chapter 4, proper checks and balances should be implemented in the legal system and government structures to ensure that such intrusive measures are conducted transparently in order to minimise unreasonable encroachments on civil liberties or abusive practices that are conducted for selfish corrupt purposes. However, as demonstrated in chapter 4, some exceptional circumstances that involve classified state information may mean that some ‘surveillance principles’ may be overridden and certain information cannot be disclosed to the public. Hence, most importantly, the key issue should be to keep checks on how the government handles the information gathered through cyber-surveillance in order to ensure that sensitive information of citizens and other users will not be abused by those who have access to it. How information is gathered (the input level), though it is important, should not be the primary concern. Rather, the main concern should be how the information gathered is processed (the output level). The society must have some degree of assurance that the government’s securitisation of cyberspace is not an attempt to institute a tyrannical rule but to ensure security and a reasonably free environment for all participants to pursue their objectives.

Therefore, it is recommended thereof that greater emphasis in cybersecurity policy must be placed on appropriate checks and balances at the output level (processing of information) of intrusive measures such as surveillance of cyber activities. An all-inclusive approach that involves input from all national and international stakeholders can be utilised to reach an acceptable policy framework.

5.4. AREAS FOR FURTHER RESEARCH

This study has demonstrated how the domain of cyberspace has influenced civil liberties and national security, thereby, making cybersecurity a national security priority with unavoidable intrusive implications on civil liberties. However, some important areas on this topic needs further probing:

- A comprehensive study on the public opinion and attitudes on cybersecurity, cyber-threats and the impact of securitisation of cyberspace on civil liberties in South Africa. This is important in democratic South Africa to either corroborate or refute the supposed popular viewpoint propagated by some civil society groups arguing that most cybersecurity policies are draconian and not in the interest of the public. Quantitative studies conducted in Europe and North America in the aftermath of the “Edward Snowden leaks” in 2013 revealed that public opinion and attitudes on the subjects of national security, cyber-surveillance and civil liberties, even among politically active citizens, is inconsistent and conflicting (Bakir *et al*, 2015; Cable, 2015: Dencik & Cable, 2017).

- Methods to improve transparency in implementing cybersecurity policy in order to significantly minimise arbitrary violations of civil liberties of investigative tools such as cyber-surveillance.
- An integrated cybersecurity approach involving the state and the private sector in South Africa.
- The capacity of the South African state on implementing effective cybersecurity policies.

BIBLIOGRAPHY

Abbas, G. 2016. Cyber sleuths to probe Armscor hack. Independent Online (IOL). Internet: https://www.iol.co.za/news/politics/cyber-sleuths-to-probe-armscor-hack-2044890. Access: 19 November 2017.

African National Congress (ANC).1992. Ready to Govern: ANC policy guidelines for a democratic South Africa. Internet: http://www.anc.org.za/docs/pol/1992/readyto.html. Access: 18 Aug 2017.

Alexander, L. & Shore, M. 2016. Internet access is now a basic human right: part 1 – Chips with everything tech podcast. The Guardian. Internet: https://www.theguardian.com/technology/audio/2016/jul/29/internet-access-human-right-tech-podcast. Access: 07 August 2017.

Andress, J., & Winterfeld, S. 2011. Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners. Waltham: Elsevier.

Armerding, T. 2017. The 16 biggest data breaches of the 21st century. CSO. Internet: https://www.csoonline.com/article/2130877/data-breach/the-16-biggest-data-breaches-of-the-21st-century.html. Access: 03 September 2017.

Arvinth, K. 2016. Anonymous leaks South African government employee details. International Business Times. Internet: http://www.ibtimes.co.uk/anonymous-leaks-south-african-government-employee-details-1544307. Access: 29 August 2017.

Baker, N. V. 2003. National Security versus Civil Liberties. Presidential Studies Quarterly, 33 (3): 547-567.

Bakir, A., Cable. J., Dencik, L. Hintz, A., & McStay, A. 2015. Public Feeling on Privacy, Security and Surveillance: A Report by DATA-PSST and DCSS. Internet: https://sites.cardiff.ac.uk/dcssproject/files/2015/11/Public-Feeling-on-Privacy-Security-Surveillance-DATAPSST-DCSS-Nov2015.pdf. Access: 24 February 2018.

Baldwin, D. A. 1997. The concept of security. Review of International Studies, 23: 5-26.

Banks, W. C. 2017. Cyber Espionage and Electronic Surveillance: Beyond the Media Coverage. Emory Law Journal, 66: 513–525.

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

Beach, D. 2012. Analysing Foreign Policy. Houndsmills: Palgrave Macmillan.

Belayneh, B. 2013. If you want cyber peace, prepare for cyber war. Mail & Guardian Online. Internet: https://mg.co.za/article/2013-06-14-00-if-you-want-cyber-peace-prepare-for-cyber-war. Access: 18 December 2017.

Bendrath, R. 2003. The American Cyber-Angst and the Real World - Any Link?. In Bombs and Bandwidth: The Emerging Relationship between Information Technology and Security. Edited by Robert Latham. New York: The New Press.

Berlin, I. 1969. Four Essays on Liberty. Oxford: Oxford University Press.

Blackstone, W. 1803. Commentaries on the Laws of England. (St. George Tucker ed., reprint, 1969). New Jersey: Rothman Reprint Co.

Bourne, M. 2014.Understanding Security. London. Palgrave Macmillan.

Branigan, T. 2010. Chinese army to target cyber war threat. The Guardian. Internet. https://www.theguardian.com/world/2010/jul/22/chinese-army-cyber-war-department. Access: 20 November 2017.

Brenner, J. 2014. The New Industrial Espionage. The American Interest, 10 (3): 1–13.

Brümmer, S. 2015. Zuma: Mbeki offered me a R20m bribe. Mail & Guardian. Internet: https://mg.co.za/article/2015-04-16-zuma-mbeki-offered-me-a-r20m-bribe. Access: 26 February 2018.

Brunst, P. W. 2010. Terrorism and the Internet: New Threats Posed by Cyberterrorism and Terrorist Use of the Internet. In A War on Terror?: The European Stance on a New Threat, Changing Laws and Human Rights Implications. Edited by Wade, M. & Maljevic, A. New York: Springer-Verlag.

Burger, J. 2013. 'National crisis' of cybercrime poses major threat to SA business. BusinessDay. Internet: https://www.businesslive.co.za/bd/opinion/2013-09-18-national-crisis-of-cybercrime-poses-major-threat-to-sa-business/. Access: 29 September 2017.

Business Insider Intelligence. 2016. There will be 24 billion IoT devices installed on Earth by 2020. Business Insider. Internet: http://www.businessinsider.com/there-will-be-34-billion-iot-devices-installed-on-earth-by-2020-2016-5?IR=T. Access: 22 September 2017.

Buzan, B., Kelstrup, M., Lemaitre, P. & Tromer, E. 1990. The European Security Order Recast: Scenarios for the Post-Cold War Era. London: Pinter.

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

Carr, J. 2010. Inside Cyber Warfare: Mapping the cyber underworld. Sebastopol, CA: O'Reilly Media.

Cartwright, R. C. & Condé, H. V. 2000. Human Rights in the United States: A Dictionary and Documents, Volume 2. Minnesota: ABC-CLIO.

Cable, J. 2015. Working Paper - An overview of public opinion polls since the Edward Snowden revelations in June 2013. UK Public Opinion Review. Internet: https://sites.cardiff.ac.uk/dcssproject/files/2015/08/UK-Public-Opinion-Review-180615.pdf. Access: 23 February 2018.

Castells, E. 2014. The Impact of the Internet on Society: A Global Perspective. OpenMind. Internet: https://www.bbvaopenmind.com/en/article/the-impact-of-the-internet-on-society-a-global-perspective/?fullscreen=true. Access: 02 September 2017.

Chandra, S. & Bhonsle, R. 2015. National Security: Concept, Measurement and Management. Strategic Analysis, 39 (4): 337-359.

Chuipka, A. 2016. The Strategies of Cyberterrorism: Is Cyberterrorism an effective means to Achieving the Goals of Terrorists?. Major Research Paper. Internet: https://ruor.uottawa.ca/bitstream/10393/35695/1/CHUIPKA%2C%20Adam%2020169.pdf. Access: 04 September 2017.

Cisco. 2017. Shortage in cybersecurity skills – a challenge and opportunity. Cisco (NASDAQ: CSCO). Internet: https://www.cisco.com/c/en_za/about/press-releases-south-africa/2017/20170704.html. Access: 13 January 2018.

Cobb, A. 1999. Electronic Gallipoli? Australian Journal of International Affairs, 53(2):133–149.

Cole, D. & Dempsey, J. X. 2002. Terrorism and the Constitution: Sacrificing Civil Liberties in the Name of National Security. New York: New Press.

Constant, B. 1988. Political Writings. Cambridge: Cambridge University Press.

Coser, I. 2014. The Concept of Liberty: the Polemic between the NeoRepublicans and Isaiah Berlin. Brazilian Political Science Review, 8 (3): 39–65.

Craigen, D., Diakun-Thibault, N., & Purse, R. 2014. Defining Cybersecurity. Technology Innovation Management Review. Internet: https://www.researchgate.net/publication/267631801_Defining_Cybersecurity. Access: 18 August 2017.

DefenceWeb. 2016. Denel forms cyber security division. Internet: http://www.defenceweb.co.za/index.php?option=com_content&task=view&id=45119&catid=90&Itemid=204. Access: 28 November 2017.

Deibert, R. & Rohozinski, R. 2010a. Liberation vs. Control: the future of cyberspace. Journal of Democracy, 21 (4): 42– 57.

Deibert, R. & Rohozinski, R. 2010b. Risking Security: The Policies and Paradoxes of Cyberspace Security. International Political Sociology, 4: 15– 32.

Dencik, L. & Cable, J. 2017. The Advent of Surveillance Realism: Public Opinion and Activist Responses to the Snowden Leaks. International Journal of Communication, 11: 763–781.

Denning, D. 1999. Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy. Washington DC: Nautilus.

Dinh, V. D.2002. Freedom and Security after September 11. Harvard Journal of Law and Public Policy399, 25(2).

Dlamini, I.Z. 2012. Cyber Security Awareness Initiatives in South Africa: A Synergy Approach. CSIR Research space. Internet: http://researchspace.csir.co.za/dspace/bitstream/handle/10204/5941/Dlamini_2012.p df;jsessionid=6C4E81DF82BCF91750152C2C5CCF030B?sequence=1. Access: 28 October 2017.

Duffy, S. 2016. SA's new cybercrimes law explained. Gadget. Internet: http://www.gadget.co.za/sas-new-cybercrimes-law-explained/. Access: 18 November 2017.

Duncan, J. 2013. Cybercrime in South Africa a crisis: expert. Mail & Guardian. Internet: https://mybroadband.co.za/news/security/80589-cybercrime-in-south-africa-a-crisis-expert.html. Access: 29 September 2017.

Dunn-Cavelty, M. 2013. From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse. International Studies Review 15 105–122.

Dworkin, R. 2003. Terror and the Attack on Civil Liberties. New York Review of Books, 50(17).

ECTA. 2002. Electronic Communications and Transactions Act, 2002. Government Gazette- Republic of South Africa. Internet: https://www.gov.za/sites/www.gov.za/files/a25-02.pdf. Access: 30 November 2017.

Encyclopædia Britannica. 2017. Libertas. Internet: https://www.britannica.com/topic/Libertas-Roman-religion. Access: 22 Aug 2017.

Etzioni, A. 2015. NSA: National Security vs. Individual Rights. Intelligence and National Security, 30:1, 100-136. 13 December 2017.

Farwell, J. P. & Rohozinski, R. 2011. Stuxnet and the Future of Cyber War. Survival, 53 (1): 23-40.

Fichardt, C. 2015. Just how big a threat is cybercrime to South Africa?. Memeburn. Internet: https://memeburn.com/2015/06/just-how-big-a-threat-is-cybercrime-to-south-africa/. Access: 11 December 2017.

Finkelstein, A. E. et al. 2017. Trade-Offs Between Civil Liberties and National Security: A Discrete Choice Experiment. Contemporary Economic Policy, 35 (2): 292–311.

Fjäder, C. 2014. The nation-state, national security and resilience in the age of globalization. Resilience, 2 (2): 114-129.

Garcia, B. E. & Geva, N. 2016. Security versus Liberty in the Context of Counterterrorism: An Experimental Approach. Terrorism and Political Violence, 28 (1): 30-48.

Geers, K. 2011. Strategic Cyber Security. Tallinn: CCD COE Publication. Internet: https://korben.info/wp-content/uploads/defcon/SpeakerPresentations/Geers/DEFCON-20-Kenneth-Geers-Strategic-Cyber-Security.pdf. Access: 27 August 2017.

George, F. C. 2005. Civil Liberties vs. National Security: The Enduring Tension, 19Notre Dame J.L. Ethics & Pub. Pol'y219. Internet: http://scholarship.law.nd.edu/ndjlepp/vol19/iss1/8. Access: 18 September 2017.

Gerber, J. 2017. Spooks should not run cybersecurity - R2K. News24. Internet: https://www.news24.com/SouthAfrica/News/spooks-should-not-run-cybersecurity-r2k-20170913. Access: 9 November 2017.

Gibson, W. 1984. Neuromancer. New York: Ace Books.

Gillham, S., Hosken, G., & Smillie, S. 2015. PE spy cables terror shock. The Herald (South Africa). Internet: https://www.pressreader.com/south-africa/the-herald-south-africa/20150225/281479274864007. Access: 29 September 2017.

Gillwald, A., Moyo, M., & Stork, C. 2014. Understanding what is happening in ICT in South Africa: A supply- and demand- side analysis of the ICT sector. Evidence for ICT Policy Action.

Goldman, E. O. 2001. 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.

Gomez. M. A. N. 2016. Arming Cyberspace: The Militarization of a Virtual Domain. Global Security and Intelligence Studies, 1 (2): 41–65.

Gourevitch, V. 1997. Rousseau: The Social Contract and Other Later Political Writings. Cambridge: Cambridge University Press.

Grobler, M., van Vuuren, J. J., & Zaaiman, J. 2013. Preparing South Africa for Cyber Crime and Cyber Defence. Systemics, Cybernetics and Informatics, 11 (7): 32–41.

GSMA. 2014. Understanding the Internet of Things (IoT). Internet: https://www.gsma.com/iot/wp-content/uploads/2014/08/cl_iot_wp_07_14.pdf. Access: 16 February 2018.

Haftendorn, H. 1991. The Security Puzzle: Theory-Building and Discipline-Building in International Security. International Studies Quarterly, 35 (1): 3-17.

Hansen, L. & Nissenbaum, H. 2009. Digital Disaster, Cyber Security, and the Copenhagen School. International Studies Quarterly, 53 (4): 1155–1175.

Heickerö, R. 2014. Cyber Terrorism: Electronic Jihad. Strategic Analysis, 38 (4): 554-565.

Heyman, S. J. 1992. Positive and Negative Liberty - Chicago-Kent Dedication Symposium: Topics in Jurisprudence. Chicago-Kent Law Review. 68 (81): 81-90.

Hobbes, T. 1651. Leviathan: or the Matter, Forme, & Power of a Common-wealth Ecclesiasticall and Civill. Internet. https://socserv2.socsci.mcmaster.ca/econ/ugcm/3ll3/hobbes/Leviathan.pdf. Access: 19 November 2017.

Hoscheidt, M. M. & Eichner, F. E. 2014. Legal and Political Measures to Address Cybercrime. UFRGS Model United Nations, 2: 445-477.

Hunter, M. 2017. GroundUp: Cybercrimes Bill threatens our freedom. Daily Maverick. Internet: https://www.dailymaverick.co.za/article/2017-07-26-groundup-cybercrimes-bill-threatens-our-freedom/#.Wm3GoHaWbIU. Access: 16 January 2018.

Huysmans, J. 1998. Revisiting Copenhagen: Or, On the Creative Development of a Security Studies Agenda in Europe. European Journal of International Relations, 4 (4): 479-505.

IOL, 2016. Panic hits as Anonymous hack SA sites. Independent Online, Politics. Internet: http://www.iol.co.za/news/politics/panic-hits-as-anonymous-hack-sa-sites-1984103. Access: 08 September 2017.

IOL. 2017. SA has third highest number of cybercrime victims in world. Internet: https://www.iol.co.za/capetimes/news/sa-has-third-highest-number-of-cybercrime-victims-in-world-11594553. Access: 18 November 2017.

ISO/IEC 27032: 2012. Information technology — Security techniques — Guidelines for cybersecurity. Internet: https://www.iso.org/obp/ui/#iso:std:iso-iec:27032:ed-1:v1:en. Access: 27 October 2017.

ITU. 2011. The ITU National Cybersecurity Strategy Guide. International Telecommunication Union. Internet: http://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf. Access: 28 October 2017.

ITU. 2012. Understanding cybercrime: Phenomena, challenges and legal response. International Telecommunication Union. Internet: http://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf. Access: 2 October 2017.

ITU. 2015. ITU releases 2015 ICT figures: Statistics confirm ICT revolution of the past 15 years. International Telecommunication Union. Internet: http://www.itu.int/net/pressoffice/press_releases/2015/17.aspx#.WrrsgnpubIV. Access: 20 February 2018.

ITU. 2018. Definition of cybersecurity. Internet: https://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx. Access: 2 October 2017.

Jacobs, M. 2013. Cyber heist mastermind in court again. ITWeb. Internet: https://www.itweb.co.za/content/VJBwEr7n81Aq6Db2. Access: 25 September 2017.

Jacobsson-Purewal, S. 2012. Hackers steal $6.7 million in cyber bank robbery. PC World. Internet: https://www.pcworld.com/article/248340/hackers_steal_6_7_million_in_cyber_bank_robbery.html Access: 18 October 2017.

Jaffe, M. 2014. IoT Won’t Work Without Artificial Intelligence. Wired. Internet: https://www.wired.com/insights/2014/11/iot-wont-work-without-artificial-intelligence/. Access: 28 November 2017.

Jordan, W. 2015a. Spy Cables expose S Africa's alarming security failings. Al Jazeera. Internet: http://www.aljazeera.com/news/2015/02/spy-cables-expose-south-africa-alarming-security-failings-guardian-ssa-150224162919994.html. Access: 16 October 2017.

Jordan, W. 2015b. Israeli cable reveals S Africa missile theft cover-up. Al Jazeera. Internet: http://www.aljazeera.com/news/2015/02/israeli-cable-reveals-south-africa-missile-theft-cover-makopa-south-ssa-guardian-mos-150219180058280.html. Access: 16 October 2017.

Kenney, M. 2015. Cyber-Terrorism in a Post-Stuxnet World. Orbis, 59 (1): 111–128.

Kilian, A. 2017. Cybercrime becoming a major threat in South Africa. Engineering News. Internet: http://engineeringnews.co.za/article/cybercrime-becoming-a-major-threat-in-south-africa-2017-09-19. Access: 17 October 2017.

Kosenkov, A. 2016. Cyber Conflicts as a New Global Threat. Future Internet, 8 (45): 1-9.

Kramer, F.D. 2009. Cyberpower and National Security: Policy Recommendations for a Strategic Framework. In Cyberpower and National Security. Edited by Kramer, F.D., Starr, S., & Wentz, L. K. Washington DC: National Defense University Press.

Krause, K. & Williams, M. C. 1996. Broadening the Agenda of Security Studies: Politics and Methods. International Studies Review, 40 (2): 229-254.

Kuehl, D. 2009. From Cyberspace to Cyberpower: Defining the Problem. In Cyberpower and National Security. Edited by Kramer, F.D., Starr, S., & Wentz, L. K. Washington DC: National Defense University Press.

Latham, R. 2003. Introduction. In Bombs and Bandwidth: The Emerging Relationship between Information Technology and Security. Edited by Robert Latham. New York: The New Press.

Lawrie, M. 1997. The History of the Internet in South Africa: How it began. Internet: http://archive.hmvh.net/txtfiles/interbbs/SAInternetHistory.pdf. Access: 4 October 2017.

Leyden, J. 2010. Hacker almost derailed Mandela election in South Africa. The Register. Internet: http://www.theregister.co.uk/2010/10/27/sa_election_hack/. Access: 17 October 2017.

LeVPN, 2017. Where Does Cybercrime Come From? The Origin & Evolution of Cybercrime. LeVPN. Internet: https://www.le-vpn.com/history-cyber-crime-origin-evolution/. Access: 03 September 2017.

Liff, A. P. 2012. Cyberwar: A New ‘Absolute Weapon’? The Proliferation of Cyberwarfare Capabilities and Interstate War. Journal of Strategic Studies, 35 (3): 401-428.

Lillemose, J. & Kryger, M. 2015. The (Re) invention of Cyberspace. Kunstkritikk. Internet: http://www.kunstkritikk.com/kommentar/the-reinvention-of-cyberspace/. Access: 27 August 2017.

Locke, J. 1690a. An Essay Concerning Human Understanding. Internet: ftp://ftp.dca.fee.unicamp.br/pub/docs/ia005/humanund.pdf. Access: 17 Aug 2017.

Locke, J. 1690b. Second Treatise of Government. Internet: https://ia802205.us.archive.org/1/items/ost-history-second_treatise_of_government/Second_Treatise_of_Government.pdf. Access: 22 November 2017.

Lopach, J. J. & Luckowski, J. A. 2006. National Security and Civil Liberty: Striking the Balance. The Social Studies, 97(6): 245-248.

Lowi, T. J. & Ginsberg, B. 2000. American Government: Freedom and Power. New York: W.W. Norton.

Lowe, D. 2016. Surveillance and International Terrorism Intelligence Exchange: Balancing the Interests of National Security and Individual Liberty. Terrorism and Political Violence, 28 (4): 653-673.

MacAskill, E *et al*. 2013. GCHQ intercepted foreign politicians' communications at G20 summits. The Guardian. Internet: https://www.theguardian.com/uk/2013/jun/16/gchq-intercepted-communications-g20-summits. Access: 16 January 2018.

Martin, G. 2017. DoD outlines 2017 defence priorities. Defenceweb. Internet: http://www.defenceweb.co.za/index.php?option=com_content&view=article&id=49445:dod-outlines-2017-defence-priorities&catid=111:sa-defence&Itemid=242. Access: 29 November 2017.

Mayer, M., et al. 2014. How would you define Cyberspace? Internet: https://www.academia.edu/7096442/How_would_you_define_Cyberspace. Access: 05 September 2017.

Mayer, M., et al. 2013. International Politics in the Digital Age: Power Diffusion or Power Concentration? Internet: https://www.academia.edu/14336129/International_Politics_in_the_Digital_Age. Access: 05 September 2017.

McDonald, M. 2008. Securitization and the Construction of Security. European Journal of International Relations, 14 (4): 563–587.

McGraw, G. 2013. Cyber War is Inevitable (Unless We Build Security In). Journal of Strategic Studies, 36 (1): 109-119.

McSweeney, B. 1999.Security, Identity and Interests: A Sociology of International Relations. Cambridge: Cambridge University Press.

McQuade, S. 2011. Cybercrime. In The Oxford Handbook of Crime and Public Policy. Edited by Tonry, M. Oxford: Oxford University Press.

McQuade, S. & Sampat, N. 2008. Survey on Internet and At-Risk Behaviours. Rochester: Rochester Institute of Technology Libraries.

Michaelsen, P. 2006. Balancing Civil Liberties against National Security? A Critique of Counterterrorism Rhetoric. UNSW Law Journal, 29(2): 1-21.

Miller, D .1991. Liberty. (ed). Oxford: Oxford University Press.

Mohammed, Z.K.A., & Ahmed, E.S.A. Internet of Things: Applications, Challenges and Related Future Technologies. World Scientific News, 67(2): 126-148.

Monama, T. 2014. Global cybercrime syndicate bust in SA. IOL. Internet: https://www.iol.co.za/news/global-cyber-crime-syndicate-bust-in-sa-1692132. Access: 23 February 2018.

Morag, N. 2014. Cybercrime, Cyberespionage, and Cybersabotage: Understanding Emerging Threats. Colorado Technical University. Internet: http://www.coloradotech.edu/~/media/CTU/Files/ThoughtLeadership/cybercrime-white-paper.ashx. Access: 29 August 2017.

Morgenthau, H. J. 1952. Another "Great Debate": The National Interest of the United States. The American Political Science Review, 46 (4): 961-988.

Naudé, A. M. E. 1999. Communication technology and development: can South Africa afford the information explosion?. Communicatio, 25 (1-2): 58-64.

Naughton, J. 2017. North Korea's deadliest weapon? Its hackers. The Guardian. Internet: https://www.theguardian.com/commentisfree/2017/oct/22/north-korea-deadliest-weapon-cyber-operations-sony-pictures. Access: 24 February 2018.

Necessary & Proportionate. 2014. International Principles on the Application of Human Rights to Communications Surveillance. Internet: https://necessaryandproportionate.org/files/2016/03/04/en_principles_2014.pdf. Access: 18 November 2018.

Neocleous, M. 2006. From Social to National Security: On the Fabrication of Economic Order. Security Dialogue, 37 (3): 363–384.

Nissenbaum, H. 2005. Where Computer Security Meets National Security. Ethics and Information Technology 7 (2): 61-73.

Oiaga, M. 2006. Three South African Banks Hit by Hackers. Softpedia News. Internet: http://news.softpedia.com/news/Three-South-African-Banks-Hit-by-Hackers-28590.shtml. Access: 5 December 2017.

Oppler, J. 2015. Liberty, Security, and Judicial Review in the War on Terror: An Analysis of Supreme Court Approaches to Deference in a Post-9/11 Context. Senior Independent Study Theses. Paper 6908. Internet: http://openworks.wooster.edu/independentstudy/6908. Access: 23 March 2017.

Ottis, R. & Lorents, P. 2010. Cyberspace: Definition and Implications. NATO Cooperative Cyber Defence Centre of Excellence. Tallinn, Estonia. Internet: https://www.etis.ee/File/DownloadPublic/7d491419-9237-4de0-b324-62d597a0c99f?name=Fail_2010_ICIW_Ottis_Lorents.pdf&type=application%2Fpdf. Access: 30 August 2017.

Pitts, V. 2017. Cyber Crimes: History of World's Worst Cyber Attacks. New Delhi: Vij Books.

Plaut, M. 2010. Book says hacker tried to stop Mandela coming to power. BBC News. Internet: http://www.bbc.com/news/world-africa-11630092. Access: 9 December 2017.

Posner, R. A. 2001. Notes & Dispatches – The Law: Security versus Civil Liberties. The Atlantic Monthly, 288(5): 46–47.

Potgieter, D. 2011. Absa intercepts Land Bank swindle. Independent Online (IOL). Internet: https://www.iol.co.za/business-report/companies/absa-intercepts-land-bank-swindle-1009423. Access: 11 December 2017.

PricewaterhouseCoopers. 2016. Economic Crime: A South African pandemic, no sector or region is immune. Global Economic Crime Survey 2016 5th South African edition. Internet: https://www.pwc.co.za/en/assets/pdf/south-african-crime-survey-2016.pdf. Access: 20 September 2017.

R2K. 2016. The Surveillance State: Communications surveillance and privacy in South Africa. Right2Know Campaign. Internet: https://www.mediaanddemocracy.com/uploads/1/6/5/7/16577624/sa_surveillancestate-web.pdf. Access: 16 January 2018.

R2K, 2017. Case studies: how communications surveillance has been abused in SA. Right2Know Campaign. Internet: http://www.r2k.org.za/2017/04/20/case-studies-communications-surveillance-abuse/. Access: 23 February 2018.

RICA. 2002. Regulation of Interception of Communications and Provision of Communication-related information Act, 2002. Government Gazette- Republic of South Africa. Internet: http://www.justice.gov.za/legislation/acts/2002-070.pdf. Access: 14 January 2018.

RICTA. 2015. Submission on the cybercrimes and cybersecurity bill. Research ICT Africa. Internet: https://www.researchictafrica.net/publications/Other_publications/2015_RIA_Submission_to_Cybersecurity_and_Cybercrime_Draft_Bill.pdf. Access: 11 December 2017.

Robinson, M., Jones, K., & Janicke, H. 2015. Cyber warfare: Issues and challenges. Computers & Security. Internet: https://www.researchgate.net/profile/Michael_Robinson40/publication/276248097_Cyber_warfare_Issues_and_challenges/links/5a02cd01aca2720df3cf1053/Cyber-warfare-Issues-and-challenges.pdf. Access: 24 January 2018.

RSA. 1994. White Paper on Intelligence. Republic of South Africa. Pretoria. Internet: http://www.ssa.gov.za/Portals/0/SSA%20docs/Legislation/White%20Paper%20on%20Intelligence.PDF. Access: 17 Aug 2017.

RSA. 1996. The Constitution of the Republic of South Africa. Republic of South Africa. Pretoria: Government Printers.

RSA. 2011. Cyber Security Awareness Month Fails to Deter Phishers. Internet: http://www.rsa.com/solutions/consumer_authentication/intelreport/11541_Online_Fraud_report_1011.pdf. Access: 18 January 2018.

RSA. 2015. Cybercrimes and Cybersecurity Bill Draft for Public Comment. Department Of Justice and Correctional Services. Internet: http://www.justice.gov.za/legislation/invitations/CyberCrimesBill2015.pdf. Access: 29 November 2017.

RSA. 2017. Cybercrimes and Cybersecurity Bill. Republic Of South Africa. Internet: http://www.justice.gov.za/legislation/bills/CyberCrimesBill2017.pdf. Access: 18 September 2017.

Rubenstein, D. 2014. Nation State Cyber Espionage and its Impacts. Washington University in St. Louis. Internet: http://www.cse.wustl.edu/~jain/cse571-14/ftp/cyber_espionage.pdf. Access: 6 September 2017.

Saba, A. 2017. Cop illegally bugged Sunday Times calls. Sunday Times. Internet: https://www.timeslive.co.za/sunday-times/news/2017-07-29-cop-illegally-bugged-sunday-times-calls/. Access: 26 February 2018.

Salahuddin, M. & Gow, J. 2016. The effects of Internet usage, financial development and trade openness on economic growth in South Africa: A time series analysis. Telematics and Informatics, 33: 1141–1154.

Sanger, D. E., Kirkpatrick, D. D., & Nicole Perlroth. 2017. The World Once Laughed at North Korean Cyberpower. No More. The New York Times. Internet: https://www.nytimes.com/2017/10/15/world/asia/north-korea-hacking-cyber-sony.html. Access: 23 February 2018.

Schmitt, M. N. 2013. (ed). Tallinn Manual on the International Law Applicable to Cyber Warfare: Prepared by the International Group of Experts at the Invitation of the NATO

Cooperative Cyber Defence Centre of Excellence. Cambridge: Cambridge University Press.

Seegers, A. 2010. The new security in democratic South Africa: a cautionary tale. Conflict, Security & Development, 10 (2): 263-285.

Schatz, D., Bashroush, R., & Wall, J. 2017. Towards a More Representative Definition of Cyber Security. Journal of Digital Forensics, Security and Law, 12 (2): 53-74.

Shinder, D. L. 2002. Scene of the Cybercrime: computer forensics handbook. Rockland: Syngress Publishing.

Schultze, C. L. 1973. The Economic Content of National Security Policy. Foreign Affairs, 51 (3): 529-530.

Shakarian, P., Shakarian, J., & Ruef, A. 2013. Introduction to Cyberwarfare: A Multidisciplinary Approach. Waltham: Elsevier.

Skaaning, S. E. 2006. Defining and Founding Civil Liberty. Center on Democracy, Development, and the Rule of Law (CDRL) Working Papers.

Smith, S. 1999. The increasing insecurity of security studies: Conceptualising security in the last twenty years. Contemporary Security Policy. 20 (3): 72-101.

SSA. 2015. The National Cybersecurity Policy Framework (NCPF). State Security Agency. Internet: https://www.gov.za/sites/www.gov.za/files/39475_gon609.pdf. Access: 18 November 2017.

Stats SA. 2017. Three facts about the ICT sector. Statistics South Africa. Internet: http://www.statssa.gov.za/?p=9852. Access: 30 October 2017.

Stritzel H. 2014. Security in Translation: Securitisation Theory and the Localisation of Threat. London: Palgrave Macmillan.

Sutherland, C. 2015. Cybercrime in South Africa on the rise. FA News. Internet: https://www.fanews.co.za/article/short-term-insurance/15/general/1217/cybercrime-in-south-africa-on-the-rise/17479. Access: 29 November 2017.

TechCentral. 2016. The Internet in South Africa turns 25. Internet: https://techcentral.co.za/the-internet-in-south-africa-turns-25/69971/. Access: 15 August 2017.

The Economist, 2010. Cyberwar: War in the fifth domain. Internet: http://www.economist.com/node/16478792. Access: 29 September 2017.

Theohary, C., & Rollins, J. W. 2015. Cyberwarfare and Cyberterrorism: In Brief. Congressional Research Service. Internet: https://fas.org/sgp/crs/natsec/R43955.pdf. Access: 19 December 2017.

Ullman, R. H. 1983. Redefining Security. International Security, 8 (1): 129-153.

UNHRC, 2016. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue*. UN. Internet: http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf . Access: 18 October 2017.

UNODC, 2013. Comprehensive Study on Cybercrime: Draft. United Nations Office on Drugs and Crime. Internet: https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf. Access: 22 October 2017.

U.S. Mission South Africa. 2014. Cyber-Financial Fraud Investigation Nets Numerous Arrests in South Africa, Canada, US. U.S. Embassy and Consulates in South Africa. Internet. https://za.usembassy.gov/cyber-financial-fraud-investigation-nets-numerous-arrests-in-south-africa-canada-us/. Access: 22 October 2017.

Van Heerden, R., Von Solms, S., & Mooi, R. 2016. Classification of Cyber Attacks in South Africa. IST-Africa Conference Proceedings. Internet: https://researchspace.csir.co.za/dspace/bitstream/handle/10204/8930/Van%20Heerden2_2016.pdf?sequence=1. Access: 27 January 2018.

Van Niekerk, B. 2017. An analysis of cyber-incidents in South Africa. The African Journal of Information and Communication (AJIC). 20: 113-132.

Vincente, A. 2016. Cybercrime affects a third of SA companies. ITWeb. Internet: https://www.itweb.co.za/content/APero3qZm2BMQb6m. Access: 28 December 2017.

Von Boemcken, M. & Schetter, C. 2016. Security: What Is It? What Does It Do? Think Piece 09 Reflection Group. Internet: http://library.fes.de/pdf-files/iez/12368.pdf. Access: 12 November 2017.

Wæver, O., *et al*. 1993. Identity, Migration, and the New Security Agenda in Europe. New York: St. Martin's Press.

Wæver, O. 2004. Aberystwyth, Paris, Copenhagen: New Schools in Security Theory and the Origins between Core and Periphery. Paper presented at the annual meeting of the International Studies Association, Montreal. Internet: https://www.scribd.com/doc/40010349/Ole-Waever-Aberystwyth-Paris-en-New-Schools-in-Security-Theory-and-Their-Origins-Between-Core-and-Periphery. Access: 30 September 2017.

Waltz, K. 1979. Theory of International Politics. Boston: McGraw-Hill.

Warshawsky, M. 2013. The Balance to be found between Civil Liberties and National Security. The RUSI Journal, 158 (2): 94-99.

Weimann, W. 2005. Cyberterrorism: The Sum of All Fears?. Studies in Conflict & Terrorism, 28 (2): 129-149.

William, G. Neuromancer. New York: Berkley Publishing Group.

Williams, M. C. 2003. Words, Images, Enemies: Securitization and International Politics. International Studies Quarterly, 4:1 (4): 511-529.

Wilson, R.B. 2014. A New Balance: National Security and Privacy in a Post 9-11 World. Honours Theses: Paper 729. Internet: http://digitalcommons.colby.edu/honorstheses/729. Access: 29 August 2017.

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

World Wide Worx. 2010. SA Internet growth accelerates. Internet: http://www.worldwideworx.com/sa-internet-growth-accelerates/. Access: 9 November 2017.

World Wide Worx. 2017. Internet Access in South Africa 2017: Executive Summary. Internet: http://www.worldwideworx.com/wp-content/uploads/2017/07/Exec-Summary-Internet-Access-in-SA-2017.pdf. Access: 9 November 2017.

Yould, R. E. 2003. Beyond the American Fortress: Understanding Homeland Security in the Information Age. In Bombs and Bandwidth: The Emerging Relationship between

Information Technology and Security. Edited by Robert Latham. New York: The New Press.

Zittrain, J. *et al*. 2017. The Shifting Landscape of Global Internet Censorship. Berkman Klein Center for Internet & Society Research Publication. Internet: http://nrs.harvard.edu/urn-3:HUL.InstRepos:33084425. Access: 12 September 2017.