CYBER SECURITY AS AN EMERGING CHALLENGE TO SOUTH AFRICAN NATIONAL SECURITY

By
Jordan Luke Griffiths

Student Number 10345028

A mini-dissertation submitted in partial fulfilment of the requirements for the degree
Master of Security Studies (MSS)

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

Supervisor: Mr. Roland Henwood

November 2016

UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

UNIVERSITY OF PRETORIA

FACULTY OF HUMANITIES

RESEARCH PROPOSAL & ETHICS COMMITTEE

DECLARATION

Full name : Jordan Luke Griffiths____

Student Number : 1034508____

Degree/Qualification: Master of Security Studies_________________________

Title of thesis/dissertation/mini-dissertation:

Cyber Security as an emerging challenge to South African national security

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.

SIGNATURE

15 December 2016_
DATE

ABSTRACT

As South Africa is a rapidly developing country and has become more increasingly technologically advanced through the growth in information communications technology (ICT) and the expansion of modern state infrastructure. With this growth more of the country's citizens have also become connected as access to the internet has spread. However, this advancement has also introduced a new challenge to South African national security in the form of cyber security. The spread of technology has created new vulnerabilities within the cyber domain that may directly work to undermine the country's security. Computer hackers are developing advanced software and methods designed to infiltrate and disable critical state infrastructure, capture confidential state or corporate information, engage in identity theft and fraud, rob banks and financial institutions and even undermine democratic processes such as elections. Terrorists have also embraced cyber space as a domain where they can recruit followers, spread propaganda, and provide advice and encouragement to those who wish to conduct terrorist operations. States are now not only creating cyber teams that can counter these terrorists but they are also developing cyber weapons which can be deployed to disrupt the operations of other countries should the need arise.

This study analyses the challenge that cyber security poses to South African national security. This research contextualises the concept of cyber security within the theoretical understanding of national security. In highlighting the destructive capabilities of cyber attacks, the study provides detail on four examples, namely the 2007 attacks against Estonia, the impact of the Stuxnet worm on Iranian centrifuges in 2010, Chinese hackers targeting the USA and the hack on the Democratic National Committee. This then provides a foundation through which South Africa's cyber security position can be evaluated.

The study also analyses several public cyber attacks that have targeted South Africa and presents a number of research reports which identify the country as one of the most targeted nations in the world. Although South Africa has acknowledged the role of ICT in its development, the country has failed to engage on the importance of cyber security. This study examines the country's policy progress with regards to cyber security which has ultimately lead to the Cyber Security and Cyber Crimes bill which was released for public comment in December 2015. However, the country's cyber position is weakened by its lack of cyber skills and capacity, as such the research also provides some recommendations on how South Africa can strengthen its overall approach to cyber security.

ACKNOWLEGEMENTS

This research would not have been possible without the support of my department and supervisor, Mr Roland Henwood. Through Mr Henwood's guidance I was also able to better focus my argument and structure my research. He also greatly assisted in identifying gaps in the research and areas for improvement.

I am also thankful to the researchers at the CSIR who assisted me in sourcing journal articles that related specifically to South Africa. Craig Rosewarne, the managing director of Wolfpack, was also very helpful in providing information on the emerging trends that are occurring in the cyber domain.

A special word of thanks also goes to my brother Dominic Griffiths who assisted me in editing and structuring my thoughts. Finally, I would like to thank Caitlin Botha who consistently provided encouragement throughout the writing process and regularly sent me ideas to improve my research.

TABLE OF CONTENTS

ABBREVIATIONS/ACCRONYMS

APT	– Advanced Persistent Threats
ARPANET	– Advanced Research Projects Agency Network
ASGISA	– Accelerated and Shared Growth Initiative for South Africa
BDS	– Boycott Divestment and Sanctions
CERT	– Computer Emergency Response Team
CISRT	– Computer Incident Security Response Team
CNII	– Critical national information infrastructure
CRC	– Cyber Response Committee
CSIR	– Council for Scientific and Industrial Research
CSS	– Cyber Security Strategy
CSTB	– Computer Science and Telecommunications Board
DDoS	– Distributed denial of service
DNC	– Democratic National Committee
DoS	– Denial of service
DPCI	– Directorate for Priority Crime Investigation
ECT	– Electronic Communications and Transactions
EU	– European Union
FIRST	– Forum of Incident Response and Security Teams
GDP	– Gross domestic product
GEAR	– Growth, Employment and Redistribution
HIPSSA	– Harmonisation of Information and Communications Technology
ICISS	– International Commission on Intervention and State Sovereignty
ICT	– Information and communications technology
ISIS	– Islamic State of Syria and Iraq
ISP	– Internet Service Provider
ISS	– Institute of Security Studies
IT	– Information technology
JCPS	– Justice, Crime Prevention and Security Cluster
NATO	– North Atlantic Treaty Organisation

NCAC	– National Cyber Security Advisory Council
NCSPF	– National Cyber Security Policy Framework
NDP	– National Development Plan
NGO	– Non-governmental organisation
NGP	– New Growth Plan
NIA	– National Intelligence Agency
NSA	– National Security Agency
PALA	– Promotion of Access to Information Act
PLC	–Programmable logic controllers
RDP	–Reconstruction and Development Program
SADC	– Southern African Development Community
SAPS	– South African Police Service
SCADA	–Supervisory control and data acquisition
SQL	– Structured Query Language
SSA	– State Security Agency
UNDP	– United Nations Development Program
US	– United States
USA	– United States of America
WEF	–World Economic Forum

1. CHAPTER ONE – RESEARCH OVERVIEW

1.1 INTRODUCTION

Cyber security is an emerging challenge for national security for South Africa and countries across the world, as cyber attacks have become more advanced and frequent over the years. South Africa is considered to be one of the worst affected countries by cyber attacks in the world, costing the economy an estimated R5 billion a year (Fripp, 2014a). A number of the attacks have threatened major state institutions and actors. For example, in February 2015, leaked spy cables released by the news network Al-Jazeera highlighted that South Africa may have been directly threatened by Israel in June 2012. This came after it was reported that then finance minister Pravin Gordhan had received a hand-written note threatening a mass cyber attack unless action was taken against the Boycott Divestment and Sanctions (BDS) campaign (Sapa, 2015). In May 2014 another public sector cyber attack occurred targeting state infrastructure in South Africa when a suspected member of the hacktivist group, Anonymous, hacked the personal details of an estimated 16 000 whistle-blowers on the South African Police Service (SAPS) computer database. The hacker posted the details online and stated that the attack was in response to the 2012 Marikana shooting, in which police killed 34 miners during a strike. This type of hacking attack represents a major breach of security. Even more disturbing is that the attack directly targeted the computer systems of the country's police service (Roane, 2013).

Other large scale attacks conducted by criminals seeking financial gain have also been conducted in the country. In November 2014, the Directorate for Priority Crime Investigation made a number of arrests after attempts were made to hack into the Gautrain Management Agencies accounts, with an estimated R800 million at risk (Hosken, 2014). However, perhaps the most brazen cyber robbery targeting a state institution occurred in 2012, when the SA Post Office was robbed of R42 million after hackers were able to create a number of Postbank accounts from which they made a series of withdrawals. The attack was so serious that the country's National Intelligence Agency (NIA) had to investigate (Sapa, 2012).

Whatever the motivation or location of the hackers, these attacks have direct security, financial and personal consequences for South Africa and its citizens. Attacks against financial institutions such as banks and private business represent a direct threat not only to the country's economic security but also its national security, as they hamper economic growth. For instance in 2013, the estimated costs of cyber crime in the South African private sector came to R5.8 billion, which was 0.14% of the country's gross domestic product (GDP) (Fripp, 2014a). These cyber attacks also place businesses at risk and jeopardise the security of individuals, as attacks can lead to identity theft or the capture of personal information.

While states worldwide are finding cyber attacks as a serious challenge, South Africa is particularly vulnerable for several reasons. Over the last decade, the growth of internet connectivity in South Africa in relation to the rest of Africa has been rapid. In a study conducted by the World Wide Worx (a leader in internet and cell phone connectivity market research in South Africa), the number of broadband subscriptions in the country grew from 3.6 million in 2010 to 8.2 million in 2012. This is a growth rate of 128% (World Wide Worx, 2012). South Africa has a relatively sophisticated information and communications technology (ICT) sector. The country has two national fixed-line phone providers, five different mobile operations, and hundreds of internet service providers (ISPs). In 2009, South Africa had some of the highest internet bandwidth prices in the world because the country's bandwidth was driven by satellite and a single undersea cable. However, it is now connected to four undersea cables which have significantly lowered the price of broadband in the country and allowed for faster connectivity and increased access. These cables can transfer data of rates between 4.5 and 5.2 terabits per second (tbps). The South African government is also driving the development of ICT with the National Integrated ICT Policy Green Paper which is expected to enhance the introduction of e-government services (Gillwald, et al., 2012:16-19). This rapid growth has assisted the country in developing, but it has also opened South Africa up to a variety of new security challenges from the cyber environment. A report by Norton (2013), a global leader in antivirus software and cyber security, finds that in 2013 South Africa had the third-highest number of cyber-crime victims in the world. The majority of the attacks are conducted by hackers operating outside of the country, who enjoy access to faster internet and more advanced software (Fripp, 2014b).

Clearly, cyber security is becoming a growing issue in South Africa, across both the public and private sector, and needs to be properly understood in relation to the country's national security. All sectors of society including government, businesses, households and individuals, use the internet and its services, and proper attention must be paid by state security agencies to ensuring that the state and its people are protected against the threats that emerge from the country's increasing rates of internet connectivity. Rather than improving South Africa's cyber security, existing official documentation contributes to its weakness. The country has no official policy on cyber security and the National Cyber Security Policy Framework passed by the country's executive three years ago in 2012, was only released publicly late in November 2015. Not long after this the government then released the Cyber Security and Cyber Crimes bill in December 2015 for public comment. This is the country's first cyber related bill, but it has yet to be approved and this progress has taken a year. This is despite the State Security Minister stating in his 2015 budget speech that cyber security will be a top priority for the country.

Strategic policy documents similarly provide no concrete plans. In the South African National Development Plan (NDP), a policy document which aims to achieve a significant reduction in poverty and inequality by 2030, the internet is acknowledged as a major factor contributing to growth and innovation. To this end the policy acknowledges that South Africa cannot be caught in the "digital divide", by which is meant a space of inequality where citizens have limited or unreliable access to information communication and technology systems (ICT). Not only is the "digital divide" harmful to development but it also creates challenges for information security if rival states are becoming relatively more technologically advanced. In comparing South Africa's position to international standards, the NDP acknowledges that South Africa's ICT infrastructure is "abysmal" (National Development Plan, 2012:36), without stating precisely which components of this infrastructure are lacking; this vagueness in diagnosing the country's ICT weaknesses highlights the failure of the state in the management of vital infrastructure.

The NDP does mention the need for vast improvements such as the establishment of national, regional and municipal fibre-optic networks to provide better broadband access, but unfortunately the policy does not take cognisance of the need for enhanced cyber security through these developments (National Development Plan, 2012). The 2015 Defence Review similarly notes how security is now a broad, encompassing idea, such that national security includes the safety and security of South Africa's people – in other words, human security – and is key in maintaining the country's political and economic independence and protecting its institutions, values and freedoms (Defence Review Committee, 2015). Yet it only briefly mentions cyber security as a topic in focus, and fails to provide significant detail on what South Africa's approach to this security should be. As these examples demonstrate, although acknowledging the threat, the government has still failed to make any tangible effort aimed at strengthening South Africa's cyber security, a factor which will continue to put the country at risk of further attack.

It is clear, that when considering the growing frequency of cyber attacks both in South Africa and globally; the country's particular sensitivity to such attacks; and the lack of a well-developed cyber security policy from South Africa's government, that a thorough review is needed of where the country currently stands with regards to cyber security, and the importance of cyber security to South African national security. As such, this analysis aims to provide an exploratory study on cyber security as an emerging issue for South African national security.

1.2 FORMULATION AND DEMARCATION OF THE RESEARCH PROBLEM

The research focus this study addresses is how cyber security is an emerging and important challenge in South Africa. The study explores the following statements:

- Cyber security and its relevance to national security
- The types of threats present in the cyber space and the damages they can incur
- An assessment of South Africa's current approach to cyber security

By understanding the destructive and disruptive nature of well-coordinated cyber attacks, the research will show that cyber security is a pressing issue facing the national security of South Africa, particularly as various national institutions such as power stations, water delivery systems, finance institutions, transport systems, and government agencies, are heavily dependent on ICT technologies. A further aggravating factor will also be discussed, namely the South African government's failure to formulate an explicit and concerted approach to cyber security, as an integral part of its national security policy.

The study will highlight how cyber issues have come to be framed as security issues impacting national security. This will require exploring the key concepts associated with cyber security and an examination of four of the most public and destructive cyber attacks that have been conducted to date, namely the attack against the Estonian government in 2007, the Stuxnet computer worm that targeted Iran in 2010, the on-going case of five Chinese nationals who were charged in 2014 in the US for computer hacking and economic espionage across nuclear, metal and solar industries, and finally the hack that targeted the Democratic

National Committee. These examples aim to highlight how cyber attacks can be focused on state institutions and also target private sector actors, causing not only infrastructure damage but also economic damage.

Considering the above, the study is based on the following assumptions:

- Cyber attacks are growing in frequency, adapting and becoming more complex as the world advances technologically. With increased inter-connectedness between people, economies and governments, cyber threats are showing more prominence.
- South Africa's advancement in the development of ICT infrastructure has highlighted the prevalence of cyber security as a growing challenge to the country's national security.

The focus of this study is between the period 2000 to 2015 as this is when notable cyber attacks took place across the world. During this time South Africa also witnessed significant growth in its internet and ICT capabilities.

1.3 LITERATURE REVIEW

The goal of this literature review is to provide context to this study by evaluating the writings of leading theorists in the field of cyber security. The literature review is divided into four sections: exploring national security in relation to cyber security, a definition and short history of cyber security, cyber security attacks and their impact, and lastly cyber security in South Africa and cyber developments from around the world.

The study will examine how new threats like those presented by cyber attacks are changing the way theorists think about national security (Nye, 1999). A shift in the theorising of national security became necessary in the early 1990s, when the collapse of the Soviet Union caused transnational threats such as terrorism, civil wars, rogue states and insurgencies to rise in significance, and more traditional conceptualisations of national security to become obsolete. As traditionally understood by the school of realism, national security is state-centric, whereas more recent conceptualisations see it as a space in which states have seen their power and influence significantly reduced. This decrease in state control is particularly true in the cyber security environment. Given this change the research will seek to explore the definition of national security by theorists such as Goldman (2004), Sorensen (1990), and Zelikow (2003). This will be done in order to analyse how national security is often reevaulated particularly as new advancements are introduced in ICT. This is relevant when discussing South African national security later in the study and how it is impacted by ICT. This analysis will also examine how cyber security has changed the field of security studies and added to what is understood as the broadened security agenda. In doing so the research will examine Buzan and Waever's notion of securitsation (1998), that is, using methods such as government speeches and communications to prioritise certain issues and direct a security focus towards them. This notion of securitisation will be particularly useful for this research into South Africa and the country's approach to cyber security.

This study also requires an explicitly developed theoretical basis, so that the terms of the evaluation are clear. The emergence of the World Wide Web and the internet have necessitated the introduction of a range of new terms and phrases into our modern vocabulary, with which we aim to understand these increasing levels of connectivity. John Sheldon's *Strategy in the Contemporary World* (2013) assists in explaining ICT terminology as he examines the history of the term "cyber space", which first emerged in 1982. According to Sheldon (2013) the term cyber space was first coined in 1982 and yet the idea of cyber space began as far back as 1968 with the Advanced Research Projects Agency Network (ARPANET) (Singer & Friedman, 2014). There is no consensus on an agreed upon term for cyberspace although some such as Dorothy Denning (1999) suggest the best way to understand it is as "the sum total of all computer networks". The study will explore this definition and others such as those provided by Daniel Kuehl (2009) and the US Department of Defence (2013) as this will assist in unpacking the term in its entirety.

Sheldon (2013) also explores the notion of cyber power in relation to the other military domains such as land, air and naval power, and notes that the cyber environment favours the attacker. He argues that defenders cannot stop attacks from occurring, but rather can merely mitigate the worst effects. This characteristic of cyber power means that exactly what is meant by "cyber security" must be carefully unpacked. This will be critical in leading into the discussion on the rise of cyber security as a concept and how it can be seen across three different cyber spheres as identified by Helen Nissenbaum (2005). In describing the emergence of the term cyber security there are also various elements that go with it, such as the types of threats present in the cyber domain (for example worms or computer viruses). The writings of Derek Reveron (2012) give a strong basis for understanding the different types of threats as does the work of P.W. Singer and Allan Friedman (2014). Key within this discussion will also be to distinguish between cyber attacks conducted by criminals or hacktivists against states, cyber attacks conducted by states against states along with then exploring attacks which target individuals or companies and are aimed at financial gain.

Building on this sound exposition of current theory on cyber and national security, this study will then examine the nature of cyber threats in more detail by means of four different examples. The examples will be the cyber attacks on the Estonian government (Herzog, 2011), the Stuxnet worm which was embedded in an Iranian nuclear facility (Collins & McCombie, 2012; Farwell & Rohozinski, 2011), the ongoing damages incurred by the US due to Chinese hackers (Chon, 2015) and the hack that targeted the Democratic National Committee (Spector, 2016). These examples will demonstrate the destructive capacity of cyber attacks and the impact these attacks can have on critical national infrastructure in the public sector, along with the implications in relation to economic sabotage through the private sector, and the difficulty the government experiences in countering such attacks. These examples lead into analysing the notion of cyber weapons and how countries are developing advanced software capabilities to wage war with the click of a button. These international attacks provide valuable insights into the relevance of cyber security for South Africa, as considering the country's NDP goals with respect to ICT development and infrastructure, the threat of such attacks as an ongoing and increasing problem must be taken seriously.

To complement this discussion on international cyber attacks and further demonstrate the challenge of cyber security for South Africa this study will analyse some of the most public attacks that have been launched against South African entities over the last five years. Banking has been the most affected sector of the country, especially due to the increased popularity of internet banking. Government infrastructure has also come under attack, as hackers have attempted to capture confidential information from the South African Police Service (Roane, 2013). The research will examine existing studies on the cyber environment and cyber attacks in relation to South Africa's national security. It is important to note that such studies are few in number. The recent assessment by the Institute of Security Studies on South Africa's preparedness for cyberspace challenges will be discussed, the assessment includes a discussion by the South African Police Service (SAPS) Electronic Crime Unit on the prevalent threats facing the country (Institute for Security Studies, 2015). Another study of South Africa's cyber security was produced by Wolfpack, a leading cyber security firm in

South Africa. This assessment provides a comprehensive view of the major trends that can be expected in the cyber environment as South Africa moves forward, and examines the risks across three different sectors, namely finance, government, and telecommunications. It also highlights the likelihood of different internet attacks (Wolfpack, 2013). Similar impacts studies conducted by McAfee (2014), Norton (2013) and Kaspersky (2014) will also be consulted. The potential bias of these entities is noted as they do in fact sell cyber security software. However, the use of several specific findings in these reports is indicative of the lack of solid statistics available on the impact of cyber attacks in South Africa. Collectively the findings in all of these reports also emphasizes the concern around cyber security in South Africa.

The increasing threat presented by cyber attacks to South Africa's national security having been demonstrated, the final element of the study will be an overview of how the government is responding to this threat. Primary sources that will be used to define and explore South Africa's provisions for national security will include firstly the country's Constitution (Republic of South Africa, 1996) and the Defence Review (Defence Review Committee, 2015). The Defence Review gives insight into the most recent understanding of South Africa's national security, and is also valuable in that it identifies some of South Africa's cyber vulnerabilities and the types of challenges that South Africa must be aware of, such as attacks on critical infrastructure, and the manner in which the internet enables radical groups to fund themselves and recruit members. The country is particularly at risk as a developing nation, as often in developing states establishing ICT infrastructure is the priority, and ensuring protection against cyber attacks is a distant afterthought. As mentioned in the introduction, the South African government has admitted in its NDP that ICT infrastructure is "abysmal" (National Development Plan, 2012), while failing to explicitly state what elements are lacking. This is problematic as it suggests that the key element of cyber security has been overlooked in the country's future strategic planning. The NDP is thus the third significant primary document that will be discussed. The speech made in March 2014 by State Security Minister Siyabonga Cwele will also be examined, as it gave insight into how the country intends to proceed into the future regarding the development of cyber security (Cwele, 2014). This is one of the first major speeches made by a minister in which cyber attacks are discussed as an issue that needs proper securitisation. With the Cybercrime and Cybersecurity bill having been released for comment in November 2015, this will also be analysed in relation to the country's current cyber security position (Ministry of Justice and Correctional

Services, 2015). In terms of secondary sources, the writings of Hough, Du Plessis and Kruys (2007) about South African strategic and security perceptions will also provide insight into what the country's national security priorities have been since it became a democracy in 1994. Grobler, Jansen van Vuuren and Zaaiman (2013) also provide valuable insight into how prepared the country is with regards to cyber defences. The World Economic Forum Global Cyber Security Index (2015) will also be incorporated in this study as it deliver some key ideas for where South Africa could improve its cyber position.

The above mentioned sources will provide an essential context to the growing importance of cyber security in South Africa. However, literature which evaluates South Africa's current cyber security position and the country's general approach to cyber security is still in its early phases. It is in this regard that this research aims to contribute a more integrated analysis on how cyber security affects South Africa's national security.

1.4 RESEARCH METHODOLOGY

The understanding of cyber security as an emerging challenge to South African national security will be done through an exploratory study which will use a qualitative research approach, which combines two research methods. The first is desk research. Primary sources here will include government policy documents such as the National Development Plan (NDP), speeches by government ministers, the Defence Review, and the Constitution, the National Cyber Security Policy Framework along with the Cybercrimes and Cybersecurity bill. The second research method is an analytical and descriptive research approach which will explore some of the most publicly destructive cyber attacks that have taken place globally. This research will also explore some of the most public cyber attacks that have targeted South Africa directly. Together the desk research and the various examples of cyber attacks will provide a clear picture on the importance of cyber security to South African national security. As such it will be both a literature analysis but also include some comparative dimensions. The information from secondary sources on cyber security will be sourced from journal articles, academic papers and books, and contemporary news sites, along with specialised media which a focus on technology.

In evaluating this primary and secondary literature, this study will aim to demonstrate that cyber attack threats need to be considered far more seriously within South Africa's national security than they have been thus far. Cyber attacks directed at the financial sector are likely to incur large costs in the future, and will hamper economic development. Threats to critical infrastructure could also increase in frequency, and the deployment of cyber weapons is now also a reality, as countries across the world are using the internet as a way of gathering information on other nation states and even to disrupt their operations. South Africa is facing the predicament where the government is sporadically engaging with the public and the country's private sector over the importance of increased cyber security, but has been unable to effectively implement anything tangible. The lack of actual action is disturbing, as it suggests that the government is failing to address cyber security with the seriousness it deserves.

1.5 RESEARCH DESIGN

The research will be presented in five chapters, outlined as follows:

CHAPTER ONE – RESEARCH OVERVIEW

Chapter one will set out the research focus and research problem, and indicate the significance of the study by giving its context, namely the growing importance of cyber security in the theory and practice of national security. The chapter will also explain the need for research into cyber security in South Africa, provided that this is a relatively new field of study within security studies. The methodology of the study will be discussed, in its twin approaches of desk research and the use of comparative examples. This chapter will also provide the context for understanding why cyber security is so important for South Africa.

CHAPTER TWO – EXPLORING NATIONAL SECURITY AND CYBER SECURITY

Chapter two will provide a conceptualisation of national security and cyber security. Key aspects within this analysis will be examining the field of critical security studies and how cyber security has added to a broadening of security agendas and become a securitised issue. The notions of cyberspace and cyber power will also be discussed as they provide the backdrop under which cyber security falls. The chapter will explore the different types of cyber attacks that exist and why these are threats to national security, along with examining the concept of cyber weapons. This will lead into examining the cyber attacks that were directed against Estonia, Iran and the USA as these hold value in exploring how destructive cyber attacks can be and what lessons can be taken away from their impact.

CHAPTER THREE – CYBER SECURITY IN SOUTH AFRICA

Chapter three will assist in contextualising South Africa's cyber security position by analysing some of the most public attacks that have targeted the country. This will lead into an evaluation of a number of different research reports produced by leading think tanks and cyber security firms which highlight the total costs and scale of cyber attacks that have been directed against the country. Key policy documents which explain South Africa's national security will then be examined. This will ultimately lead into a discussion on the manner in which the country has gradually recgonised how cyber security has becoming increasingly relevant to national security.

CHAPTER FOUR – CYBER SECURITY DEVELOPMENTS IN SOUTH AFRICA AND THE REST OF THE WORLD

Chapter four will provide detail on South Africa's progress with regards to cyber security and highlight what legislation has been developed in order to deal with cyber matters. The chapter will also identify the country's weakness with regards to cyber security and provide possible strategies for the future. This will be assisted by examining some of the strategies from around the world which South Africa could choose to implement.

CHAPTER FIVE – CONCLUSION

Chapter five will conclude the study by summarising the research and emphasising how the study was conducted. This will lead into an explanation on how South Africa can improve its cyber security position along with identifying areas for future research.

2. CHAPTER TWO - EXPLORING NATIONAL SECURITY AND CYBER SECURITY

2.1 INTRODUCTION

The chapter will examine the notion of national security and explore how the traditional understanding of the term has changed since the end of the Cold War. This will also allow discussion on what is now a far broadened security agenda. Part of this discussion will highlight the role of the Copenhagen School and the theory of securitisation. Thereafter the chapter will briefly discuss the history of cyber space and highlight how the term "cyber security" emerged within the field of security studies. The study will also explore the various definitions and key terms that are attached to the cyber environment and cyber security. Subsequently the research will then explore the notion of securitisation within cyber space and discuss the different forms that a cyber attack can take and the different manners in which they can threaten infrastructure. The chapter will unpack four examples of cyber attacks namely those in Estonia, the Stuxnet worm in Iran, the continued infringements by Chinese hackers against American infrastructure and the hack targeting the Democratic National Committee. This will seek to highlight the destructive and hampering capabilities that a coordinated cyber assault can have on state infrastructure or democratic processes and the implications of such assaults.

2.2 UNDERSTANDING NATIONAL SECURITY

For Emily Goldman (2004:45) national interests play a vital role in national security because "national security, whether understood as a process or as an objective, refers to the protection of core national interests from external threats". According to Goldman there is little argument over what can be defined as a states' key national interest, because these interests are generally highly stable and the only way they are likely to change is if a state is able to increase its power significantly. For example, in Goldman's case a national interest such as survival would be a constant (2004:45). Hans Morgenthau (2005) held similar views where he argued that national interest was often focused around survival and involved the protecting of physical, political and cultural identities from other state encroachments. Morgenthau believed interest could only be defined in terms of power, defining interest in this manner thus allowed you to get a better understanding of how states could be expected to act as their interests will be constrained by the power they demonstrate in world politics i.e. military, diplomatic and economic power (2005:2).

Thus in conceptualising national security a key component in understanding the term is the notion of national interest. Joseph Nye (1999:23) defines national interest within a democracy as "the set of shared priorities regarding relations with the rest of the world". This includes key values that relate to human rights such as freedom, democracy and justice, matters that the public considers to be important to their identity and to society as a whole. Donald Nuechterlein's (1976:247) interpretation of national interest states that "it is the perceived needs and desires of one sovereign state in relation to other operating states comprising the external environment. Both Nuechterlein and Nye share similar views in that they understand national interest as the manner in which states navigate their interactions with the rest of the world. While Nye's approach is more value based and Nuechterlein's includes the notion of perception, between both theorists the following can be deduced. National interest is a way in which states guide their interactions with the rest of the world to ensure their continued survival and development. Thus, a state's national interest is shaped by a number of factors such as the key values or ideas present within society, its political system along with the actual power and influence that a state may have.

Both Nye and Nuechterlein's views on the national interest were shaped during the Cold War. However since the end of the Cold War, debates surrounding national security and how it is understood have had to deal with the fact that the world underwent a fundamental change within the realm of international security. Theodore Sorensen (1990:6-7) identifies this by exploring how the USA rethought national security after there was a change in global power relations with the collapse of the Soviet Union at the end of the Cold War. Sorensen points out how in the case of the USA there was a temptation to try and include every national interest as part of the country's national security. However, this must be avoided because not every foreign action that affects the population's psyche requires state action. In deciphering how to frame national security, Sorensen (1990:6-7) argued that states have to consider "what kind of world, in the next decade and beyond would best protect our values and strengths". This is important because it speaks to how states need to constantly re-evaluate their national security based on their current historical context. The type of threats facing a state may change and societies may evolve through technological change. States may need to adjust their views on national security in order to adapt to these changes. None is truer than in the case of cyber security which has forced states to confront the fact that they can face a threat from unknown sources operating in a foreign country.

Sorensen's view flows into the discussions developed by Phillip Zelikow (2003:19-25) who suggests that national security is a term that needs to be examined through a number of different lenses. First he looks at how national security has changed in relation to geography, traditionally it involved territories and physical armies, today the frontiers are totally different because they can be found everywhere. Borders have been broken down and the information age has created unparalleled access into state activity. The integration of Europe is a good example of this as countries have relinquished certain aspects of their sovereignty in order to better align their development and integration. The North Atlantic Treaty Organisation (NATO) has also experienced significant advancements as member states are constantly sharing important security information. Zelikow also examines national security as a function of time, for in the past, threats were often slow to emerge and easier to identify as tactical decisions such as mass conscription could be seen or an increase in weapons production monitored. However, now the nature of the threats is changing, they can emerge quickly without the need to accumulate a mass of men or weapons. These two ideas that Zelikow identifies are particularly relevant to the realm of cyber security as technological advancements can lead to rapid changes in the cyber domain (Zelikow, 2003:19-25).

Another important element which has changed the way in which countries think about national security relates to the emergence of the concept of "human security". The concept of human security was largely advanced by the United Nations through the 1994 Human Development Program (UNDP). The UNDP (1994:23-24) defined human security as "first, safety from such chronic threats as hunger, disease and repression. And second it means protection from sudden and hurtful disruptions in the patterns of daily like – whether in homes, in jobs or in communities. Such threats can exist at all levels of national income and development." The UNDP (1994:23-24) goes further in describing that human security is the condition of safety from seven categories, economic security, food security, health security, environmental security, personal security, community security and political security. This is captured through two core tenets namely "freedom from fear and freedom from want". The notion of human security further contributed to the idea of the broadened security agenda and this move away from a realist focus on territorial and state security to an emphasis on people's security. In this sense, overall human welfare is considered to be a guiding factor when it comes to human security. The UNDP (1994: 22) acknowledges that security has been defined too narrowly and thus states that "it has been related more to nation states then to people". As such the focus should now be on the individual as the referent object and not the state.

A key link that was made in terms of applying human security to national security came from the 2001 Responsibility to Protect report produced by the International Commission on Intervention and State Sovereignty (ICISS). The ICISS (2001:12-15) makes this link because it relates state sovereignty with the role of a states' responsibility to protect its citizens as a security provider. In this way the report argues that security can be expressed internally towards the citizenry but also iterates that it involves a commitment to the international community and to the United Nations as an organisation. As such should a state be in such a position where it can no longer protect its citizens then that responsibility falls on the international community to intervene (ICISS, 2001:12-13). However, it is important to note that while there is agreement that the individual should be the focus of security policy, there is constant debate on exactly what threats should be included as part of threatening human security. In his writings on critical human security studies, Edward Newman (2010:82) labels human security as "normatively attractive, but analytically weak". He questions the effectiveness of human security in contributing to policy because it is so broad and can allow for any threat to life to be characterised as a security threat. In this way the concept becomes so broad that it can ultimately become "meaningless" (Newman, 2010:82). The other challenge with human security is that it is very difficult to respond to these criticisms by then arbitrarily trying to create criteria in which you classify what is considered a human security threat and what is not. However, despite its critics, human security has allowed renewed focus in terms of how states consider national security. This is also particularly important in relation to the cyber realm as cyber attacks can often be directed towards individuals and threaten their own personal security. Later in the research the study will also highlight how the notion of human security has influenced South Africa's national security after 1994.

Considering the different definitions presented the concept of national security can be summarised as follows. National security is focused on protecting the core or prioritised national interests of a state or advancing a specific interest. These interests can be unique to different states and are defined by key values that inform how a state identifies itself to the global community. National interest can also be constrained by the level of power that a state possess in the global arena as this will determine how effective it is in driving its agenda. When thinking about national security, it is a dynamic term which requires constant revision as it is informed by the present historical context. The focus of national security is also being influenced by arguments which advocate for more of a human centred approach in thinking about security issues. As such, national security can change and evolve as societies develop and undergo changes in their preferences and views on politics.

2.3 SECURITY STUDIES AND THE COPENHAGEN SCHOOL

Within the field of security studies, the traditional approach to understanding national security was always state centric. The state is the highest form of authority and the anarchic nature of the international system often meant that wars or conflict were an inherent feature of the international system. However, this paradigm was centered mainly around the global system as it was structured during the Cold War. With the end of the Cold War there was a gradual change that emerged in terms of thinking about security studies, as the narrow state centric way of viewing the world was too static and lead to criticisms in how security had always been traditionally understood. It is within this realm of critical security studies that understanding the role of cyber security can be best interpreted (Buzan, et al., 1998).

Critical security studies is underpinned by three key ideas. The first is the notion of security as a “derivative concept” (Peoples & Vaughan-Williams, 2010:22). This is the view that security and how one understands security is dependent on one’s understanding of the world and personal interpretation of politics. It is these views which will determine what someone considers to be a threat and what protection is required to counter that threat. Within the context of this study it is critical to understand this, because it highlights security as a relative term. For example, someone from a rural area with limited access to information technology will interpret the notion of cyber security very differently to someone in an urban area operating in an environment where they are heavily dependent on network computing and technology. The second component of critical security studies is that of the broadened security agenda. Traditionally, the role of the military has always been viewed as the primary point of departure in understanding potential threats. However, since the end of the Cold War this entire notion has changed. The security agenda is no longer restricted to just that of the military but now encompasses a wide spectrum that takes into account environment, economic, political and societal factors which could emerge onto the security agenda. This is particularly relevant for cyber security, because although it some cases cyber operations can be led by militaries, they can also be led by criminal syndicates, terrorists, organisations or individuals driven by their own individual agendas. Finally, the last defining component in critical security studies is the view that the individual is the referent object, in contrast to the traditional view as the state being the central tenant. As such the theory behind critical security studies works from the basis that when one considers threats, they must be considered in relation to individual people, because these individuals are ultimately what constitute a state (Peoples & Vaughan-Williams, 2010:22-23).

One of the leading schools of thought in acknowledging the role of the broadened security agenda has been the Copenhagen school and authors such as Barry Buzan and Ole Waever (1998). Their work holds particular importance when thinking about cyber security because their focus is not on objectively trying to classify what is a threat or a vulnerability but rather, what conditions or state of affairs need to be initiated by specific actors in order for an action to emerge as a threat. This is what is known as the process of securitization and it is the procedure by which the theorists can determine what should and what should not be defined as a security issue. It is important to note that it works from the basis that there is a broadened security agenda and it is because of this widened scope that there is a need to be able to distinguish what should actually be classified as a security threat. Thus as aligned with critical security studies the Copenhagen school moves away from the traditional view that a threat needs to be militarily based, or that the referent object is always the state. (Buzan, et al., 1998:25-30).

In this movement away from a threat having a military component to a more general interpretation, the Copenhagen school retains a key feature of the notion of a threat, which is that a threat must be dire and existential. “Thus the exact definition and criteria of securitization is constituted by the intersubjective establishment of an existential threat with a saliency sufficient to have substantial political effects” (Buzan, et al., 1998:28). The importance of this definition is that an issue must be framed to have serious political consequences. However, the other vital component is that a threat must be accepted by an audience as fatal to a particular referent object and in need of an actionable approach. For example in the case of a state, a securitised threat would place national sovereignty or political autonomy at risk. Representing a threat towards a collective such as society in general involves demonstrating how it could jeopardise key aspects of a societal identity (Nissenbaum, 2005:66).

Buzan et al (1998:25) argue that security "frames the issue either as a special kind of politics or as above politics". This introduces what is known as the spectrum of securitisation. Initially an issue would be non-politicised, suggesting that the state has no interest in dealing with it nor is it a matter particularly high on the public agenda. Thereafter it can become politicised whereby it becomes part of public policy and requires some form of governmental decision making and public engagement. Finally an issue can be securitised, in which case it is no longer a matter that is up for debate but has been allocated a high priority with a requirement for urgent action (Hansen & Nissenbaum, 2009).

The other key element attached to the securitisation process is that discussions around the topics must be led by a securitising actor. This is an actor who is in an actual position of authority and has sufficient social and political influence to convince an audience of the existence of a particular threat through a speech act where they discuss the threat's severity. In many cases it can be led by a senior member of government, a security expert, a leader in industry, or military leaders. Without the sufficient influence attached to your person, the process of securitisation is unlikely to be successful. This is why some actors are more successful than others in raising concern about a particular issue. However, it is also a fluid process as the influence of a specific actor can rise or fall as it is dependent on the public perceptions of their ability at the time (Peoples & Vaughan-Williams, 2010:79).

To summarise these findings, the process of securitising a particular activity is to highlight that it is an imminent and existential threat to a certain collective. It is a process which is enhanced if it is led by a known securitising actor who is acknowledged to have strong influence over that particular collective.

2.4 DEFINING CYBERSPACE

Within the realm of security studies there is still significant debate over the definition of cyberspace. The aim within the field is to attempt to create uniformity in the definition so that it can relate to other key definitions such as land, sea, air or space power. The challenge in defining cyberspace is that what we see today as cyberspace is fundamentally different to what was experienced when it was first created (Sheldon, 2013). The idea of cyberspace began when the United States Department of Defence started the early computing networks which became known as the Advanced Research Projects Agency Network (ARPANET) in

1968. This was later the network which underpinned the internet. However, since 1968 there have been repeated attempts to provide a definition for cyber space as the term's meaning has gradually expanded over time (Singer & Friedman, 2014:13). In order to demonstrate the complexity of the term the study will present and then discuss three definitions.

In the latest attempt to define cyberspace, the Pentagon released the following definition:

> Cyberspace is the global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the internet, telecommunications networks, computer systems and embedded processors and controllers (US Department of Defence, 2013:2).

In *Information Warfare and Security*, Dorothy Denning (1999:22) defines it as "the information space consisting of the sum total of all computer networks". Lastly, a popular definition is the one provided by Daniel Kuehl (2009:28) stating that cyberspace is:

> A global domain within the information environment whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange, and exploit information via interdependent and interconnected networks using information-communication technologies.

In order to incorporate these ideas cyberspace can be defined as a virtual information environment where digital data can be stored, created and shared. However, it also comprises actual hardware such as the computers that store the data and the actual infrastructure that can connect these computers together such as fibre optic cables, mobile technologies, satellites and other elements that allow the systems to run. The notion of virtual space is important because while information within the cyber domain can be stored on physical hardware, it can also be held in a virtual non-physical space which is highly interconnected. As Denning (1999:22) defines it, it is this "sum total of all computer networks". Significantly cyberspace also comprises of a human element, the actual users behind the computers. This is important as it is human action which shapes cyberspace. Thus, when considering all these different elements it is easy to understand how cyberspace is constantly evolving because it is made up of this nexus of technology and human interaction which changes at a rapid rate.

2.5 THE RISE OF CYBERSECURITY

Cyber security as a concept only really emerged into the 1990s in the post-Cold War era as computer advances in technology began to have serious geopolitical consequences. Initially the term only highlighted the challenges facing networked computers and how hardware could be corrupted. Later it moved away from this technical understanding as scientists argued that the threats emerging through new technologies could be harnessed in such a way that they could have serious societal impact and cause direct harm to a state and its citizens. Helen Nissenbaum (2005:65) argues that cyber-security is a term which is often used by government authorities, policy makers and corporate leaders and it attempts to make the link between computer security and national security. In order to better understand the realm to which cyber security applies, Nissenbaum defines the concept across three different categories (2005:65).

The first category is what Nissenbaum identifies as “the use of networked computers as a medium or staging ground for antisocial, disruptive or dangerous organisations and communications” (2005:66). This would include hate or racial groups, criminal syndicates who use websites to try and conduct illegal activities (usually fraud) along with terrorist organisations who use the internet for coordinating possible attacks. The second category Nissenbaum identifies are “threats of attack on critical societal infrastructures, including utilities, banking, government administration, education, healthcare, manufacturing and communications media” (2005:66). In this case, because these systems are highly dependent on network infrastructure they are particularly vulnerable. The final category is broad based and examines “threats to the networked information system itself” (2005:66), this ranges from attacks which aim to disable systems or completely compromise them and cause loss of revenue, to the theft of intellectual property or even loss of life.

Thus cyber security clearly involves technical computer security but it is also broader in that it crosses into the realm of national security because attacks could have a direct impact on state infrastructure. From a human security perspective it can also then have a direct impact on individual citizens. These points will be further explored in analysing the role cyber security within the field of security studies.

2.6 SECURITISING CYBER-SPACE

In order to understand cyber space as being securitised it requires an understanding of what the term “security” means within the context of computer security. In the US Computer Science and Telecommunications Board’s (CSTB) (1991) report titled *Computers at Risk: Safe Computing in the Information Age,* security is defined as “the protection against unwarranted disclosure, modification, or destruction of data in a system and also the safeguarding of systems themselves.” The report also highlights that security is comprised of human elements along with administrative, physical facility and procedural components. However, this focus on the technical aspects of computer security makes a difficult concept to securitise. The challenge is that the discourse is largely driven by computer scientists who see computer security as a concept which centers around the development of software and programs that assists in preventing disruption to computer networks from malware, bugs, viruses or direct access from outside hackers.

The securitising element comes in the way in which computer security has involved as concept to become known as cyber security. Cyber security represents the nexus where the technical aspects of computer security are incorporated within a broader understanding of national security. As such cyber security is computer security plus securitisation.

One of the defining ways in which cyber security attaches to the broadened security agenda, is examining how the term relates to the referent object as defined within the context of critical security studies. As has already been discussed, the Copenhagen school acknowledges that the broadened security agenda is a space where the referent object does not necessarily have to be the state. This is particularly relevant in understanding cyber security because cyber attacks can end up targeting a variety of different referent objects, in fact because of the dynamic nature of cyber space the referent object that is under attack can change rapidly based on the type of threat experienced. For example, cyber attacks can target individuals in their personal capacity through theft of data, they can go after intellectual property from a major corporation or try to steal funds. They can also directly target the state and try to disrupt state operations or shut down critical national infrastructure. However, in understanding the nature of cyber attacks there is value in discussing the different types of attacks that can be orchestrated.

2.7 IDENTIFYING THE TOOLS USED IN CYBER ATTACKS AND THE ACTORS THAT MAY DEPLOY THEM

Cyber attackers have a diversity of tools at their disposal which can be deployed to disrupt, damage computer systems or capture confidential information. Highly sophisticated cyber attacks will often utilise a variety of different tools in order to maximise their effectiveness.

Phishing is one of the most common terms associated with cyber security. Phishing usually occurs via an email which takes on the appearance of official correspondence from a trusted source such as a bank, employer or a known entity. The aim is to redirect the user to a website where they then enter account details or hand over personal data unknowingly, this can then be used by the initiators of the attack to attempt to defraud you or use or details for a criminal purpose. Thus attackers bait or "phish" for a users' confidential information. Attackers can take it a step further by doing a targeted "spear phishing" attack which involves gaining prior knowledge about an individual before then trying to capture their details (Singer & Friedman, 2014:39-41). Another type of attack with similar goals to phishing is known as a Structured Query Language (SQL) injection which is a common way in which websites and companies are attacked. SQL is a programming language which assists in the management of data and is often used to store and capture information. Attackers will, instead of entering the requested personal details on a website chose to enter specific command codes which allow them access to the website's database as a whole. Essentially the computer has interpreted the data as an actual instruction and in doing so, compromised itself. The access can be so far reaching that it allows an attacker to take control of an entire web service (Singer & Friedman, 2014:42-45).

Attackers have also designed malware which is malicious software that aims to target a specific vulnerability in a computer. These are referred to as viruses or worms and they often have detailed instructions attached to them which guide them through a system that has been compromised. Computer viruses embed themselves in a particular file by making a copy of themselves. They then prevent files from being able to execute properly. Viruses generally require some kind of human involvement or interaction (unknowingly) in order to replicate. Worms operate independently and are able to replicate themselves as they move from one computer system to another and don't require human involvement. They spread across a network of computers often overwhelming IT infrastructure as they can attempt to replicate files and slow down computer functions. Some worms are designed to capture personal data while others are designed to focus on destroying data on a target's computer. A Trojan horse refers to computer software that has been designed to conceal harmful code. It hides itself as a useful program and then activates when a user unwittingly executes a particular aspect of the software and begins hampering computer systems. Spyware, refers to a type of malware which is designed to track and monitor a computer user's data and send it on to an unauthorised third party (Sharma, 2010:46-47).

The use of malware becomes layered as attackers can sometimes seek to create an army of computers by creating networks of compromised "zombie" computers which can be used to coordinate an operation on a target. This is what is referred to as botnets and it can allow millions of machines to be controlled by a single user. Botnets are commonly used for distributed denial of service (DDoS) attacks which aim to attack the systems that allow connection to the internet (Singer & Friedman, 2014:39-45). It is based on the fact that data transfers consume computational and bandwidth resources. As such it is a way in which whole systems become overwhelmed and ultimately crash. The ability to block a single attacker is easy, however trying to stop millions is impossible, as the attacks often involve a number of computers they are generally hard to trace. This means they can often be used as a diversion in some cases while attackers have a more targeted attack they want to take place (Singer & Friedman, 2014:39-45). It is important to make the distinction between a Denial of Service (DoS) attack and a Distributed Denial of Service (DDoS) attacks. A DoS attack refers to an attack where a single user attempts to disrupt a connection while a DDoS attack refers to a coordinated attack from a distributed system of computers (Sharma, 2010):46.

The explanations highlighted above aim to demonstrate the different tools available to cyber attackers who are looking to try and compromise a system. One of the key concerns which has shaped cyber security in relation to national security has been how cyber attacks can threaten or disrupt critical national infrastructure. These state entities represent a high value to potential attackers because if their systems are compromised they can cause wide spread harm. The base worst case scenario for such attacks is that hackers would launch a computer virus which targets a country's national energy regulator's mainframe. The attack would lead to a root compromise which occurs when the virus allows the hacker access to the main administration settings of the computer mainframe. Once this is achieved hackers can run their own programs, change how the system works and then also try and hide traces of their intrusion. Particular malware can also be deployed which follows a predefined set of instructions once the mainframe has been compromised. Once disrupted the attack would likely result in blackouts in selected areas in the country, communications systems would fail and company switchboards and computer systems would be offline. Security systems across the country would switch to battery modes and then ultimately run themselves down when the power remains off. This would then compromise the security of actual physical structures in the black out affected areas and could then lead to instances of theft, further damage and possible panic until security is restored (Grobler & Jansen van Vuuren, 2012:64).

One of the key elements of ICT is the fact that it can be globally accessible and with the diffusion of computer skills around the world, various communities are now are becoming computer proficient. The challenge is that some of these communities direct their skills in a malicious manner. What follows is a brief breakdown of the forms in which these communities might appear.

2.7.1 CYBER TERRORISM

Jonalan Brickey (2012:1) defines cyber terrorism as “the use of cyber capabilities to conduct enabling, disruptive, and destructive militant operations in cyberspace to create and exploit fear through violence or the threat of violence in the pursuit of political change”. Cyber terrorism can be used to recruit or radicalise individuals, provide training, channel commands and financing, along with the conducting of actual terror operations. Critical infrastructure systems such as government services, transport, energy infrastructure and major financial services are prominent targets for attacks because if they are compromised the damage can be far reaching. In operations against the terrorist organisation Al-Qaeda, US authorities discovered that the terrorist group had been engaged in cyber operations which allowed them to gain knowledge on the stress weaknesses in key infrastructure such as bridges and dams in the US (Rudner, 2013:453-460). With the gradual decline of Al-Qaeda and the emergence of the Islamic State of Syria and Iraq (ISIS) there has a strong resurgence in the use of cyber terrorism. The group has actively used the internet as a recruiting ground and as a means to distribute anti-Western propaganda, while also encouraging its followers to target people in their home countries. The most public attack by the group came in January 2015 when they hacked the Twitter and YouTube accounts of the US Central Military Command. The group had the statement “I love you ISIS” depicted across the pages and sent out pictures of US personnel and military documents to possibly demonstrate that they had infiltrated US military establishments. The attack resembled more of a cyber type graffiti tagging than anything else, however it highlighted the group's growing cyber capabilities and brazen tactics. The more capable ISIS becomes in the cyber environment the more likely they are to try and use the cyber environment to launch large scale cyber attacks (Graham-Harrison, 2015).

2.7.2 STATE SPONSORED CYBER TERRORISM

The challenge with cyber terrorism is that it is not just necessarily a terrorist organisation on the other side of the computer. In some cases they are being actively supported by a country in their operations. This can be through the provision of technical support or by merely allowing a particular group the ability to operate within the state's borders with impunity. In some cases terrorist cells may share a similar agenda to a particular state and as such are willing to act as proxies for that state. State backed hackers are a growing concern as not only are they very hard to track but they are equally hard to prosecute if they are operating with the support of a government. State sponsored terrorist attacks are often known as Advanced Persistent Threats (APT) because they take the form of a continuous barrage against computer systems. APT attacks aim to navigate and map information on critical control systems in infrastructure such as power stations, energy grids, financial networks and transportation networks. These attacks can compromise these systems and then allow the attackers a chance to copy or steal information about their design or operating procedures. Attackers can often leave malware in place that can remain dormant and then be deployed to destroy or damage the systems at a later date. The attacks on Estonia and the Stuxnet worm are two of the most public displays of APT attacks where state sponsored proxies were suspected to have been involved, both of these cases will be covered later in the chapter (Rudner, 2013:460-463).

2.7.3 HACKTIVISM

An increasingly popular movement within the cyber world is the notion of hacktivism. The name derives from the words "hack" which is generally used to describe the use of cyber-technology to attack a computer system and the word "activism" which involves bringing social or political change. Hacktivism is commonly carried by organisations or individuals who operated in informally structured groups held together by a particular philosophy or shared set of values. These groups are not motivated by financial or criminal gain, but use their cyber skills to attract attention to a particular cause or injustice that they have identified. The most established group in the world is *Anonymous* who have claimed responsibility for a number of cyber attacks on high profile institutions. In 2010 in the wake of WikiLeaks and the distribution of thousands of classified documents and diplomatic cables, Anonymous hacked and disabled the online payment system PayPal after the company stopped processing donations for WikiLeaks. The group also shut down the New York Stock Exchange during the Occupy Wall Street demonstrations. In November 2012 *Anonymous* along with a number of collaborators launched a full scale assault on the Israeli government and private sector websites in the country with millions of different cyber attacks in protest against the country's "Operation Pillar of Defence" as it responded to rocket fire from Gaza. As a community, hacktivists have demonstrated that they are quite capable of organising sophisticated attacks against state infrastructure (Rudner, 2013:463-467).

2.7.4 INSIDER THREATS

Insider threats are considered to be cyber attacks which emerge due to an action committed by a staff member of the workforce who is employed or operates in a specific company or government entity. These can often be carried out by disgruntled personnel due to disagreements over a particular policy or business action. Insider threats can have significant consequences because the staff behind them could have access to key information or intricate knowledge of an entity's network infrastructure. A highly public example was that of the WikiLeaks exposure of the military operations in Iraq. This was due to the access that US soldier Chelsea Manning had to classified intelligence databases. In 2010 Manning released thousands of classified documents detailing US military activities to WikiLeaks which the organisation then distributed to the public. A similar intelligence leak took place in 2013, this time by Edward Snowden who worked for the National Security Agency (NSA). Snowden released documents which unpacked the global surveillance collaboration between the US, the UK, Australia, Canada and New Zealand, commonly referred to as the Five Eyes alliance. The defining feature of the leak was the invasion of privacy and level of spying that the US was conducting on its own citizens. The leak was an embarrassment to US authorities as it showed that they accessed email accounts, instant messaging and even developed the ability to harvest call records and map the location of cellphones. It has been defined as one of the country's biggest security leaks (Rudner, 2013:467-469).

2.8 STATES GOING ON THE OFFENSIVE: CYBER WEAPONS

Although the analysis has detailed the way in which many non-state actors operate in the cyber sphere, a critical component is how states engage in the cyber environment and understand how it can be used as an instrument of war. This is in particular reference to the development of cyber weapons. There is no universally accepted definition for the term cyber weapon but it can basically be understood as a computer code that is designed with the aim to threaten or cause physical damage or harm to structures, systems or even humans themselves. In thinking about cyber weapons there is also an element of asymmetrical strategy attached to their use, because the more technically advanced a state is, the more likely it is going to be a target for attack. Hence in the cyber environment, the very aspects that make a state dominant in terms of cyber capabilities such as advanced software and hardware, make it vulnerable to attack as well. Despite this, major powers around the world have acknowledged the importance of being able to project their cyber capabilities globally.

In China, the country's military have placed the responsibility for defensive and offensive cyber operations under one authority, the People's Liberation Army (PLA). In offensive operations the PLA's goal is to disrupt a rival state's ability to process and collect information. Part of China's strategy even underscores the potential that well-orchestrated cyber attacks have in disrupting financial institutions. In fact, an element of Chinese doctrine concerning cyber security is that active offence is a key component in disrupting an adversary's capabilities (Sharma, 2010:36-44). Russian military approaches in thinking about cyber weapons share similarities with the Chinese, however they also acknowledge the role that they can play in influencing the consciousness of a nation's people. For the Russians a critical component in cyber weapons is that they can be used to control information and this can be incredibly useful in relation to psychological applications in influencing a population (Darczewska, 2014). In the United States, the Joint Publication on Information Operations clearly acknowledges the role of cyber weapons in stating that:

> Information operations (which include computer network operations) are designed to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting our own (US Department of Defense, 2012).

With this acknowledgement on the role of cyber weapons as a form of military tool, many countries have undertaken the development of specialist teams and units which are tasked primarily with cyber defence and offence within the military. Although the deployment of such capabilities is very hard to trace there have been a number of high profile incidents over the last decade where state involvement has been suspected.

The study will now highlight a number of examples which aim to demonstrate the destructive and hampering capabilities of cyber attacks and the debates that have emerged as a result.

2.8.1 2007 ESTONIAN ATTACKS

On April 30, 2007 the Estonian government decided to move a statue from the Soviet period known as the Bronze Soldier from its location in Tõnismägi Park in central Tallinn to the Tallinn Military Cemetery. The decision sparked rioting among the country's ethnic Russian minority who took to the streets to express their outrage. Tensions between Estonia and Russia have existed for decades, as during the Cold War the Soviet Union settled thousands of Russians in Estonia in the hope it would bring the two nations closer together and align elements of Estonian culture to Russian values. However, with the end of the Cold War, Estonia rapidly moved away from Russia. Estonia soon opted to focus on its integration into Europe, joining the North Atlantic Treaty Organisation (NATO) and the European Union (EU) in 2004. The decision to move the statue sparked unrest not only from Russians based in Estonian but across the country's border in Russian territory as well. It resulted in a mass distributed denial-of-service attack which targeted infrastructure, government ministries, major banks and political parties (Herzog, 2011:50).

Estonia has always prided itself on its advanced information communication technologies and in 2007 it was one of the most advanced states in the world with regards to internet connectivity. In discussing the country's IT capabilities the head of IT security at its defence ministry stated that Estonia is heavily dependent on the internet because the country has a "paperless government" (BBC, 2007). In 2007, 60% of the country's population used the internet on a daily basis and an estimated 97% of all banking transactions occurred online. Critical infrastructure such as electronic networks, power grids, water delivery systems and banking services are heavily dependent on the internet. The attackers shut down the parliamentary website and then closed off the IT abilities of several key government ministries which severely hampered the Estonian government's ability to respond and communicate on the attacks. In targeting the banking industry, the attackers were able to prevent credit card and ATM transactions from occurring and hamper financial flows. Many of the attacks were orchestrated through the use of botnets of zombie computers which had been hijacked by the attackers in countries such as Egypt, Russia and even the United States. They were employed in a swarm DDoS attack and ultimately websites such as government ministries which were used to receiving 1000 hits a day, suddenly experienced 2000 hits a second which lead to them crashing and going offline (Herzog, 2011:49-55).

Tracing the attacks proved incredibly difficult and although the Estonian government made a number of in country arrests, it was suspected that the majority of the attackers were based abroad. Suspicion was soon cast on Russia, although the Kremlin denied any involvement. While NATO could not find any hard evidence that the Russian government had been involved, many within the alliance felt that the coordination behind the attacks suggested that it had definitely been a concentrated effort from highly trained hackers with some form of state backing. Estonia was so unprepared for the attack that the government Computer Emergency Response Team (CERT) had to get assistance from Finnish, German, Israeli and Slovenian teams in order to restore the operations that had been taken offline (Ruus, 2008:5-8).

The attack on Estonia sent shockwaves across the international community, particularly in Europe as it demonstrated how easy it was for individuals to interfere in the operations of a state from the comfort of their own home. It lead to a number of debates within NATO over the level of preparedness for cyber attacks within the alliance and resulted in the creation of key policies relating to cyber defence and the centralising of defensive operations across the organisation. Despite the damage done by the cyber attacks, they could have been significantly worst. The hackers could have gone after water supply systems, electrical grids, air traffic control electronics or even military systems. The attack highlighted the manner in which states tend to pursue technological advancement without taking care to properly secure their integration into new systems and create the right levels of security infrastructure. In Estonia's case, the country's well developed internet and network infrastructure also made it a very easy target for hackers who were intent on creating chaos.

2.8.2 STUXNET

In May 2010 an anti-virus company known as Virusblokada based in Belarus reported that they had found a troublesome computer worm after the company had been contracted to investigate a computer in Iran that had continuously started to reboot itself for no reason. The worm was also present in computer networks globally as well. The company discovered that the worm was significantly large in size and very complex, suggesting there had been a number of resources put into its development. The worm had begun infecting supervisory control and data acquisition (SCADA) systems in computers around the world, these are systems that monitor and run industrial processes. SCADA processes are used in a number of ways, such as in management and operation of power plants, electrical grids, water distribution and waste collection, oil and gas pipelines, railway transport, right to the packaging processes for sweets and chocolate. The company issued a global alert, warning the world of what would become the Stuxnet worm. It led to an international effort to track down the worm's source. Computer scientists from across the world cooperated in trying to decipher what vulnerabilities the worm was targeting and the systems that it had damaged as computers had been infected in a number of countries, from India to Finland to the USA. However, it soon became clear that the bulk of the infections, almost 60% were in Iran (Collins & McCombie, 2012:85-91).

As the computer scientists began to unravel Stuxnet the complexity of the malware soon came to the fore. Stuxnet had been equipped with four "zero days", a zero day represents a vulnerability that has not yet been identified by the creators of a particular piece of software. It is basically a security glitch within a piece of software. Generally, malware has only one zero day as hackers have to spend hours searching for a particular glitch in a piece of software that they can exploit. The fact that Stuxnet had four zero days suggested that significant resources had gone into its creation as it was designed to exploit multiple security vulnerabilities. Stuxnet was also programmed to work on all Windows operating systems right back to Windows 95 so that it could cover a vast spectrum of computer networks. In order to operate in the Windows operating system without raising any suspicion, Stuxnet also used two legitimate digital signatures which had been stolen from two companies operating in Taiwan. This is what allowed the malware to move through the Windows operating system and give it the ability to act as a trusted entity without the threat of detection (Farwell & Rohozinski, 2011:23-35).

Aside from the advanced programing behind Stuxnet, what was most striking about the malware was that it hunted for a target purpose. Stuxnet was designed to access a specific program used in Siemens WinCC/PCS 7 SCADA control systems. If the malware did not detect this program to be present on a particular computer it would basically shut itself down. The worm would also not try and spread to as many computers as possible but was aimed to target no more than three at a time in order to control its growth and prevent detection. However, the targeting of Stuxnet soon became even more specific, as the malware unravelled it was shown that it was going after a very specific controller, those used in nuclear centrifuges. It was very precise about the centrifuges as well, they were of a certain size and number (984) and had to be linked together. They were also only found in the Natanza nuclear facility which was a suspected site of Iran's nuclear weapons program. Once in the system Stuxnet went after the programmable logic controllers (PLCs) which are the computers that control key electrical functions such as switches, relays or timers. In doing so the malware was able to manipulate the adjustments for the centrifuges used in the enrichment of uranium. It would make small adjustments to the pressure inside the centrifuges to destabilise them over time. The worm would alter the speed of their rotors causing them to slow down and speed up at different rates to throw off their synch, and then sometimes it would even push the motors to above their maximum speeds to cause lasting damage. This process would not only prevent the centrifuges from producing refined uranium but it would also lead to frequent breakdowns and result in the machines spinning out of control until they destroyed themselves (Farwell & Rohozinski, 2011:23-35).

The malware was so effective that it operated within the Iranian centrifuges for over a year. It was also able to remain undetected because the Iranian computers were air-gripped so they were effectively disconnected from the Internet. Thus it was suspected that Stuxnet was introduced into the computer network via a USB drive which allowed it to spread through the nuclear facility's computer network before then going out into the Internet. The complexity and level of development involved in Stuxnet suggested to many within the international community that it was not the work of everyday hackers or cyber criminals. In a US senate hearing on the malware, it was estimated that around 10 000 man hours went into its production and it would have required the skills of people who were not only experts in Microsoft operating systems but also incredibly knowledgeable on the computer languages that govern computer networks. It was also huge, with 15 000 lines of code and an estimated 4 000 different functions (Collins & McCombie, 2012:85-91).

Stuxnet's deployment against Iranian centrifuges challenged a number of beliefs held about computer systems and the information environment. It highlighted how operating systems like SCADA which are often isolated and disconnected from the global internet are still very much at risk due to their own internal networks. It also showed for the first time how the cyber environment can be used as a space where actual physical infrastructure can be destroyed, and yet this can be done without any loss of human life. In Iran's case it was estimated the country's nuclear program was ultimately set back by two years. While Estonia suffered from DDoS attacks which succeeded in overwhelming its online systems, Stuxnet demonstrated an evolution in the way cyber tools can be deployed. It showed the destructive capability that stealthily designed and expertly engineered malware can have on critical infrastructure. Another element which raised concern was the manner in which the malware became a global phenomenon. Although its damage was mainly centered in Iran once it had spread through the country's computer networks it started appearing elsewhere in the world with dominant presences in India and Indonesia. In addressing the US Senate hearing, Senator Susan Collins highlighted that if malware similar to Stuxnet targeted a transformer in the US power grid it could result in severe blackouts in the country and threaten national security or lead to the capture of vital state information, this is highlighted in the next example (US Senate, 2010).

2.8.3 CYBER ESPIONAGE AND SPYING: A GROWING TREND

Aside from the attacks against Estonia and the deployment of Stuxnet as a cyber weapon, over the course of the last decade there has been a increase in what is deemed as cyber espionage. In May 2014 the United States Department of Justice charged five Chinese military hackers for cyber espionage. It was the first time the charges were laid against confirmed state actors for hacking. The investigation showed that the Chinese nationals had conspired to hack into key American industries in nuclear power, coal power and metals. The hackers intended to steal information that would be useful to companies back in China, particularly the country's state owned entities. The indictment showed that they had also stolen sensitive internal communications documents which provided the details on the business strategies and challenges facing some of the American entities. The hackers also proved to be members of China's cyber division within the People's Liberation Army known as Unit 61398. It had taken the US authorities years to track them down and it is believed that the group had been in operation from 2006 till when they were indicted in 2014 (US Department of Justice, 2014).

However, one year after Attorney General Eric Holder presented the case to the world, the five hackers have still not appeared in a US court room because China will not extradite them. The case has hurt diplomatic relations between the US and China and has also failed to deter the ongoing attacks against US firms and infrastructure (Chon, 2015). In fact since in the indictment, Chinese hackers have changed their strategy and introduced new software tools and malware that they use to target the US. US agencies have also reported that they deal with thousands of attacks a day which originate from China. The US government has now responded by creating legislation that would allow the country to actually sanction Chinese companies which receive information via hacking. By closing these companies out of the key financial flows in US markets it is hoped that they will act as an effective deterrence method against future hacking (Groll, 2015).

Despite this, cyber espionage between the US and China continues to be an issue hampering relations between the two states. In September 2015 the leaders of the two countries came to an agreement that they would refrain from the utilisation of cyber attacks to steal intellectual property or trade secrets. Unfortunately the very next day after the agreement, the US reported that a number of technology and pharmaceutical companies had come under repeated attack from hackers based in China. Three weeks since the agreement, cyber attacks continued to take place against US companies. The attacks have not only highlighted the difficulty involved in enforcing agreements between states when it comes to cyber security but also illustrated that states are often genuinely unwilling to obey the agreements due to a lack of trust. For instance in the National Security Agency (NSA) leaks by Edward Snowden, it showed that the US had once hacked Huawei over fears that Huawei's networking infrastructure in the US had been compromised by the Chinese government. Huawei is a Chinese technology firm and one of its biggest revenue streams comes from the installation of servers that form the backbone of a company's internet connectivity. US authorities were concerned that these servers could provide a "backdoor" to the Chinese government to monitor communications or capture sensitive information on corporate activity in the US. (Mozur, 2015).

2.8.4 CYBER ATTACK AGAINST THE DEMOCRATIC NATIONAL COMMITTEE

While maintaining the cyber security of company secrets, corporate activity and confidential information has always been a priority, in 2016 a new type of motive emerged behind a cyber attack which targeted the US. On 22 July 2016, over 20 000 emails which had been exchanged by members of the Democratic National Committee (DNC) were released to the public by Wikileaks. This was done just days before the Democratic Party would have its national conventional where Hillary Clinton was chosen as the party's candidate for the presidential elections. Then on 12 August, a hacker named "Guccifer 2.0" followed up on the DNC emails by releasing the personal cellphone numbers and email addresses of over 200 US lawmakers. The DNC later confirmed that they were made aware that their systems had been hacked in April 2016 and that the hackers had likely had access to their data for almost a year (Parlapiano, 2016).

The hack significantly damaged the integrity of the DNC as the emails showed clear favouritism by DNC staff members towards Hillary Clinton. There were even conversations which discussed what efforts could be used to undermine her Democratic opponent, Bernie Sanders. The emails also revealed how fund-raisers had tried to request favours after they gave donations. The leak resulted in the resignation of the DNC chairperson Representative Debbie Wasserman Schultz and three other top Democratic Party officials. It also led to unrest in the Democratic Party and resulted in protests from Bernie Sanders supporters at the convention (Parlapiano, 2016).

Those responsible for the attack are still not publicly known, however an internal investigation lead by Crowdstrike traced the attack back to two groups associated with Russian intelligence. The strategy behind the hack remains unclear, but supporters of Hillary Clinton have come to the fore stating that they believe the attack was carried out to drive support to Donald Trump, the Republican presidential candidate. Trump is reportedly more pro-Putin than Clinton who is considered to be more of a tough adversary for Russia. However, what is clear is that the hack and the subsequent email leak were aimed at creating some kind of disunity within the Democratic Party and was definitely an attempt to interfere in the democratic process surrounding the country's election (Keane, 2016). Attacks of this nature are disturbing because they suggest that a foreign party tried to somehow influence the outcome of the US Presidential election. Susan Hennessey (2016) believes that "There is significant evidence that individuals acting at the direction of or on the behalf of Russia – the degree of co-ordination is unclear – are attempting to use organisational doxing to influence the United States presidential election." The hack also raises concern regarding the integrity and security of the election results for the national election later this year. Another concern is whether a country like the US acknowledges that the systems that political parties use in their election campaigns can be considered to be critical infrastructure as they form an integral role of the country's democracy. If this is the case then the hack on the DNC could even be viewed as a cyberwar incursion (Spector, 2016).

2.9 SUMMARY

In summary, the research in this chapter has sought to provide a strong overview on the cyber environment and national security. The goal has been to provide a theoretical understanding of what is meant by the term cyber space and a brief exploration of how the term is challenging to define as cyber space continues to expand with advances in modern technology. This has followed into a discussion on national security and how the term has evolved since the end of the Cold War. Part of this has been exploring critical security studies and how the broadened security agenda now includes a variety of factors which can threaten different referent objects. Core within this analysis has been the role of securitisation and how the Copenhagen school understands the way in which new threats can emerge within the security discourse.

Within this analysis the study has also sought to highlight how the term cyber security represents the nexus of computer security and national security. Hence, cyber security is a way of acknowledging that cyber threats and attacks can have very real consequences towards states, companies or even individuals. The chapter has highlighted the different types of tools that cyber attackers have in their arsenal and the manner in which these tools are deployed to disrupt operations. This analysis has then linked to the different types of communities that may engage in cyber attacks.

Finally the chapter has provided brief discussions on the most public cyber attacks that have shaped discussions within the cyber community. The cyber attacks against Estonia triggered a massive response in the way in which states think about cyber defence and their vulnerabilities, while the deployment of Stuxnet against Iranian centrifuges demonstrated the actual physical damage that can be accomplished through a well-coordinated cyber attack. The ongoing skirmishes by Chinese hackers against US entities is a continuous matter being reported on in the media. It highlights the complexities states have in enforcing regulations regarding cyber security agreements and the distinctive lack of trust that characterises the entire environment. The hack that targeted the DNC also then illustrated how attacks can deviate from being about some form of corporate gain but can focus on a direct attempt to undermine democracy.

3 CHAPTER THREE – CYBER SECURITY IN SOUTH AFRICA

3.1 INTRODUCTION

In the previous chapter the foundation was laid for understanding the theoretical base behind terms such as national security and cyber security. It provided clarity on the different forms of cyber attack and analysed a number of international examples of destructive cyber attacks. This has assisted in contextualising the study and providing a framework for this next chapter that will focus on how cyber issues are framed in South Africa and discuss their impact on the country's national security. This study will examine some of the most public cyber attacks that have been launched against South Africa and analyse how leading cyber security companies and think tanks have framed the country's current cyber security position. This will lead into a discussion on the development of South Africa's national security position since becoming a democracy in 1994. This will then assist in evaluating how matters concerning cyber security have gradually been introduced into policy discussions concerning South Africa's national security.

3.2 CYBER ATTACKS IN SOUTH AFRICA

A damning example of an information security breach in South Africa occurred in February 2015 when the news agency Al-Jazeera announced that it was in possession of a number of classified spy cables that had been leaked to the company. It is suspected that the leak is likely to have come from a source within the South African State Security Agency (SSA) which is particularly troubling. The documents contained reports filed by field operatives, and gave critical evidence on a number of challenges facing South African intelligence operations. The leaked information provided details on areas where the country was vulnerable to foreign spies. The spy cables stated that SSA agents had tracked 140 foreign operatives, suspected of trying to steal military plans and hack computers for blueprints. The cables reported that South Africa had "experienced the theft of Rooivalk Helicopter Blueprints by a known foreign intelligence service". The Rooivalk is the most advanced attack helicopter in the country's military and is recognised globally as one of the best combat helicopters in the world (Sapa, 2015).

The person responsible for the spy cables leak was never publicly identified so it is hard to decipher whether the documents were themselves hacked, or an insider source leaked sensitive information to the media, as was highlighted in chapter two. Regardless of how the leak occurred, it was a major breach of cyber security in South Africa, particularly as it emanated from the country's national state intelligence agency, considered part of critical national infrastructure.

In 2014 a second South African security agency faced embarrassment after a security breach at the South Africa Police Service (SAPS). The SAPS website was hacked by a suspected member of the hactivist group *Anonymous*. The hacker was able to download 15 000 lines of personal data on whistleblowers who were assisting the police. This information was then reproduced on another website and made available to the public. The hacker stated that the attack was motivated by the government's lack of action in arresting the police officers who were involved in the Marikana shooting that took place in August 2012 (Roane, 2013). The hack exposed a severe flaw in online data management by the SAPS and highlighted how state security actors have failed to adequately secure their data.

South African security services have also demonstrated their ability to prevent cyber attacks. In 2014 a plot was uncovered to steal R800 million from the Gautrain Management Agency. This attack was an insider threat because it was planned by an ex-employee with knowledge of the Gautrain's financial management systems. The attacker used specialised software to manipulate the system in an attempt to access banking details and passwords. The attack was discovered after a routine audit on the company's financial system which identified a breach in the computer system. The attacker was arrested through joint collaboration between the Gautrain management and the Police Directorate for Priority Crime Investigation (DPCI) (Hosken, 2014).

A cyber attack on state infrastructure in South Africa occurred in 2012 when a cyber crime syndicate stole R42 million from Postbank, a financial services provider that is part of the SA Post Office. The country's National Intelligence Agency (NIA – now known as the State Security Agency) was required to investigate how the systems at Postbank were compromised, as it is a state institution. During the investigation the NIA used the services of a private auditing firm and a forensic risk management company. The use of external companies highlights the lack of relevant skills present in the government when it comes to dealing with cyber crime (Chauke, 2012). Postbank holds over R4 billion in deposits and is responsible for distributing social security payments to South Africans across the country.

The theft of this large sum of money, particularly money from the government, is a matter of major national concern and speaks to the challenges relating to cyber security in the country (Sapa, 2012). This was an example of a direct attack on state infrastructure as Postbank is not only responsible for administering the payment of social grants but also provides other valuable financial services to millions of South Africans.

South Africa has not only been targeted by cyber attacks aimed at state institutions, the country has also grappled with terrorist organisations trying to recruit its citizens. The use of the internet has been a tool which has been employed by terrorist organisations to recruit members from around the globe. This is a key method which the Islamic State of Syria and Iraq (ISIS) used to expand its following. The group maintains an active presence on social media and uses its fighters and supporters to spread propaganda and actively recruit new members. The organisation has managed to extract either pledges of support or allegiance from over 30 jihadist groups across the world (Stack, 2015). The group has used social media to encourage its supporters to carry out acts of terror in Europe and the USA. For instance, on 14 July 2016, a Tunisian national living in France drove a 19-ton truck across the promenade in Nice during Bastille Day celebrations, killing over 80 people. A few days after the attack an Afghan teenager went on a rampage in a train in Germany with an axe and knife, wounding four people before he was shot by police. The media has initially reported on these attacks as conducted by "lone wolves", but upon closer inspection authorities have discovered that the attackers had links to ISIS or affiliated cells through their digital interactions. They had been receiving orders or advice from the group via the internet (Gartenstein-Ross & Barr, 2016).

South Africa is part of the globally connected community and the country forms part of ISIS's potential recruitment arena. The terrorist organisation has used digital communication to engage with supporters in South Africa. In April 2015, a 15 year old girl was prevented from boarding a plane at OR Tambo International Airport. She was travelling to Turkey and it was suspected that she intended to join ISIS. She intended to join the group after a number of internet exchanges. After this incident, the country's State Security Minister David Mahlobo announced that local security agencies were monitoring cyberspace and in particular social media platforms to track ISIS recruiters who may be targeting South Africans (Wakeford, 2015). Despite state security actively trying to prevent terrorist recruitment, the news agency Al-Jazeera later reported that at least 23 South Africans had joined ISIS after online recruitment (Patel, 2015).

The use of the internet for the recruitment and radicalising of new members to terrorist groups is of increasing concern in South Africa. During July 2016 two brothers were arrested in Johannesburg after intelligence exposed their ties to ISIS and their plans to bomb the USA embassy in Pretoria, along with Jewish institutions in the country. A raid on their house by the Directorate for Priority Crime Investigation uncovered that they were in possession of grenades and ammunition and had maintained online communication with ISIS. The brothers later appeared in court and were charged with conspiracy and incitement to commit the crime of terrorism (Pijoos, 2016). South African security services were able to stop the pair before they acted on their plans. This event highlights how the digital space can be used by organisations such as ISIS to encourage and assist terrorists in planning and actioning attacks.

The above discussion has provided a breakdown on the most high profile cyber attacks that have taken place in South Africa. In many cases attacks are not reported as companies or organisations will not publicly admit the losses incurred or concede that their security procedures failed. The same is true for attacks on state institutions. Attacks that make it into the public space have often been leaked to the media. The examples discussed above provide insight into the numerous vulnerabilities facing South African national security. The country has suffered financial effects, had confidential state information compromised and seen its citizens recruited to join terrorist organisations. These have occurred either through criminal acts aimed at personal gain or they have been aimed directly at undermining state institutions. Collectively they undermine the country’s ability to secure its people and its sovereignty through their impact on national security. A challenge facing South Africa is that the country’s progress towards developing tangible initiatives to actively counter cyber attacks has been slow and made it more vulnerable. This is further developed in the following section which highlights how much damage is being caused by cyber attacks to the country.

3.3 CYBER SECURITY AS A GROWING CONCERN IN SOUTH AFRICA

The previous section highlighted some of the major cyber attacks targeting South Africa and provided the context for an analysis on the total scale and costs that cyber attacks incur on the country. South Africa has not experienced the extensive damage caused by cyber attacks as reviewed in chapter two but the country is still considered a prime target for cyber attacks. This argument will be presented through the use of recent research reports which explore the costs of cyber attacks to the South African economy. It is important to note that much of this research has come from corporate entities that operate in the cyber sphere, and are responsible for the sale of computer software. Although they have a corporate interest in cyber security, they are also best placed for tracking out the costs of cyber attacks. Unfortunately in South Africa the government has yet to produce any research report which fully details the effects and costs of cyber attacks in the country. The next section presents statistics and research from a number of different companies and institutions which collectively demonstrate that cyber attacks are a significant challenge to the country.

A leading cyber security company in South Africa, Wolfpack, provided a comprehensive analysis on the state of South Africa's cyber security for the period 2012 -2013. The report contains valuable insights for understanding the cyber environment in the country. Wolfpack's analysis identified that denial of service (DoS) attacks proved to be the most common attacks that are targeting the finance, governmental and telecommunications sectors. Theft of information was also a prominent concern, as a breach of sensitive information on business decisions and security protocols could have potentially devastating consequences. The most targeted services are global credit card and financial networks along with e-commerce sites. There is concern that critical infrastructure will be increasingly at risk which could lead to massive traffic disruptions, telecommunications failing or even power outages (Wolfpack, 2013:36).

Research conducted by the SAPS Electronic Crime Unit (ECU), through the Institute of Security Studies, shows that cyber attacks are often transnational and planned by organised criminal syndicates operating abroad. This presents difficulties in tracking and arresting criminals as they are able to operate in foreign countries with near impunity. There are also challenges in securing digital evidence as mistakes are often made early on in the investigations where evidence can be overlooked or even mistakenly deleted. A lack of technical skills in areas such as forensic cyber investigations and cryptography is a contributing factor to these mistakes. Prosecution relies heavily on international cooperation which can often be difficult to secure and time consuming. Another factor which is hampering the ability to trace cyber attacks is that many attacks go unreported, or in a number of cases, victims were unaware that their computer systems have been compromised (Institute for Security Studies, 2015).

In 2013 the global computer antivirus company Norton released a report which examined the levels of cybercrime in 24 countries. The report found that in the sample set of countries an average of 61% of adults had experienced some form of cyber crime. For South Africa the report showed that this number was 73%. South Africa emerged as the third worst affected country by cyber crimes, Russia was first and China came in second. South Africa's ranking in this report has even been acknowledged by the country's government in the National Cyber Security Policy Framework (Justice, Crime preventation and Security Cluster, 2011:13). Norton showed that the estimated global cost of cyber crimes was US$113 billion over a 12 month period. In South Africa alone it was estimated to have cost the country US$337 million. Overall South Africa incurred 30% of the total costs of cyber crime out of the 24 different countries (Norton, 2013).

McAfee, considered to be the world's largest security technology company, also published a report where the firm estimated that the costs of cybercrime in South Africa are higher than Norton's estimate, putting the number at US$550 million. This is about R5.8 billion in local currency and around 0.14% of the country's total gross domestic product (GDP). McAfee considers a variety of consequences from cyber attacks which sees the company calculating a bigger cost. In McAfee's case the company includes financial impacts on the country's performance and the nation's economy. The report showed that globally the largest contributor to financial losses from cyber crime related to the theft of research and intellectual property. This significantly slows down the rate of innovation and impacts on the return for investors. The second biggest loss is from financial theft where credit card information or bank details are jeopardised by hackers. This includes attempts to hack into banking systems directly to siphon off funds. McAfee states that these particular crimes are driven by well trained groups who are conducting financial crime on an almost industrial scale. The theft of confidential business information is the third biggest driver in terms of financial crime. This involves hackers attempting to gain access to sensitive business material such as pricing strategies, investment information, competitor analysis and exploration data. It is the information that businesses use to conduct their operations at a senior level and the compromising of this information can significantly set back business decisions (McAfee, 2014).

Kaspersky, a Russian based cyber security firm and the fourth largest vendor in the world of IT security software, also regularly releases reports on cyber security trends. In the first quarter of 2014 the company reported that 49 million different cyber attacks and malware infections had been detected in Africa. Of that, an estimated 4.6 million attacks were directed at South Africa, which was 10% of the African continent's total number (Kaspersky, 2014).

In a separate research report compiled in November 2015, Kaspersky indicated that cyber attacks in South Africa had more than tripled. The firm recorded 25 million attacks in 2014 and 81.6 million attacks in 2015. The company believes that the rapid increase in the number of attacks is likely due to the growing number of South Africans that have gained internet access. South Africa is also seen as a soft target for cyber attacks due to the lack of cyber security in the country (Alfreds, 2015a). Kaspersky warned that in 2016 attacks are likely to be further diversified and advanced, particularly with the growth of smart phone usage. Cyber attacks are likely to change form where they no longer focus on stealthily penetrating a network but will now be encrypted with malware that actively destroys any evidence of an attack. Attacks will be faster and harder to detect as hackers make further advancements in the development of software that can compromise not only computer networks but smartphone and tablet devices (Avenant, 2015).

Another factor that needs to be included in this discussion is the role of the commercial sector, particularly the banking sector when it comes to cyber security. Cyber security is considered to be one of the top concerns for South African banks according to the 2015 Deloitte Banking Outlook report. Local banks are forced to invest heavily in safeguards in order to protect their services (Dirk, 2015). A challenge facing South Africa is that there is no legislation in place that forces businesses to disclose when they are targeted in a cyber attack. Banks will try and avoid engaging or publishing information on the prevalence of individual cyber attacks because it could cause concern among customers. In some cases such a disclosure is unavoidable if the losses are too great. This occurred with Standard Bank in May 2016 when it emerged that a hacking syndicate stole R300-million from the bank through a series of fraudulent transactions carried out in Japan. Although Standard Bank stated that they were quick to respond and contain the matter, they have still not provided the public with an update on whether the perpetrators have been brought to justice (Mamabolo, 2016). This lack of disclosure surrounding cyber attacks, particularly in the commercial sector, makes it difficult to truly measure cyber threats or allow for proper coordination in terms of solutions.

The reports released by Wolfpack, the Institute of Security Studies, McAfee, Norton and Kaspersky demonstrate the concern regarding the increased prevalance of cyber attacks directed against South Africa. Collectively their research shows that cyber attacks are a significant challenge in South Africa and highlights the growing need to enhance cyber security.

The above section which analysed the scale of cyber attacks in the country combined with the previous section which traced out some of the most public cyber attacks that have targeted the country have provided the context to examine South Africa's cyber security position. Now the research will turn to analysing the development of South Africa's national security since 1994 and thereafter explore how cyber security has gradually been introduced into national security discourse.

3.4 SOUTH AFRICA'S NATIONAL SECURITY

A key feature of South Africa's national security is that it has not been framed by any single defining policy document. Instead the country's national security since 1994 has been shaped by various policy documents. In Chapter 11 of the South African constitution, national security is not defined explicitly, but rather four key principles are highlighted which are expected to govern the country's national security. These are as follows (Constitution of the Republic of South Africa, 1996: Chapter 11 section 198):

a) 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.
b) The resolve to live in peace and harmony precludes any South African citizen from participating in armed conflict, nationally or internationally, except as, provided for in terms of the constitution or national legislation
c) National security must be pursued in compliance with the law, including inter-. national law
d) National security is subject to the authority of Parliament and the national executive.

Although not explicity stated in the constitution it is important to note that one of the core tenets that has guided South Africa's national security since 1994 has been the concept of human security. The ideas surrounding human security can be seen and reflected in the constitution as captured by point a) above. Esterhuyse (2016:44) argues that since 1994 the country made "a deliberate effort to institutionalise the human security agenda as the primary security paradigm for thinking about defence and security in the South Africa military". This was aimed at trying to demilitarise the country's society and promote the government's project of reconcilliation from 1994 onwards.

The inclusion of human security as a principle in the country's national security emerged prominently in the 1994 White Paper on Intelligence, which was adopted by the country's first democratically elected parliament. The policy reflected that, traditionally, security had always been seen in a narrow focus with an emphasis on military threats. It was noted that internationally the security agenda was changing with the growing influence of political, economic, social, religious and technological factors. "Security is conceived as a holistic phenomenon and incorprates political, social, economic and environmental issues. The objectives of security policy go beyond achieving an absence of war to encompass the pursuit of democracy, sustainable economic development and social justice" (South African government, 1994). The White Paper on Defence which was adopted in 1996 further emphasized this point stating that "security is an all-encompassing condition in which individual citizens live in freedom, peace and safety; particpate fully in the process of governance; enjoy the protection of fundamental rights; have access to resources and the basic necessities of life; and inhabit an environment which is not detrimental to their health and well-being". The policy went a step further in stating that South Africa's national security "is no longer viewed as a predominantly military and police problem. It has been broadened to incorporate political, economic, social and environmental matters. At the heart of this new approach is a paramount concern with the security of people". As such human security was a defining tenet for the country's defence framework (South African government, 1996).

Both of the above mentioned documents were also created within the context of the Reconstruction and Development Program (RDP). The RDP was South Africa's growth plan to guide the country forward after becoming a democracy in 1994. One of the core principles in the RDP was that it must be a "people-driven process" in that it will focus on serving the immediate and long-term needs of South Africa's people (Reconstruction and Development Program, 1994:8). In doing so the policy aimed to create an active citizenry. The RDP also identified poverty as the most important challenge facing the country. The role of peace and security were basic requirements in order to effectively counter poverty. The document also stated that in providing peace and security for all, the country's security forces must be "non-partisan, professional and uphold the Constitution and respect human rights" (Reconstruction and Development Program, 1994:8). Through this the policy advocated for nation building which creates "respect, protects minorities and provides a process to accomdate those wishing to retain their cultural identity" (Reconstruction and Development Program, 1994:8). From the outset of democracy in 1994 it was clear that human security would play a defining role in shaping South Africa's national security.

In 1996 the government wanted to accelerate economic growth so from a policy perspective the country's priorities then also evolved as the RDP was replaced by the Growth, Employment and Redistribution (GEAR) strategy. This policy focused primarily on changing the economy to generate formal employment and facilitating the redistribution of income. GEAR's objectives were never fully met and so in 2006 the government introduced the Accelerated and Shared Growth Initiative for South Africa (AsgiSA). The focus of AsgiSA was a goal of economic growth that averages 4.5% between 2006 and 2009 and then a sustainable growth rate of 6% between 2010 and 2014. The aim was to halve poverty and unemployment in the country by 2014. AsgiSA was then later replaced by a different economic policy, the New Growth Plan (NGP) which was introduced in 2010 and was also aimed at reducing poverty. Finally, government choose to introduce the National Development Plan (NDP) which would be the framework guiding development until 2030. The reason these policies are mentioned is because after the RDP, a people centred or human security based approach was always taken by the government in terms of thinking about development. Thus fighting to eradicate poverty aligned with the human security notion of freedom from want which is considered to be a key component of the country's national security (Bhorat, et al., 2014).

Sandy Africa (2015:183) has argued that although entrenching human security from a policy perspective, South Africa has had a mixed record in terms of actually achieving its people centred goals in practical terms. She argues that the country has struggled to find the "proper balance between security and development" and has not stayed true to the notion of making the individual the referent object. She has criticised the government for the manner in which it readily deploys the security apparatus and coercive powers of the state to deal with socio-economic challenges in the country. Abel Esterhuyse (2016:45) has echoed similar sentiments where he has stated that the emphasis on human security in South Africa has created unpredictability within the security apparatus. The broad interpretation of the term human security, he believes, has resulted in it being used as a way to reinforce "regime security" (2015:45). He goes further in stating that in not having properly interpreted how the term human security should be operationalised in a practical sense, the government has undermined its defence capabilities (2015:45).

The criticisms from Africa and Esterhuyse are important because they demonstrate how South Africa has deviated from the notion of human security. Both authors argue that the government has increased its focus more towards regime security in the way in which the security powers of the state have been deployed. This links into why cyber security is a challenge for South African national security in that it is not taken seriously, because the government has been focusing its priorities on ensuring the security and stability of its rule over the country. This emphasises a theme which reoccurs throughout this study in that South Africa lacks a clear direction with regards to cyber security.

Aside from the country's growth policies, a more recent document which explicitly describes South African national security is the Defence Review. The Defence Review is a document which is authored by a group of people from both military and civilian backgrounds. Submissions are taken from different military experts and debated, before ultimately it is submitted to the government for approval. The goal of the document is to provide a basis for government to plot the way forward on the future of the country's defence force. The most recent review was approved by the country's parliament in June 2015 (Stupart, 2015). The Defence Review is important in this study because it is one of the most current and few documents which has directly referenced cyber security as a matter which is relevant to national security.

The 2015 Defence Review starts with its basis as the constitution for guidance in defining South Africa's national security. The document builds on the constitution in noting that addressing the causes of insecurity will in turn promote an environment which is conducive to human development. The Defence Review maintains the need for a people-centred approach when it comes to thinking about security in South Africa, as was discussed earlier in the various economic and growth policies. The Defence Review notes that the role of a strong and capable developmental state is a core feature in maintaining national security. This is broken down across three 'Ps', namely people, the planet and prosperity (Defence Review Committee (2015:94). The Defence Review promotes the idea that national security aims to promote well-being and development in the country in order to free people from fear or want, in similar notion to what was stated in Chapter 11 section 198 from the South African constitution. The protection of the planet is also critical as the natural environment must be sustained in order for future generations to prosper. The notion of prosperity is also important as achieving prosperity is critical to unlocking potential not only in South Africa, but also in the Southern African region and the continent as a whole (Defence Review Committee, 2015). Considering the points highlighted above, the Defence Review goes on to provide a strong definition for framing the country's national security:

> South Africa's national security focuses on the interrelated priorities of national sovereignty, territorial integrity, constitutional order, the security and continuance of national institutions, the well-being, prosperity and upliftment of the South African people, the growth of the economy and demonstratable good governance (Defence Review Committee, 2015: 3-5)

Thus to summarise, South Africa's national security is based on core values and ideals drawn from the country's constitution which have then been further advanced by other policy documents as analysed above. Since becoming a democracy in 1994 the country has also moved to a more people and human driven national security approach, which aims to preserve the country's unique way of life. With South Africa's transition from Apartheid, the country emerged as a beacon of peace and reconcilliaton. These are two core values which have further advanced the notion of human security as a key feature of national security. The application of human security to South Africa's national security has also faced scrutiny as sometimes it seems to be a concept in theory alone while in practice the government often directs more focus to regime security.

The central tenet and role of human security is critical to emphasise as in this research there are elements within the cyber environment which can often work towards directly undermining human security and thus threatening South African national security. South Africa's challenge has been that as cyber attacks have become more prominent in the last decade, the country has failed to demonstrate and identify the importance of cyber security in relation to national security. The Constitution, RDP, White papers on Defence and Intelligence although providing a strong basis on which one can understand South African national security were not used to communicate on the notion of cyber security. This is likely because at the time of their writing, cyber issues were not as prevalent as they are today. The importance of cyber security to South African national security is a critical element of this study as it remains under-estimated in terms of policy in the country.

3.5 EXPLORING CYBER SECURITY IN RELATION TO SOUTH AFRICA'S NATIONAL SECURITY

The South African Defence Review of 2015 is one of the few policy documents which provided a basic breakdown of how cyber threats could harm South African national security. The Defence Review acknowledges that cyber security should be a concern for all of South African society, given that the country has been affected by cyber attacks across a number of different spheres. The document demonstrates that these attacks can also be classified into one of four categories. The first is that of cyber espionage, which involves the gathering of information from a particular source without the permission of that source. This information is ultimately used for commercial gain, the practice is known colloquially as 'phishing' (see section 2.7 pg23 of this document). The second is cyber crime which involves the use of malware or viruses (see section 2.6 pg24) to gain unauthorised access to particular information, which is then duplicated or used to hamper the operations of a targeted system. This includes identity theft, computer related extortion, forgery and fraud. The third category is cyber warfare (see section 2.8 pg28), which is the focused attempt by states to conduct offensive cyber operations against another state or even a non-state actor such as a business or NGO. The final category is cyber terrorism (see section 2.7.1 pg25) which are actions taken by terrorists within the cyber environment, with the aim of disrupting state operations or causing harm to civilians (Defence Review Committee, 2015:2-18).

With South Africa's increasing reliance on ICT the country is becoming more vulnerable in terms of cyber attacks, given the lack of a robust cyber defence response/strategy. The most recent research into South Africa's internet growth was released in the Cisco Virtual

Networking Index in July 2015. This index is based on continual analysis and forecasts of the use of internet protocol networks world wide. The forecast for South Africa estimates that the country will grow from 15 million users in 2014 to 27 million users by 2019. Internet traffic is expected to grow by 44% in the same period (Alfreds, 2015b). One of the documents which addresses the country's ICT development is the National Development Plan (NDP). The NDP is South Africa's current guiding policy document which aims to reduce poverty and inequality in the country by 2030. It explains numerous objectives and projects that will need to be undertaken in order to achieve this goal such as the application of technological improvement to enhance the country's innovative edge.

"This ecosystem of digital networks, services, applications, content and devices, will be firmly integrated into the economic and social fabric of the country. Together, these broadband elements provide an enabling platform for economic enterprise, active citizenship and social engagement and innovation. It will connect public administration to the active citizen; promote economic growth; development and competitiveness; drive the creation of decent work; underpin nation-building and strengthen social cohesion; and support local, national and regional integration" (National Development Plan, 2012).

The NDP has identified that one of the hindrances to this goal is the high cost of broadband internet in the country. There is a need to strengthen the country's ICT environment in order to better faciliate access to technological improvement to strengthen the country's development for the future (National Development Plan, 23: 2012). Within this context the Department of Communications developed the policy known as 'South Africa Connect; Creating Opportunities, Ensuring Inclusion: South Africa's Broadband Policy' which in line with the NDP set out the department's 2020 vision. The aim is to provide 100% of South Africas access to broadband services at approximately 2.5% or less of the population's average monthly income (Department of Communications, 2013:15).

The NDP states plainly that compared with international standards, the state of ICT in South Africa is "abysmal" (2012:23). However, the NDP does not then detail what exact international standards are being referenced. There is no clarity on what exactly is "abysmal" as the policy does not provide any international benchmarks that the country should strive to achieve. The document also proposes the development of national, regional and municipal fibre optic lines to strengthen the country's broadband connectivity. The NDP as a policy document, does not make any mention of the cyber environment or the need to develop enhanced cyber capabilities. This is a matter which has been lacking in South African policy frameworks, because ensuring the security of information systems is just as important as the process whereby those systems are brought online. They should occur jointly and not on the basis where the security of those systems is an after thought. Even the South Africa Connect policy explained above barely makes mention of the need for cyber security development. In a 52 page document the policy merely states that "An effective and secure online experience is an important contributor to increased broadband uptake and usage by the general public" (Department of Communications, 2013:35). The document even goes a step further in stating that "the Electronic Communications and Transactions (ECT) Act, is over a decade old and needs to be aligned with this rapidly changing digital world in order to provide users with confidence to use services and products and thereby stimulate broadband use" (2013:24). In this sense the policy acknowledged that South Africa was falling behind when it comes to ICT development. However, despite this acknowledgement, the development of more up to date policy, particularly regarding cyber security was not given the priority it deserves. This has been a repeated challenge for the country in that development policies are created which aim to further connectivity in the country yet these are not linked to policies that focus on cyber security. This is problematic as it means the country takes a retrospective approach to cyber security and only considers the need for proper cyber defence after instititutions and citizens have been connected to the internet.

As was highlighted in chapter two, one of the ways in which a particular issue gains prominence is through the process of securitisation. A contributing factor to this process can be a speech act from an established security actor. One of the most prominent speech acts concerning cyber security and South Africa's ICT challenges was made by the country's previous Minister of State Security, Siyabonga Cwele, on 27 March 2014 to the University of the Witswatersrand School of Governance (Cwele, 2014). In his speech the minister highlighted the importance of ICT development for South Africa's growth and society, and the need to ensure that this development is adequately protected. He discussed the rise of cyber crime in South Africa and how the country is reportedly losing R1 billion a year due to financially driven cyber criminals often targeting the country's banks or e-commerce sector. He also discussed the non-financially motivated crimes that have targeted the country. Although not going into detail he states that the theft of intellectual property rights has been increasing in the country, as well as attacks directed at strategic South African installations.

These attacks likely originate from Asian countries although the minister was not specific as to which states in particular he considers responsible (Cwele, 2014).

Another significant document that Cwele discussed during this speech was the National Cyber Security Policy Framework (NCSPF) which was approved by the country's cabinet on 7 March 2012. Cwele (2014) emphasizes that the NCSPF highlights the need for a cyber security culture, the strengthening of intelligence, investigating and prosecuting capabilities, the protection of national critical infrastructure, the need for strong legal frameworks and the development of the capacity to secure the country's cyber space. Cwele's reference to the NCSPF is significant because the NCSPF is a guiding draft policy document that provides a framework agreed upon by the Justice, Crime Preventation and Security Cluster (JCPS) in the run-up to actively designing a cyber security policy for the country. The aim of the NCSPF is to offer a holistic approach to tackling cyber security in South Africa by capturing the role of all the major actors in the country, such as government, business, civil society, interest groups down to households. Notably, the NCSPF introduces the term 'national cybersecurity'. This is defined as "aspects of electronic information, data and media services that affect a country's security, economy and well being" (Justice, Crime prevention and Security Cluster, 10: 2011).

The NCSPF is a critical document in South Africa's cyber security journey because it shows that the government had identified the need to address cyber security concerns as far back as 2011 when the NCSPF was drafted. In March 2012 the country's cabinet announced that it had approved the NCSPF as a guiding document for policy development. However, progress since this event has been slow as the document was only released into the public domain in 2015. Nonetheless, there are a number of key matters addressed in the NCSPF which are relevant to this research which will be dicussed.

The NCSPF acknowledges that there is a shortage of implementation and coordination between different government spheres and departments when it comes to addressing South Africa's cyber security challenges. Attached to this is that the development of ICT is crucial to the country's economic growth, but it is also dependent on the secure use of ICT networks. The NCSPF identifies the critical lack of skills in South Africa when it comes to cyber security and advocates for the creation of an environment where vital cyber security skills are further developed in the country. The NCSPF goes as far as to dedicate an entire section towards the protection of critical national information infrastructure (CNII) and the need for the development of strict criteria to ascertain the different areas in which CNII establishments could become compromised (Justice, Crime preventation and Security Cluster, 2011:10).

This policy is significant because it was the country's first attempt at creating a cyber security focused framework. The document itself captured several key aspects concerning the cyber domain. The first was the need for enhanced cooperation of cyber security activities in the country as this will assist in creating better coordinated approaches to cyber crime. Part of this also advocated for a developed information society and knowledge-based economy. The policy also calls for strengthening the gathering of intelligence on cyber matters, along with furthering the development of the processes required in investigation and prosecutions of cyber crimes. Another factor is the need to be able to anticipate emerging cyber threats, particularly those that may target CNII and design responses to these threats. The policy also calls for the development of public-private partnerships between the government, private sector and civil society. This also includes the need for the country to become a key contributor to discussions on cyber security matters at an international level (Justice, Crime preventation and Security Cluster, 2011:4 -11)

Thus from 2011 discussions surrounding South Africa's cyber security vulnerabilities were gaining momentum. A leading driver of this was the 2007 attack against Estonia which demonstrated to the world the manner in which the cyber environment could be harnessed against a particular state, the attack is even referenced in the NCSPF (Justice, Crime preventation and Security Cluster, 2011:10). However, despite the government putting the NCSPF together, the draft policy failed to really get the attention that it needed. In the next chapter the research will highlight how it was only during the period 2015 - 2016 that cyber security issues emerged once again on the policy agenda in South Africa. This is likely because the number of attacks and challenges facing the country within the cyber environment began to increase.

3.6 SUMMARY

The research in this chapter has highlighted how issues surrounding cyber security have gained prominence in South Africa. Cyber attacks directed towards the country have been increasing year on year and the costs to the country's economy are significant, going well into billions of rands. This research has demonstrated that South Africa is one of the top countries targeted for cyber attacks due to its weak cyber security measures and the challenges it faces in policing the cyber domain as a developmental state. Attacks have targeted not only state institutions, but major banks, financial institutions along with individual citizens in the country. All of which significantly undermine national security as they result in financial losses for the economy and jeopardise personal security. In some cases the attacks have even directly targeted cyber infrastructure belonging to the country's police service and accessed the personal details of police informants.

The country's national security has also undergone a significant change in thinking since 1994 with a number of different documents informing how policy makers think about the country's strategic interests. An overwhelming trend across the policy documents such as the country's constitution and the most recent Defence Review analyse how human security has been of key importance when understanding the country's national security. The research has also demonstrated how there has been a gradual acknowledgement in terms of how cyber security relates to national security, as captured by documents such as the Defence Review and the National Cyber Security Policy Framework. When one considers the scale of cyber attacks that have targeted various institutions and government entities as was discussed in this chapter it is clear to see why cyber security is a challenge to the country. With South Africa's national security heavily influenced by the notion of human security, cyber attacks are a direct concern to not only human security but national security as a whole. Cyber attacks threaten the state as well as the well being of its citizens who can often be targeted as individuals.

4. CHAPTER FOUR – CYBER SECURITY DEVELOPMENTS IN SOUTH AFRICA AND THE REST OF THE WORLD

4.1 INTRODUCTION

The National Cyber Security Policy Framework (NCSPF) as discussed in Chapter 3 was the first major document that the country designed that was aimed at addressing cyber issues within a national security framework. Drafted in 2011, approved by cabinet in 2012 and released to the public in November 2015, this was the primary policy framework guiding the country's journey with regards to cyber security policy. However, the country's progress in strengthening its cyber security position and capacity still lacks urgency or prioritisation. The NCSPF was merely a guiding document. In this section this research will provide insights into two different dimensions of cyber security. The first will explore South Africa's domestic progress with regards to cyber security development. This section will trace out the various cyber security initiatives that have taken place in the country and the progress made in developing cyber related legislation along with identifying possible areas for improvement domestically. The second section will then provide a brief analysis on international trends with regards to cyber security and identify areas where South Africa could strenghten its cyber capabilities based on what has worked in the rest of the world.

4.2 SOUTH AFRICA'S DOMESTIC CYBER SECURITY PROGRESS

South Africa has been active in creating legislation that protects information, despite the lack of a formalised cyber security policy. In 1996 the country's constitution enshrined the right to privacy in chapter 2 section 14. In 2000, the Promotion of Access to Information Act (PALA) was passed which was set to give effect to chapter 2 section 32 of the constitution, namely the right to access government information. This legislation aimed to create limitations regarding the protection of privacy, commercial information and information specific to the state. These rights are balanced with other rights in the consitution, particularly those protected in the Bill of Rights. In 2002 the Electronic Communications and Transactions (ECT) act was approved to better regulate electronic transactions and communications. The country also passed the Regulation of Interception of Communications and Provision of Communication-related information (RIC) act, aiming to legislate how certain communications, signals and frequencies can be monitored. The Protection of Personal Information (PPI) bill is also in force and ensures that information that belongs to individuals which is accessed by a public or private entity must be protected. Finally, and somewhat controversially, the government created the Protection of State Information Bill in 2013 which allows the government to classify certain information in order to safeguard national interests from possible attacks. It has not yet been signed into law by the President. There was significant criticism from civil society and the media on this bill as it granted too much power to government officials in deciding what information can be classified (Grobler, et al., 2013:35-37).

South Africa created various laws to ensure that there are some safeguards to protect both the state and citizens in relation to the protection of information and information security. This is a core element of cyber security as many cyber attacks specifically try and target classified or valuable information. However, the theft of information is not the only target of cyber attacks, as has been highlighted in this research there is a real possibility that attacks can do damage to critical infrastructure. Hackers also target financial institutions and steal funds on a massive scale. There is still a critical need for South Africa to address these and the other challenges which could emerge from cyber attacks.

In 2013 the country launched its National Cyber Security Advisory Council (NCAC), a body which was tasked with advising the government on cyber security policy and technical issues. The NCAC was created by the country's Communications ministry. The NCAC's creation resulted from findings in the NCSPF, which had been approved by cabinet the year before and advocated the need for a cyber council such as NCAC. The council's role was to ensure that government more effectively coordinates with the private sector and civil society in tackling cyber security threats (IT News Africa, 2013). However, not long after establishing the NCAC, another cyber body was created known as the Cyber Response Committee (CRC). This committee which was chaired by the State Security Agency and made up of representatives from government departments, including Justice, Defence, Science and Technology, Telecommunications and the Postal services along with the Police. The CRC was formed in November 2014 and was tasked with coordinating and monitoring the development of policies and strategies to combat the risk of cyber threats. This body was tasked with drafting the country's cyber security policies (Czernowalow, 2014). The introduction of the NCAC and CRC over the period of a year highlights the flaws that have plagued South Africa's approach to cyber security, where the country acknowledged the threat, but is struggling to create a united reponse and approach to dealing with cyber attacks. When the CRC was formed there was little understanding if it would work with the NCAC jointly as there was no coordination between the two entities. The NCAC included academics, IT specialists and members of civil society while the CRC was compromised of only government members; this shows a disunity in how the government considers the need to include external stakeholders. The country's inability to coordinate engagements between these two entities and the fact that they were created so quickly after one another undermines its entire approach to cyber security. There remains a lack of clarity on how these two different bodies interacted or if they even interacted at all. It also explains why it has likely taken so long for the introduction of legislation which actively addresses cyber security issues. Although differentiating responsibility between the two different groups could be useful, there does not appear to be any focused cooperation or clear designation as to what their key responsibilities were, whether it be policy generation or more of an advisory and oversight role.

In October 2015 the country launched a virtual hub to tackle cyber crimes in conjunction with the Council for Scientific and Industrial Research (CSIR). The new National Cybersecurity Hub will see government, civil society and industry working together to defend the country against the growing threat of cyber attacks. The development of a cyber unit was another factor that was stipulated in NCSPF, which advanced the need for a dedicated cyber hub. This was further supported in the Electronic Communications and Transactions Act Amendment bill gazetted in October 2012, which provided for the establishment of a cyber security hub. The new hub will be charged with creating awareness around cyber crimes and will need to respond rapidly to incidents or threats which arise in the cyber domain. It will also act as a platform where government can foster cooperation with the private sector, civil society and the international community. Through the hub the government will also introduce a National Cybersecurity Response team which will grow to inform the country on possible threats and also to take proactive mesaures to reduce the the threat of cyber security incidents or breaches (ANA, 2015).

In December 2015 the South African government released the Cybercrimes and Cybersecurity bill for public comment. The bill provides a basis to ensure that the government tackles various elements relating to the country's cyber security. The bill's initial synopsis states the following:

> Create offenses and impose penalties which have a bearing on cybercrime, regulate jurisdication of the courts, further regulate powers to investigate, search and access or seize, regulate aspects of international cooperation in respect of the investigation of cybercrime and provide for the establishment of 24/7 Point of Contact and establish various structures to deal with cyber security (Ministry of Justice and Correctional Services, 2015:2).

The bill also recognises the importance of critical national infrastructure by stating that it will "regulate the identification and declaration of National Critical Information Infrastructures and the measures to protect National Critical Information Infrastructures" (2015:2).

Chapter 7 in the bill is a significant section as it goes into detail on the country's approach to the protection of critical national infrastructure and details the requirements for specifying whether a particular entity can be classified as such. This power is directed by the minister for State Security, who must adhere to specific requirements in classifying an identified entity. The bill has made provision for infrastructure which is not controlled by the state to also be classifed as critical national infrastructure, so long as the State Security Minister has engaged with all the relevant parties (Ministry of Justice and Correctional Services, 2015:105). Should the interference, damage or loss of information in a particular institution compromise the following, state security, public health, the delivery of essential services, economic stability or create a public emergency then the Minister of State Security must investigate, declaring such infrastrucutre as critical to the state.

In this way the country has been able to create a somewhat holistic approach to cyber security as the government has acknowledged the value of information systems that are run within the private sector. This helps to enhance the protection of the state and its citizens, as should the need arise, installations such as banks and/or financial institutions could be considered to form part of critical national infrastructure.

The bill has not been without criticism. Since its release it has come under intense scrutiny as media and citizens have expressed concern on how the proposed legislation encroaches on privacy rights, protected by section 14 of the South African Constitution. This is a key challenge when introducing cyber security regulation as governments must and balance the the freedoms of citizens with the need to protect the country. Criticisms towards the bill suggest that it is too broad and has not provided enough mechanisms to ensuring exceptions when it comes to accessing and disseminating information which may be in the public interest. This works contrary to the Promotion of Access to Information Act and undermines the country's constitution, with particular reference to the right to access information and freedom of expression. The bill allows the government to unduly restrict the dissemination of information, this will impact on the freedom of the press in the country (Chetty, 2015).

Another criticism directed towards the bill is its attempt to decentralise cyber activities across different government departments. Although the primary responsibility for the cyber security bill falls within the country's State Security ministry, the bill proposes that there must be enhanced cooperation across different departments in identifying what can be deemed critical national infrastructure. For example, if an institution of critical national infrastructure is identified, the cabinet member for state security must first engage with the cabinet member under which department that specific institution reports to. There must then be a process for the department to respond to this request. The bill spreads particular responsibilies across three key departments. The Department of Defence which must set up a Cyber Command. The Department of Police is tasked with the establishment of a National Cybercrime Centre and the Department of Telecommunications and Postal services must work towards advancing the country's telecommunications infrastructure (Ministry of Justice and Correctional Services, 2015:75-90). The challenge with diversifying responsibility so broadly is that it will create inefficiencies and see replicated efforts in different departments. By trying to better centralise and combine resources across the different departments the country would likely better utilise scarce technical resources in building its cyber capacity. However, centralisation is not necessarily the best option as it could also give a single department too much power and raise issues of accountability. If the bill is to work it should provide better clarity on the role of each department so as to avoid inefficiencies (The Conversation, 2015).

The country currently does not have any cyber security legislation which relates to matters concerning compliance and regulation. From a legal perspective the country needs to advance stronger legislation which relates to regulation and compliance, this includes matters such as data protection, breach notification and certification/standardization requirements. This is particularly necessary for the commercial sectors which contain critical national infrastructure such as financial institutions and banking. These are sectors where consumers are often at risk. Legislation is required to ensure that institutions such as banks have implemented measures to prevent data breaches. This includes the continuous revision of policies concerning the use of passwords, data encryption, anti-virus protection, intrustion detection and prevention systems (Burger, 2016). Once approved, the Cybercrimes and Cyber security bill will assist in some aspects but it lacks any direction in terms of specific at risk sectors in the economy. The bill is currently available for public comment and has already encountered criticism over matters concerning privacy and the power it provides to the state (Von Solms, 2015).

South Africa has a recognised agency for the implementation of a national cyber security strategy which is designated to the State Security Agency (SSA). The agency is in the process of setting up the country's Electronics Communications Security – Computer Incident Security Response Team (ECS-CISRT) division. The division currently offers its core services to organs of the state with its main aim being to create a single point of contact where the state can receive assistance on cyber security matters. The team is a member of the Forum of Incident Response and Security Teams (FIRST). FIRST is a globally recognised network of cyber security response teams from governments, commercial and academic sectors (State Security Agency, 2015).

Government officials in departments such as State Security require adequate training to develop competency in cyber security skills. Unfortunately, the country does not have any officially approved training programs, particularly for public sector professionals to advance skills development for cyber security. The promotion of cyber security training is lacking as the country also does not have any awareness initiatives aimed at driving interest towards cyber security courses in areas of higher education. The country has also not undertaken any international exchange programs which aim to advance the development of cyber skills within the public sphere. From a research perspective the unveiling of the Cyber security Hub at the Council for Scientific and Industrial Research (CSIR) has been the only major initiative to provide a through point for information on cyber attacks to stakeholders in government and the corporate sector (CSIR, 2015).

From a research institute perspective, the country is lacking in actively driving capacity building in areas concerning cyber research. This was particularly true with regards to sourcing information for this specific research project. Currently, much of the research concerning cyber attacks in the country is published through corporate entities that sell cyber security services. This was clear when it came to determining the types of cyber attacks that have targeted the country and the estimated cost of those attacks. There was no research that was driven through the public sector or any statistics captured by research institutes in the country that could provide clarity. The need for more rigous state assessment and tracking of cyber security attacks in South Africa is critical in order for the country to truly grasp the nature of the problem. The lack of a state driven data on cyber security means that government is forced to use external data from corporate entities. This undermines government's attempt to create legislation free from corporate bias and address cyber security from a holistic and local perspective.

Overall, the country's progress with regards to cyber security has been slow. The release of the Cybersecurity and Cybercrimes bill in December 2015 for public comment is just one step towards creating legislation to more effectively govern cyber space in the country. The bill still needs to be further debated in a parliamentary committee and then ultimately make its way to the country's national assembly to be discussed and then possibly approved. This process will likely take most of 2016 and roll into 2017 if it continues to face public scrutiny. Policy discussions on the country's cyber capabilities started in 2010, yet to date no cyber specific legislation has been implemented. This highlights how little prominence has been given to cyber matters by the country's government. Creating legislation is one matter but ensuring that it can be policed by personnel who have a strong IT technical background in cyber security is another. The launch of the Cyber Security Hub at the CSIR in October 2015 shows that the government is working towards enabling this process by trying to create a cyber defence capacity, but is is unlikely that this initiative alone will feed the growing demand for cyber security skills.

4.3 CYBER SECURITY DEVELOPMENTS IN THE REST OF THE WORLD

The previous section analysed South Africa's progress with regards to cyber security. Examples of cyber security initiatives from the rest of the world may be useful to the country's cyber strategy. Cyber initiatives are difficult to introduce given that internet and technological advances move significantly faster than a country's abilities to create legislation. By the time a government introduces a particular cyber security project it could already be out-dated. Effective cyber security requires an all-inclusive approach which intertwines domestic and international legislation applicable to the cyber domain. Countries are often unable to effectively legislate in isolation because of the transnational nature of cyber threats. This is problematic as there are no globally accepted treaties that are enforced with regards to cyber security (Grobler, et al., 2013:32-37).

The first international treaty regarding cyber security was the Convention on Cybercrime, which was opened for signatures in November 2001 and then entered into force in July 2004. However, as of March 2016 only 49 countries have ratified the treaty, the vast majority of which are in Europe. This is likely because the treaty was overseen by the Council of Europe. The treaty was created to form a foundation for law enforcement in cyberspace and assist countries in creating uniform anti-cybercrime laws that can guide the behaviour of policing bodies. For countries to effectively counter the risk of cyber attacks there needs to be agreement that an offence in one country will be considered an offence in another country as well (Council of Europe, 2016). Without this kind of policy alignment it would prove impossible for countries to effectively prosecute transnational cyber criminals. South Africa signed the treaty in 2001 and is one of the few non-Council of Europe states that has engaged in the process. Dominant global powers such as China and Russia have refused to sign the treaty due to concerns on issues regarding sovereignty and have instead tried to engage the United Nations directly on a code of conduct for cyberspace. Sovereignty and enforcement are likely to remain factors which hinder the development of globally accepted cyber treaties. The signing of international treaties is not necessarily a prerequisite to the advancement of cyber security. For instance, while China is unwilling to commit to treaties the country continues to pursue cyber security collaboration with different partners. In Africa, the Chinese have committed to work with the African Union (AU) towards the advancement of cyber security on the continent by launching multi-dimensional cooperation projects with African countries in the realm of internet development and management (Ogundeji, 2016). In February 2014, Chinese President Xi Jinping declared that he will do everything in his power to ensure that China becomes a cyber power by driving science and technology development in the country (Austin, 2016).

Increased cross border cyber defence collaboration is vital in countering transnational cyber attacks. The cyber environment is globalised and cannot be approached in isolation or on a purely national basis. Countries may have critical national infrastructure that even extends across borders such as power utilities. Companies which manage critical national infrastructure may also be foreign owned and have systems which are inter-connected across the world. Grobler and Van Vuuren (2012:64) have argued that if South Africa's online government banking services had ever been targeted by the world's largest botnet Metulji, it would likely have required an international assistance in order to manage and repel the threat. Coordinated international efforts ultimately lead to the destruction of Metulji and the arrest of two of its creators in June 2011. It is suspected that the botnet controlled over 12 million individual zombie computers and facilitated the theft of millions of dollars through identity and banking theft (Grobler & Jansen van Vuuren, 2012: 64).

In the Southern African Development Community (SADC) the Harmonisation of Information and Communications Technology Policies in Sub-Saharan Africa (HIPSSA) is one such example of how as a region, collaboration is assisting SADC countries in aligning legal frameworks, developing best practices and identifying areas for improvement in cyber defence. Further collaboration through stakeholder workshops and the inclusion of experts from other regions in the world will likely better prepare SADC for potential future cyber attacks. However, for South Africa to effectively participate in cyber collaboration the country must patrol its own cyber borders. The government must enhance the capabilities of the CSIRT team to ensure that it can identify cyber attacks that are being conducted from within the country's borders. Failure at internal cyber policing will make South Africa ineffective in assisting neighbouring states in repelling cyber attacks. To do this effectively the country would also need to modernise and expand its network infrastructure and internet hosting abilites. Cyber defence collaboration is undermined if a particular country is weak in terms of its technological abilities because this will hamper its ability to track out attacks internally and identify the hackers (Grobler & Jansen van Vuuren, 2012:71).

In terms of continental Africa, South Africa is well placed to establish itself on cyber security matters due to the country's comparatively advanced ICT infrastructure. On 27 June 2014, the African Union (AU) adopted the Convention on Cyber Security and Personal Data Protection. The document provides a thorough breakdown on how African states can work towards building a strong information based society. It provides detail on the creation of cyber security related legislation and regulatory frameworks, along with identifying the role of national authorities who will be charged with enforcing the legislation. The treaty also commits African states towards creating agreements of mutual legal assistance and the exchange of information to advance cooperation on the continent within the cyber domain. Although the AU has approved the document, to date it has only been signed by 8 out of the

54 member countries. South Africa has not signed or ratified the document. Considering the low participation rate on the continent, this presents an opportunity for South Africa to position itself as a major player in the cyber domain. The promotion of good cyber security governance in Africa works in South Africa's favour because it will allow more continental alignment and advance the development of capacity building in terms of cyber defence. This affords South Africa the opportunity to form cyber alliances on the continent (African Union, 2014).

While South Africa can look towards enhancing cyber governance in Africa, the country can also take note of the application of desecuritisation within the cyber space. Earlier in this study the concept of securitisation was discussed and how it plays a role in the understanding of how countries prioritise particular issues in order to dedicate focused resources towards them. However, Barry Buzan (1998:29) has also explored the notion of desecuritisation, which is when a particular issue moves out of the realm of being securitised and into the realm of being politicised. In this way issues can then be dealt with in the public space and lead towards more long term stability. An example of desecuritisation can be seen in Estonia after the 2007 cyber security attacks. In 2008 the country's Ministry of Defence (MoD) put forward various policy recommendations aimed at the deterrence of cyber threats captured in the ministry's Cyber Security Strategy (CSS). The document laid out hard targets for enhancing the protection of the country's critical national infrastructure. The country's CSS also advanced the need for campaigns which aim to raise awareness about matters concerning information security, with a particular focus directed towards individual citizens and small to medium enterprises. The document laid out the need for more comprehensive legislation and enhanced international cooperation (Estonian Ministry of Defence, 2008). All these factors highlighted that even though Estonia suffered from a major cyber attack, the country still embedded the need for desecuritization within its policies to create long term stability on cyber issues.

Going forward desecuritisation should be a matter that the South African government considers in its approach to cyber security. Elements of desecuritisation will be critical in order for the government to successfully tackle cyber threats. Raising public awareness about cyber security is one step towards this as it ensures that the public are included as stakeholder. It will also emphasise that the public are made aware that they have responsibility when it comes to their own personal cyber security and that of businesses as well.

Global rankings are another way to track the country's progress and compare international cyber security strategies. In 2015 the World Economic Forum (WEF) released a Global Cybersecurity Index which provides a measure of a country's level of cyber security development. In the report, South Africa was ranked with a score of 0.382 while the United States of America was ranked as the best country in terms of cyber security with a score of 0.824. South Africa was 60th globally and 6th in Africa. These rankings systems are important because they provide a benchmark for countries which are looking to advance their cyber capabilities by examining some of the best practices in the rest of the world. There are lessons that South Africa could learn from the USA when it comes to cyber security development (World Economic Forum, 2015).

For instance, the USA has approved and implemented a number of different frameworks that align with internationally recognised cybersecurity standards. This has allowed the country to advance its cyber security partnerships and alliances. The country has also created a National Initiative for Cybersecurity Education (NICCS) which ensures that cyber security certificates and skills are maintained within a particular framework, this guarantees a competency standard for state agencies and the public sector. The country created an International Strategy for Cyberspace which was actually issued by executive order from President Barack Obama. The strategy prioritises the protection of critical national infrastructure and advances the improvement of cybersecurity for these institutions. Within the country's executive there is a US Cybersecurity Coordinator who is assigned as a special assistant to the President in order to provide guidance on cyber related matters. The USA has strong links between Homeland Security and the Department of Defence in terms of information sharing and formal agreements are in place to promote cooperation in the protection of civilian and military computer systems (World Economic Forum, 2015).

From a benchmarking perspective the USA government has created a nationally accepted security checklist which provides guidance for setting up cyber security configurations for public institutions across the country. This ensures that a generally accepted base level of security is set up in the public sector. The government has also released a best practise program which was created by the Department of Defence (DOD) which aims to assist the private sector in determing the necessary skills for IT practitioners and highlight how to engage with Homeland Security on cyber security issues. In this manner the country also drives active public-private sector partnerships within the domestic cyber domain. In terms of international cooperation the USA has official bilaterial agreements with Canada and Estonia with regards to the sharing of cybersecurity assets across borders. The USA has a cooperation agreement with the European Union (EU) on cyber security which established a working group in 2010. This group works jointly to uncover cyber crimes and incursions while also promoting public-private partnerships and raising cyber awareness (World Economic Forum, 2015). There are a number of lessons that South Africa can take from the USA, particularly with regards to a standardised cyber security training program for the public sector, increased cooperation between the country's security cluster and the role of a special assistant to the President on cyber matters.

The WEF report can also be used in examining progress on the African continent. The top ranked African countries also hold lessons which South Africa could take forward in strengthening its cyber position. In Mauritius, which the WEF report has placed first in Africa, the government has drafted four pieces of legislation which aim to tackle cyber security from various angles. These are ICT protection, Computer Misuse, Eletronic transactions and Data Protection. The government also conducts a risk assessment on the public service which feeds into informing the country's National Information and Communication Technology Plan. In Rwanda, which is also in the top African rankings, the government has established a specific IT security program within the National Police Academy to rollout training to police officers early in their development. The ministry of education ensured that information security modules are offered in all the university courses for computer engineering. In the Ivory Coast, the government has created a database in order to better track the number of cyber attacks. In this way the country is able to map out the scale of cyber attacks and provide accurate progress on its attempts to thwart incursions. This would be particularly useful for South Africa as the government has not been able to accurately capture statistics on cyber attacks in the country (World Economic Forum, 2015).

The implementation of cyber security best practices from globally leading countries but also specifically African countries would be a key mechanism that South Africa could use towards strengthening the country's cyber position. Information sharing and the creation of partnerships between state security, the police and the military is one such area where the country could also improve its position. A dedicated cyber resource which is assigned to the Presidency is another strategy to ensure that cyber security matters are given the attention they deserve. It would also bring the country in line with global standards and ensure that government is well informed on emerging cyber threats and trends.

4.4 SUMMARY

Chapter four aimed to discuss two key aspects that are relevant to the research, the first was South Africa's progress with regards to cyber security and the second aspect examined some of the best cyber security strategies from around the world. In terms of South Africa's progress the study has demonstrated the lack of any formal cyber security legislation. Despite this, South Africa acknowledged the need for the protection of information as far back as 2000, when the country passed the Promotion of Access to Information Act. The country has since created the 2002 Electronic Communications and Transactions act. Formal acknowledgement of cyber issues only gained prominence in 2012 with National Cyber Security Policy Framework which was highlighted in chapter 3 which then ultimately lead into the creation of a National Cyber Security Advisory Council (NCAC). The government then created an additional cyber team known as the Cyber Response Committee (CRC) which resulted in some confusion as there was little coordination between the NCAC and the CRC. This led into the drafting of the Cyber Security and Cyber Crime bill which was released for public comment in December 2015. The time taken to reach this point is problematic as cyber security has been and continues to be a challenge for the country. At the time of writing the Cyber Security and Cyber Crime bill had still not gone through parliament.

The country has shown some progress with regards to creating legislation but has shown limited development with regards to cyber capacity. The State Security Agency is still setting up the country's Computer Incident Reponse Team. From a training capacity there are no officially approved programs in place which aim to strengthen the cyber abilities of public sector professionals. The introduction of the Cyber security Hub at the CSIR is likely to assist with data mining in terms of providing an information on the cyber environment. However, the country still lacks research capacity as government has not been able to produce any reports which detail the scale of cyber attacks that have been targeting the country.

South Africa could adapt strategies from around with world which would strengthen the country's cyber position. The role of collaboration and the development of cyber alliances, for information sharing, capacity building and collective defence, is vital for development. The transnational nature of cyber attacks requires countries to work together to counter them. It would be beneficial for South Africa to actively pursue cyber alliances.

5. CHAPTER 5 – CONCLUSION

5.1 INTRODUCTION

The last chapter will summarise the key findings of this study. This research explored the current challenges within cyber security affecting South Africa's national security. This study provided an assessment on the concepts of national security and cyber security, discussed the evolution of South African national security and provided analysis on several public cyber attacks. Finally, this research provided information on South Africa's current cyber position and concluded with potential recommendations for strengthening the country's cyber security in the future. Considering the above information there are few matters that require emphasis in this final chapter.

5.2 THE RELEVANCE AND STRUCTURE OF THE STUDY

The purpose of the study was to analyse cyber security as an emerging challenge to South African national security. The relevance behind the study is that across the world, cyber attacks are not only occuring with increasing frequency but also have the potential to cause significant damage to states and their citizens. In South Africa this has not only been understated but also under researched. This study aimed to contribute towards broadening the knowledge and understanding on the role of cyber security and the challenges that South Africa is facing in the cyber domain. The study was structured in the following manner to achieve this goal:

Chapter 1 presented an explanation on how the research study would be conducted. The chapter provided clarity on the research methods that would be employed and how the structure of the project would unfold in terms of content, sources and the main arguments.

Chapter 2 focused on defining national security and how the term has gradually moved from being thought of in realist and militaristic terms to a broader focus which acknowledges the role of human security. This led into an analysis on the notion of securitisation and how emerging threats make their way onto the security agenda. Having discussed national security this study then moved on to unpack cyber security. This was accomplished by analysing how the internet has developed over time and how the initial focus was on the technical aspects surrounding computer security. The notion of cyber security was introduced as it represented the nexus where threats in the cyber domain could be seen as having a significant impact on society. This chapter also provided detail on the types of threats that are present in the cyber domain and how they can disrupt particular spheres of society. This led to an analysis on the most prevalent cyber attacks reported in the media, namely the attacks against Estonia, the Stuxnet worm in Iran, the ongoing attacks against the USA by Chinese hackers and the hack that targeted the Democratic National Committee.

Chapter 3 drew focus to South Africa. The chapter outlined some of the most public cyber attacks that have targeted the country and the costs that they have incurred. Core within this section was highlighting the severity of the cyber attacks which are targeting South Africa. This was achieved using a variety of research reports which emphasised the country's growing challenges within the cyber domain. In this chapter an overview on how South African national security has evolved since 1994 was provided. Of particular interest was how the country has worked towards asserting itself as nation which places human rights and human security as key elements within its national security. This research tracked the government's gradual acknowledgement on the importance of cyber security to the country's national security. This was done through analysing policy documents such as the Defence Review, the National Cyber Security Policy Framework (NCSPF) and statements made by securitising actors such as national ministers.

Chapter 4 contextualised South Africa's current domestic cyber section position when it comes to matters concerning legislation and the country's general cyber capabilities. This chapter indentified areas of weakness in South Africa's cyber security and provided strategies for strengthening the country's future cyber development. This section presented strategies that could be adapted from countries around the world and prove useful to South Africa.

Chapter 5 concluded this study by emphasising the goal of the research, highlighting how the study was structured and explaining some of the key findings to be taken forward. This chapter also addressed possible areas for future research.

5.3 RECOMMENDATIONS

Cyber security is a matter of concern for South African national security and is likely to remain an issue of growing importance. The country has already suffered a number of cyber attacks that have directly targeted state infrastructure or have focused on undermining the security of its citizens. Considering the nature of the cyber attacks that have targeted Estonia, Iran and the USA, it is clear that a sophisticated cyber offensive has the capability to cause significant damage to a country's operations. Terrorist organisations such as ISIS have also become more adept at using cyber space to drive their agenda. In South Africa, ISIS has used the internet to attract recruits and has even encouraged local citizens to conduct terrorist operations within the country's borders. Considering that South Africa's national security is heavily influenced by the notion of human security, the country requires a clear focus in terms of cyber security.

Cyber security and its influence on national security has only been properly acknowledged by the Defence Review and the speech given by previous State Security Minister Siyabonga Cwele as highlighted in chapter 3. Although the country has produced cyber policy frameworks to guide the creation of more focused legislation, there remains a lack of engagement and discourse on the importance of cyber security to national security. Even the country's National Development Plan, the guiding policy until 2030, fails to articulate any clear strategy with regards to cyber security. This speaks to one of the recurring points in this research which is that South Africa has not given cyber security the policy prioritisation and focus that it should. This is possibly because the government has under-estimated the impact that cyber attacks may have on the country. This would also explain why the government has yet to produce any form of research report which has analysed cyber security in the country. The tracking of cyber attacks and the breakdown of their costs on the South African economy is all being done by the private sector. It is this research that is informing government policy, as was highlighted in chapter 4, where even the National Cyber Security Policy Framework takes note of the findings produced by the cyber security firm Norton.

Although the South African government is now in the process of creating cyber focused legislation through the Cyber Security and Cyber Crimes bill, legislation alone will not adequately deal with the challenges that the country is facing. There is a definite need for capacity building within the public domain with particular focus on technical skills such as cyber forensics, cryptography, information security and other cyber related disciplines. One of the challenges facing the country is that proper cyber investigations cannot take place because the South Africa Police Service (SAPS) do not have the necessary skills when it comes to cyber operations. Although the Cyber Security and Cyber Crimes bill will provide better guidance in term of prosecutions, it needs to be supported by active skills training within the country's police service. The same is true for the military and state intelligence. This process can be assisted by better partnerships with the private sector and research institutes. Another problem facing the country is the lack of information sharing with regards to cyber attacks, particularly with the corporate sector as firms do not want to publicise their security failings. There is a need for government to proactively engage with companies that are continuously facing cyber attacks, such as banks and financial institutions, to obtain a better idea of how cyber security can be dealt with holistically. On the research front, government needs to not only develop more focused cyber research but also empower institutions such the Cyber security Hub at the CSIR with the necessary resources to assist in developing cyber security solutions.

It is important that South Africa also develops cyber security partnerships outside of its borders. The role of collaboration and the advancement of cyber alliances with other countries would prove invaluable towards the strenghtening of the country's cyber security position. There is also an opportunity for South Africa to establish itself on the African continent with regards to cyber security, particularly as the country suffers from the highest levels of cyber attacks on the continent. The application of cyber security intiatives from around the world would also prove useful for the country. For instance, South Africa could introduce a cyber security special advisor within the office of the Presidency to provide information on the latest cyber developments as has been done in the USA. Alternatively, the country could adapt Rwanda's approach in capacity building with the introduction of a cyber security focused module that forms part of the country's police academy training program. Estonia's strategy for cyber security awareness campaigns should also be a matter that the country interrogates, as there is a need for the public to be more informed on how they can take precautions against cyber attacks and protect their personal information. It can also be applied to the public sector in order to ensure that civil servants are better informed on the ways in which they should manage state information.

In conclusion, this study has demonstrated that cyber security is an emerging challenge to South African national security. The country has faced numerous cyber attacks in the past and this is likely to continue as South Africa further develops its ICT infrastructure. Although South Africa has made some progress with regards to cyber security, considering the scale of the issue there appears to be a lack of not only urgency but also prioritisation when it comes to how cyber security affects national security. With the development of cyber weapons and advanced cyber security teams taking place in the rest of the world, there is clear need for South Africa to direct more resources towards securitising its cyber domain. With criminal hackers and terrorist organisations also increasing their efficiency at conducting transnational cyber attacks, South Africa is going to have to strengthen its cyber position in order to protect its citizens.

5.4 AREAS FOR FUTURE RESEARCH

This research has provided a detailed overview on the state of cyber security in South Africa. However, there are various areas of research within the cyber domain that would definitely add value to the broader understanding of cyber issues in South Africa. Some of these include the following:

- What is the role and responsibility of the private sector when it comes to cyber security, is there a need for more coordination between private companies when it comes to information sharing on cyber matters and best practises?
- Is there a requirement within international law for regulations and even possibly restrictions with regards to the development of cyber weapons, particularly if they are being developed to disrupt non-military establishments such as power stations, water infrastructure or transport services?
- What is the role of international organisations such as the United Nations and the African Union when it comes to cyber security?
- Considering the debates in South Africa concerning the Cyber Crimes and Cyber Security bill and its encroachment on privacy, how should the government act in developing cyber security policy while also ensuring that basic freedoms and liberties are protected?

6. BIBLIOGRAPHY

African Union, 2014. *Africa Union Convention on Cyber Security and Personal Data Protection.* [Online]
Available at: http://www.au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection
[Accessed 26 August 2016].

Africa, S., 2015. Human security in South Africa. *Strategic Review for Southern Africa,* 37(1), pp. 178-189.

Alfreds, D., 2015a. *Cyber crooks 'double' attacks on SA.* [Online]
Available at: http://www.fin24.com/Tech/News/cyber-crooks-double-attacks-on-sa-20151203
[Accessed 15 December 2015].

Alfreds, D., 2015b. *Internet access to 'spike' in SA.* [Online]
Available at: http://www.fin24.com/Tech/News/Internet-access-to-spike-in-SA-20150629
[Accessed 10 October 2015].

ANA, 2015. *IOL.* [Online]
Available at: http://sbeta.iol.co.za/news/politics/new-cybersecurity-hub-to-protect-sa-1938479
[Accessed 21 November 2015].

Austin, G., 2016. *Evaluating China's Cyber Power.* [Online]
Available at: http://thediplomat.com/2016/10/evaluating-chinas-cyber-power/
[Accessed 30 October 2016].

Avenant, M., 2015. *Itweb.* [Online]
Available at: http://www.itweb.co.za/index.php?option=com_content&view=article&id=148330
[Accessed 14 December 2015].

BBC, 2007. *The cyber raiders hitting Estonia.* [Online]
Available at: http://news.bbc.co.uk/2/hi/europe/6665195.stm
[Accessed 12 October 2015].

Bhorat, H., Hirsh, A., Kanbur, R. & Ncube, M., 2014. *Economic policy in South Africa past, present and future,* Cape Town: University of Cape Town: Development policy research unit.

Brickey, J., 2012. Defining Cyberterrorism: Captuing a broad range of activites in cyberspace. *CTC Sentinel,* 5(No. 8).

Burger, S., 2016. *In-house training necessary to improve cybersecurity skills.* [Online]
Available at: http://www.engineeringnews.co.za/article/in-house-training-necessary-to-improve-cyber-security-intel-security-2016-09-16
[Accessed 25 October 2016].

Buzan, B., Waever, O. & De.Wilde, J., 1998. *Security: A new framework for analysis.* Boulder: Lynne Rienner.

Chauke, A., 2012. *Exclusive: Inside the R42 heist.* [Online]
Available at: http://www.timeslive.co.za/local/2012/02/10/exclusive-inside-the-r42m-heist
[Accessed 21 October 2015].

Chetty, P., 2015. *Techcentral.* [Online]
Available at: http://www.techcentral.co.za/reasons-to-fear-sas-cybersecurity-bill/61852/
[Accessed 20 December 2015].

Chon, G., 2015. *US pursues case against Chinese army hackers.* [Online]
Available at: http://www.ft.com/intl/cms/s/0/a378b4c6-62b0-11e5-9846-de406ccb37f2.html#axzz3p2ro3MEm
[Accessed 19 October 2015].

Collins, S. & McCombie, S., 2012. Stuxnet: the emergence of a new cyber weapon and its implications. *Journal of Policing, Intelligence and Counter Terrorism*, 7(1), pp. 80-91.

Computer Science and Telecommunications Board, 1991. *Computers at Risk: Safe Computing in the Information Age*. Washington D.C.: National Academy Press.

Council of Europe, 2016. *Chart of signatures and ratifications of Treaty 185.* [Online]
Available at: http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures
[Accessed 10 March 2016].

CSIR, 2015. *Cybersecurity Hub.* [Online]
Available at: https://www.cybersecurityhub.co.za/aboutus.html
[Accessed 25 May 2016].

Cwele, S., 2014. *Cyber Security Meeting, Johannesburg 27 March 2014*. Johannesburg: Government Printers.

Czernowalow, M., 2014. *IT web*. [Online]
Available at: http://www.itweb.co.za/index.php?option=com_content&view=article&id=139125
[Accessed 20 November 2015].

Darczewska, J., 2014. *The Anatomy of Russian Information Warfare," Point.* [Online]
Available at:
http://www.osw.waw.pl/sites/default/files/the_anatomy_of_russian_information_warfare.pdf.
[Accessed 11 October 2015].

Defence Review Committee, 2015. *South African Defence Review.* Pretoria: Government Printers..

Denning, D., 1999. *Information Warfare and Security.* Essex: Addison-Wesley Longman Ltd.

Department of Communications, 2013. *Electronic Communications Act: South Africa Connect: Creating opportunity, ensuring inclusion.* [Online]
Available at: www.gov.za
[Accessed 20 January 206].

Dirk, N., 2015. *Cyber security: SA banks go big.* [Online]
Available at: http://www.iol.co.za/business/news/cyber-security-sa-banks-go-big-1943685
[Accessed 26 August 2016].

Esterhuyse, A., 2016. Human security and the conceptualisation of South African defence: Time for a reappraisal. *Strategic Review for Southern Africa*, 38(1), pp. 29-45.

Estonian Ministry of Defence, 2008. *Cyber Security Strategy*, s.l.: Cyber Security Strategy Committee.

Farwell, J. P. & Rohozinski, R., 2011. Stuxnet and the Future of Cyber War. *Survival: Global Politics and Strategy*, pp. 53:1, 23-40.

a) Fripp, C., 2014. *Cybercrime costs South Africa about R5.8 billion a year.* [Online]
Available at: http://www.htxt.co.za/2014/11/11/cybercrime-costs-south-africa-about-r5-8-billion-a-year/
[Accessed 30 November 2014].

b) Fripp, C., 2014. *This is why Africa is a cybercrime target.* [Online]
Available at: http://www.htxt.co.za/2014/11/12/this-is-why-africa-is-a-cybercrime-target/
[Accessed 30 November 2014].

Gartenstein-Ross, D. & Barr, N., 2016. *The myth of lone-wolf terrorism.* [Online]
Available at: https://www.foreignaffairs.com/articles/western-europe/2016-07-26/myth-lone-wolf-terrorism?cid=nlc-fatoday-20160727
[Accessed 26 August 2016].

Gillwald, A., Moyo, M. & Stark, C., 2012. *What is happening in ICT in South Africa,* Cape Town: ResearchICTafrica.

Goldman, E., 2004. New Threats, New Identities and New Ways of War: The Sources of Change in National Security Doctrine. *The Journal of Strategic Studies*, Volume 24 (2),pp45

Graham-Harrison, E., 2015. *Could Isis's 'cyber caliphate' unleash a deadly attack on key targets?.* [Online]
Available at: http://www.theguardian.com/world/2015/apr/12/isis-cyber-caliphate-hacking-technology-arms-race
[Accessed 20 October 2015].

Grobler, M. & Jansen van Vuuren, J., 2012. Collaboration as proactive measure against cyber warfare in South Africa. *African Security Review,* Volume 21:2, pp. 61-73.

Grobler, M., Jansen van Vuuren, J. & Zaaiman, J., 2013. Preparing South Africa for cyber-crime and cyber defence. *Systemics, cybernetics and informatics volume,* p. Vol 11 No.7.

Groll, E., 2015. *The U.S. Hoped Indicting 5 Chinese Hackers Would Deter Beijing's Cyberwarriors. It Hasn't Worked..* [Online]
Available at: http://foreignpolicy.com/2015/09/02/the-u-s-hoped-indicting-5-chinese-hackers-would-deter-beijings-cyberwarriors-it-hasnt-worked/
[Accessed 19 October 2015].

Hansen, L. & Nissenbaum, H., 2009. Digital Disaster, Cyber Security and the Copenhagen School. *International Studies Quarterly,* Volume 4, pp. 1-25.

Hennessey, S., 2016. *What does the U.S. government know about Russia and the DNC hack?.* [Online]
Available at: https://www.brookings.edu/blog/techtank/2016/07/25/what-does-the-u-s-government-know-about-russia-and-the-dnc-hack/
[Accessed 26 August 2016].

Herzog, S., 2011. Revisiting the Estonian Cyber Attacks:Digital Threats and Multinational Responses. *Journal of Strategic Security* , pp. 4, no. 2 (2011): 49-60..

Hosken, G., 2014. *Gautrain hesit foiled.* [Online]
Available at: http://www.timeslive.co.za/thetimes/2014/11/13/gautrain-heist-foiled
[Accessed 7 December 2014].

Hough, M., Du Plessis, A. & Kruys, G., 2007. *Selected official South African strategic and security perceptions: 2001-2007.Ad Hoc Publication No 44: November 2007..* Pretoria: ISSUP.

Institute for Security Studies, 2015. *Is South Africa geared up for new cyberspace challenges?.* [Online]
Available at: http://www.issafrica.org/uploads/26-Jan-2015-Cybercrime-seminar-presentationspdf

International Commission on Intervention and State Sovereignty, 2001. *The Responsibility to Protect,* Ottawa: International Development Research Centre.

IT News Africa, 2013. *South Africa launches national cyber security advisory council.* [Online]
Available at: http://www.itnewsafrica.com/2013/10/south-africa-launches-national-cyber-security-advisory-council/
[Accessed 20 November 2015].

Justice, Crime prevention and Security Cluster, 2011. *National cyber security policy framework for South Africa*. Pretoria: Republic of South Africa.

Kaspersky, 2014. *Report on cyber threats in Africa 2014.* [Online]
Available at:
http://www.kaspersky.co.za/about/news/virus/2014/Kaspersky_Lab_reports_on_cyber_threats_in_Africa_in_the_first_quarter_of_2014
[Accessed 10 November 2015].

Keane, A. G., 2016. *News analysis: Pointing fingers is risky for US after hack.* [Online]
Available at: http://www.bdlive.co.za/world/americas/2016/07/27/news-analysis-pointing-fingers-is-risky-for-us-after-hack
[Accessed 26 August 2016].

Kuehl, D., 2009. Cyberspace and Cyberpower. In: F. Kramer, S. Starr & L. Wentz, eds. *Cyberpower and National Security*. Dulles: Potomac Books, p. 28.

Mamabolo, M., 2016. *Cyber threats in Africa: 'it's just the beginning' says expert.* [Online]
Available at: http://www.itwebafrica.com/security/513-africa/236297-cyber-threats-in-africa-its-just-the-beginning-says-expert
[Accessed 26 August 2016].

McAfee, 2014. *Net Loss: Estimating the Global cost of cybercrime*, Washington D.C.: Centre for Strategic and International Studies.

Ministry of Justice and Correctional Services, 2015. *Cybercrimes and Cybersecurity Bill*, Pretoria: Government printers.

Morgenthau, H., 2005. *Politics among nations*. Seventh edition ed. New York: McGraw Higer education.

Mozur, P., 2015. *Cybersecurity firms says Chinese hackers keep attacking US companies.* [Online]
Available at: http://www.nytimes.com/2015/10/20/technology/cybersecurity-firm-says-chinese-hackers-keep-attacking-us-companies.html?_r=0
[Accessed 22 October 2015].

National Development Plan, 2012. *Executive Summary of the National Development Plan 2030 - Our future - make it work*, Pretoria: Government Printers.

NATO Cooperative Cyber Defence Centre of Excellence, 2013. *Tallinn Manual on the International Law applicable to Cyber Warfare.* New York: Cambridge University Press.

Newman, E., 2010. Critical human security studies. *Review of International Studies*, Volume 36, pp. 77-94.

Nissenbaum, H., 2005. Where computer security meets national security.. *Ethics and Information Security*, 2(7), pp. 61-73.

Norton, 2013. *2013 Norton Report.* [Online]
Available at: http://www.symantec.com/content/en/us/about/presskits/b-norton-report-2013.pptx
[Accessed 30 November 2014].

Nuechterlein, D., 1976. National Interests and Foreign Policy: A Conceptual Framework forAnalysis and Decision-Making. *British Journal of International Studies*, Volume 2, pp. 246-266.

Nye, J., 1999. Redefining the National Interest. *Foreign Affairs*, p. Volume 8 (4) .

Ogundeji, O., 2016. *AU, China unite to tackle cybercrime*. [Online]
Available at: http://www.itwebafrica.com/security/513-africa/236293-au-china-unite-to-tackle-cybercrime
[Accessed 26 August 20116].

Parlapiano, A., 2016. *What we know about the cyberattack on democratic politicians.* [Online]
Available at: http://www.nytimes.com/interactive/2016/08/16/us/politics/cyberattack-on-democratic-politicians-dnc.html
[Accessed 26 August 2016].

Patel, K., 2015. *Al-jazeera.* [Online]
Available at: http://www.aljazeera.com/news/2015/05/south-african-families-isil-newest-recruits-150529094806722.html
[Accessed 09 December 2015].

Peoples, C. & Vaughan-Williams, N., 2010. *Critical Security Studies: An introduction.* First edition ed. New York: Routledge.

Pijoos, I., 2016. *SA brothers charged with planning to blow up US embassy and 'Jewish institutions'.* [Online]
Available at: http://www.news24.com/SouthAfrica/News/sa-brothers-charged-with-planning-to-blow-up-us-embassy-and-jewish-institutions-20160711
[Accessed 26 August 2016].

Raine, L., Anderson, J. & Connolly, J., 2014. *Cyber attacks likely to increase.* [Online]
Available at: http://www.pewinternet.org/2014/10/29/cyber-attacks-likely-to-increase/

Republic of South Africa, 1996. *Constitution of the Republic of South Africa*. Pretoria: Government Printer.

Reveron, D., 2012. *Cyberspace and National Security*. Washington DC: Georgetow University Press.

Roane, B., 2013. *SAPS website hacked*. [Online]
Available at: http://www.iol.co.za/news/crime-courts/saps-website-hacked-1.1520042#.VHrpBdKUdwo
[Accessed 30 November 2014].

RSA, 1994. *Reconstruction and Development Programme White Paper.* [Online]
Available at: www.gov.za
[Accessed 15 January 2016].

Rudner, M., 2013. Cyber threats to critical national infrastructure: An Intelligence challenge. *International Journal of Intelligence and Counterintelligence*, 26(3), pp. 453-481.

Ruus, K., 2008. Cyber War I: Estonia Attacked from Russia. *European Affairs*, 9(1).

Sapa, 2012. *Millions stolen in Postbank hacking*. [Online]
Available at: http://www.fin24.com/Companies/Financial-Services/Millions-stolen-in-Postbank-hacking-20120115
[Accessed 25 October 2015].

Sapa, 2015. *Spy cables: Threats of cyberattacks against SA banks.* [Online]
Available at: http://www.enca.com/south-africa/spy-cables-threats-cyberattack-sa-banks
[Accessed 15 July 2015].

Sharma, D., 2010. "Integrated Network Electronic Warfare: China's New Concept on Information Warfare. *Journal of Defense Studies 4,* 4(2).

Sheldon, J., 2013. The Rise of Cyberpower. In: *Strategy in the contemporary world.* New York: Oxford University Press, pp. 303-319.

Singer, P. & Friedman, A., 2014. *Cybersecurity and Cyberwar: What everyone needs to know.* New York: Oxford University Press.

Sorensen, T., 1990. Rethinking National Security. *Foreign Affairs*, p. Volume 69 (3).

South African government, 1994. *White Paper on Intelligence*. [Online]
Available at: www.ssa.gov.za
[Accessed 15 January 2016].

South African government, 1996. *White Paper on Defence.* [Online]
Available at: www.ssa.gov.za
[Accessed 16 January 2016].

Spector, J. B., 2016. *US 2016: Donald Trump, The Siberian Candidate?.* [Online]
Available at: http://www.dailymaverick.co.za/article/2016-07-27-us-2016-donald-j-trump-the-siberian-candidate/#.V8BDavl9603
[Accessed 26 August 2016].

Stack, L., 2015. *How ISIS expanded its threat.* [Online]
Available at: http://www.nytimes.com/interactive/2015/11/14/world/middleeast/isis-expansion.html
[Accessed 26 August 2016].

State Security Agency, 2015. *Computer Security Incident Response Team (CSIRT).* [Online]
Available at: http://www.ssa.gov.za/CSIRT.aspx
[Accessed 29 May 2016].

Stupart, J., 2015. *African defence review.* [Online]
Available at: http://www.africandefence.net/in-defence-of-the-defence-review/
[Accessed 20 November 2015].

The Conversation, 2015. *What South Africa is doing to make a dent in cyber crime*. [Online]
Available at: https://theconversation.com/what-south-africa-is-doing-to-make-a-dent-in-cyber-crime-49470?utm_medium=email&utm_campaign=Latest+from+The+Conversation+for+November+4+2015+-+3749&utm_content=Latest+from+The+Conversation+for+November+4+2015+-+3749+CID_575028
[Accessed 20 December 2015].

United Kingdom, 2011. *The UK Cyber Security Strategy: Protecting and Promoting the UK in the digital world*. [Online]
Available at:
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf
[Accessed 7 December 2014].

United Nations Development Program, 1994. *Human Development Report 1994,* New York: Oxford University Press.

US Department of Defence, 2013. *Joint Publication 3-12 (R) Cyberspace operations.* [Online]
Available at: http://www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf
[Accessed 29 September 2015].

US Department of Defense, 2012. *Joint Publications 3-13 Information Operations,.* [Online]
Available at: http://www.dtic.mil/doctrine/new_pubs/jp3_13.pdf
[Accessed 11 October 2015].

US Department of Justice, 2014. *U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage.* [Online]
Available at: http://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor
[Accessed 19 October 2015].

US Senate, 2010. *Securing critical infrastructure in the age of Stuxnet. Washington, DC: US.* [Online]
Available at: http://www.hsgac.senate.gov/hearings/securing-critical-infrastructure-in-the-age-of-stuxnet
[Accessed 18 October 2015].

Von Solms, B., 2015. *What South Africa is doing to tackle cyber crime.* [Online]
Available at: http://www.fin24.com/Tech/Opinion/What-SA-is-doing-to-tackle-cyber-crime-20151104
[Accessed 22 February 2016].

Wakeford, A., 2015. *Mail and Guardian.* [Online]
Available at: http://mg.co.za/article/2015-04-15-state-agency-monitoring-cyberspace-for-isis-recruitment
[Accessed 9 December 2015].

Wolfpack, 2013. *2012/2013 The South African Cyber Threat Barometer,* Johannesburg: Wolfpack.

World Economic Forum, 2015. *Global Cybersecurity Index and Cyberwellness Profiles.* [Online]
Available at: http://www.itu.int/dms_pub/itu-d/opb/str/D-STR-SECU-2015-PDF-E.pdf
[Accessed 26 August 2016].

World Wide Worx, 2012. *Executive Summary: Internet Access in South Africa 2012.* [Online]
Available at: http://www.worldwideworx.com/wp-content/uploads/2012/12/Exec-Summary-Internet-Access-in-SA-2012.pdf
[Accessed 30 November 2014].

Zelikow, P., 2003. The Transformation of National Security Five Redefinitions. *The National Interest.*

Zetter, K., 2016. *Everything we know about Ukraine's power plant hack.* [Online]
Available at: https://www.wired.com/2016/01/everything-we-know-about-ukraines-power-plant-hack/
[Accessed 20 March 2016].