The South African National Cyber Security Policy Framework: A critical analysis

D Bote

 orcid.org 0000-0003-1705-0824

Mini-dissertation submitted in partial fulfilment of the requirements for the degree *Master of Arts in Development and Management* at the North-West University

Supervisor: Dr BL Prinsloo

Graduation ceremony: May 2019

Student number: 29563933

DECLARATION

I, David Bote, declare that *"The South African National Cyber Security Framework: A critical analysis*" is solely my academic work. All other academic literature and sources have been acknowledged accordingly through referencing. The work has not been submitted at any other institution for the awarding of a degree certificate.

ACKNOWLEDGEMENTS

Numerous people supported me in different ways to make this portion of my academic studies possible. As they say in Shona *Kuziva mbuya huudzwa* (wisdom and ideas comes from others). My gratitude is extended to all of them.

I would have not made any significant progress had it not have been the wise guidance, counsel and correction from Dr. Barend Prinsloo my mentor. I would also want to thank the Bote, Mlambo and Nhunzvi families for their part in this journey because *nzombe huru yakabva mukurerwa* (big results have small but indispensable beginnings). My colleagues Dr Maxwell Haurovi, and David Molwantwa whose encouragement strengthened my resolve in the heat of the moment, am grateful.

ABSTRACT

Contemporary security concerns emanating from or carried out via the cyber terrain have propelled states to develop policies and frameworks such as South Africa's National Cyber Security Policy Framework (NCPF) 2015. This study addresses this and other questions by analysing the efficacy of NCPF dealing with cyber security threats. In pursuing these questions, the study employs a qualitative desktop approach. A discussion on concepts and theoretical frameworks on cyber security is done. Specifically, it compares the NCPF to policy frameworks of comparable democracies such as India and the United States of America (USA). The main realisation from the NCPF is that it significantly proffers strong points that can substantially aid South Africa's cyber security posture. Some of the strong points include calls for greater coordination, cooperation and partnerships in building cyber security in South Africa. However, several loopholes or contradictory issues have been noted such as being underspecified, lacking clarity on cooperation and partnership, and flimsy implementation by the state. The main suggestion is that the NCPF need to focus more on reducing the likelihood and consequences of both intentional and accidental cyber-attacks. Finally, recommendations and areas for possible further research are suggested.

Key Words: cyber security, policy, frameworks, neorealism, state, international relations, non-state actors

OPSOMMING

Hedendaagse sekuriteitsbekommernisse wat voortspruit uit of uitgevoer word deur die kuber terrein het lande aangewend om beleide en raamwerke soos die Suid-Afrikaanse Nasionale Kuberveiligheidsbeleidraamwerk (NCPF) 2015 te ontwikkel. Hierdie studie spreek hierdie en ander vrae aan deur die effektiwiteit van die NCPF wat met kuber handel, te analiseer veiligheidsbedreigings. In die nastrewing van hierdie vrae gebruik die studie 'n kwalitatiewe lessenaarbenadering. 'n Bespreking oor konsepte en teoretiese raamwerke oor kuberveiligheid word gedoen. Spesifiek, dit vergelyk die NCPF met beleidsraamwerke van vergelykbare demokrasieë soos Indië en die Verenigde State van Amerika (VSA). Die vernaamste besef van die NCPF is dat dit aansienlike punte lewer wat aansienlik kan help om Suid-Afrika se kuberbeveiligingsposisie te verbeter. Van die sterk punte sluit in oproepe vir groter koördinasie, samewerking en vennootskappe in die bou van kuberveiligheid in Suid-Afrika. Daar is egter verskeie skuiwergate of teenstrydige kwessies aangeteken, soos onbepaald, gebrek aan duidelikheid oor samewerking en vennootskap, en swak implementering deur die staat. Die belangrikste voorstel is dat die NCPF meer moet fokus op die vermindering van die waarskynlikheid en gevolge van beide opsetlike en toevallige kuberaanvalle. Ten slotte word aanbevelings en areas vir moontlike verdere navorsing aanbeveel.

Sleutelwoorde: kuberveiligheid, beleid, raamwerke, neorealisme, staat, internasionale betrekkinge, nie-staatsaktore

ABBREVIATIONS

ACDC	Active Cyber Defense Certainty Act
CERT-In	Indian Computer Emergency Response Team
CERT	Computer Incidence Response Team
CIA	Central Intelligence Agency
CIS	Centre for Information Security
CNA	Computer Networks Attacks
CNE	Computer Networks Exploitation
CRC	Cybersecurity Response Committee
CSIR	Centre for Scientific and Industrial Research
Constitution	Constitution of the Republic of South Africa
DFARS	Defense Acquisition Regulatory System
DHS	Department of Homeland Security
DOC	Department of Communications
DoD	Department of Defence
DTPS	Department of Telecommunications and Postal Services
EU	European Union
FBI	Federal Bureau of Investigation
GDPR	General Data Protection Regulation
HAWKS	Special Investigative Unit
HITECH	Health Information Technology and Clinical Act
IB	Intelligence Bureau
IISS	International Institute of Strategic Studies
ISS	Institute for Security Studies
ISO	International Organisation for Standards
JCB	Joint Cipher Bureau
JCPS	Justice, Crime Prevention and Security

NATO	North Atlantic Treaty Organization
NCAC	National Cyber Security Advisory Council
NCCC	National Cybercrime Coordination Centre
NCIIPC	National Critical Information Infrastructure Protection Centre
NCPF	South Africa Cyber Security Policy Framework (NCPF)
NIST	National Institute for Standards and Technology
NSC	National Security Council
NSA	National Security Agency
PCIDSS	Payment Card Industry Data Security Standard
SADC	Southern Africa Development Community
SANDF	South Africa National Defence Force
SAPS	South African Police Service
SITA	State Information Technology Agency
SSA	State Security Agency of South Africa
STEM	Science, Technology, Engineering and Mathematics
UNSC	United Nations Security Council

TABLE OF CONTENTS

CHAPTER 1: INTRODUCTION

1.1 BACKGROUND

The essential role of a state in safeguarding its territory, people, sovereignty and interests has not changed much over the years (Williams, 2008:3; Segal, 2016:2). This role is however persistently under threat, and in view of mounting threats emanating from and carried out via the cyberspace, states are being compelled to review and enhance their security policies (Barzashka, 2013:48; Betz and Stevens, 2012:4; Slack, 2016:69). Across the world, states are grappling with altering security policies to effectively assert their control, power and sovereignty in a bid to protect their varied interests. Cyberspace security is now garnering unprecedented attention from state security actors, academic experts, policy makers and human rights activists (Siman-Tov, 2012:35; Paalman, 2013:5; Bodmer *et al.*, 2014:2; Even and Adamson, 2016). Belk & Noyes (2012:9) contend that the development of cyber threats and weaponry has happened at a faster magnitude than of, 'any other battle space in history.' The complexity of cyberspace security challenges is compounded by the fact that threats can emanate from domestic or foreign, as well as state or non-state sources.

Chapter 11 of the South African Constitution (1996) and related legislation gives emphasis on state security as critical. 'State security', as conceptualised by Jetschke (2011: 3), is a state's protection that is in a fundamental way challenged from inside or outside. National security matters are to a large degree vested in the executive as well as in core security apparatus of the state such as defence, intelligence and police (Beach, 2012:34). This means building better capabilities to deal with local and international threats. Thus, a proper policy based on defence preparedness is necessary to safeguard property, lives and territorial integrity.

1.1.1 Neorealism

Neorealism is a strand of realism which has been the dominant theory of international relations in the world, with several implications to security studies (Telbami, 2002:158). Notable contributors to the approach include Kenneth Waltz, Henry Kissinger, Arnold Wolfers and Stephen Walt. The approach makes it explicit that states, above all other factors, seek self-preservation (Beach, 2012:20). This means, states place their own interest first and do not subordinate their interest to the interests of other states. A second dimension of neorealism is that states may have different preferences. At the same time states also seek to maximize influence where possible. Accordingly, neorealism has been particularly influential in security studies as it looks at defensive and offensive postures of states. In the context of South Africa, defensive realists will advocate for building robust defensive capability to deter and deal with cyber-attacks, whereas, offensive realists would advocate for South Africa to enhance its offensive capabilities for attacking other states and non-state threats as a means to increase their relative power. In other words, offensive

realists argue that South Africa would be better positioned should it acquire and develop its own arsenal of cyber war. This will be discussed in greater detail later.

1.2 CYBER SECURITY POLICIES IN SOUTH AFRICA

Cyber security has been elevated from a barely mentioned security concern to one of the greatest security dangers confronting nations across the world (Hare, 2010; Siman-Tov, 2012:37; Paalman, 2013:6; Bodmer *et al*, 2014:3; Even and Adamson, 2016). Cyber security risk is ranked 8 out of 10 on the likelihood of impact by the (Global Risk Report, 2016). Providing a policy and governance framework for cyber security for securing state interests from cyber threats has been gaining urgency given the frequency, scale and possible intensity of attacks in the interconnected world (Tang, 2009:587; Santos, 2018:4). States such as Australia, India, United Kingdom, China and Netherlands have adopted cyber security policies and strategies. Equally so, cyber-security has gradually become a top national priority for the South African government (State Security Agency (SSA), 2016). Essentially, the South Africa Cyber Security Policy Framework (NCPF) spells out standards, procedures, methodologies, and processes to address cyber threats and attacks in South Africa (Government Gazzete, 2015).

The current and future cyber warfare is changing the way in which the security apparatus in South Africa is preparing for possible breaches and it is equally challenging security governance (Bendiek and Metzger, 2015:4). What has been more salient is that in the process of governing the space, states are being challenged to come up with policies and a governance framework that addresses security issues. Cyber has emerged as a pressing security concern in recent years, with states facing threats from many angles (Cavelty, 2014:702; Radu, 2014:3). There have been concerns over how policies on cyber security have several adverse implications on liberties, privacy, and civil society activities (Nojeim, 2010:119; Hart *et al*, 2014:2862; Rigoglioso 2014:5).

Cyberspace securitisation is contentious and brings along with it several controversies with regard to how policy framework identifies a challenge(s) and proffers solutions (Guitton, 2013:22; Stevens, 2016:180). Efficacious representation of something as an existential threat to a referent object legitimises apportioning of resources as well as change of strategy (Diez *et al*., 2016:15). For example, a security policy may be used as a means toward dissenting voices as well as legitimising internet censorship in both mature democracies and authoritarian states. Through securitization, it is justified that the issue is dealt with in an extraordinary manner, usually above the normal political rules and level (Buzan *et al*., 1998:239).

As Considine (1994:1) concedes, “policy making is a powerful political tool”. In order to build a resilient cyberspace South Africa launched the Cyber Security Policy Framework designed to secure assets and protect people (Government Gazette, 2015). In other words, the broader

objective of this policy framework is to create a secure cyberspace environment and reinforce the regulatory framework. Among other factors, the aim is to protect information infrastructure in cyberspace, reducing vulnerabilities, build capabilities to prevent and respond to cyber-attacks and threats. It also seeks to minimize damage from cyber incidents through an amalgamation of institutional structures, people, processes, technology and cooperation (Government Gazette, 2015). What is more important is a deep scrutiny of the details of the NCPF to untangle it vis-à-vis the tenets of a policy.

This study provides a critical analysis of the NCPF that was approved by cabinet on the 7th of March 2012 for public information. The draft of (NCPF) appears on Government Gazette, 4 December 2015, and was driven by the State Security Agency of South Africa (SSA).

1.3 PROBLEM STATEMENT

South Africa is among countries that are deemed most vulnerable in the cyber domain, thus necessitating a critical review of the NCPF *vis-à-vis* other similar policies. For South Africa, any substantial disruption emanating from cyber space is a threatening prospect. Yet little critique has been presented on the NCPF, particularly with regard to whether it can be classified or qualifies as a policy. This means assessing if it conforms to the core elements of policy frameworks and questioning if it can address the evolving patterns in cyber security challenges. Understanding the NCPF is especially important because of the wider implications towards implementation and evaluation of the performance of the document. The implications are both in the short-term as well as in the long-term. A poorly designed security policy is a high-risk factor for South Africa as it exposes the country's vulnerability to the mounting and fast evolving cyber threats. A comprehensive analysis of the adequacy and robustness of the 'policy document' adds more understanding to the nature of the NCPF and whether it can achieve its self-stated aims to protect information infrastructure in cyberspace, reduce vulnerabilities, and build capabilities to prevent and respond to cyber-attacks and threats. It also seeks to minimise damage from cyber incidents through an amalgamation of institutional structures, people, process, technology and cooperation. The primary research question is therefore: *How robust and comprehensive is the NCPF to achieve its self-stated goals?*

1.4 RESEARCH QUESTIONS

1.4.1. What are the theoretical underpinnings of cyberspace security?

1.4.2. What are the main elements of a security policy framework such as the NCPF?

1.4.3 How effective has the NCPF been since being introduced to achieve its self-stated aims?

1.4.4. Is the NCPF a sufficient policy framework for cyber security in South Africa?

1.5 OBJECTIVES OF THE STUDY

1.5.1. To analyse and explain the theoretical underpinnings of cyber security.

1.5.2. To identify the key elements of a security policy framework such as the NCPF.

1.5.3. To assess the effectiveness of the NCPF against its stated aims.

1.5.4. To provide recommendations to cyber policy development in South Africa.

1.6 CENTRAL THEORETICAL STATEMENT

South Africa, just like many other states in the world, is yet to have reliable partners to which it can delegate the responsibility of securing its cyberspace. Neither can it look to international collaboration nor cyber supranational bodies. The study uses the neorealism approach as its central theoretical statement. Neorealism, as a theoretical approach, has three compelling points that can be expanded by this particular study. Firstly, it has the ability to enrich the understanding of the nature and scale of cyberspace security challenges for states (Tuthill, 2012:24; Kaiser:2015:11). Secondly, the approach has persuasive explanatory and analytical power, which is relevant for policy analysis and improvement. It has a compelling ability to explain the behaviour of the state in crafting security policies (Singer and Friedman, 2015:163). As such, if a policy lacks ability to address future challenges it will likely cause severe harm to the security of a state such as South Africa because the state will not be well prepared against such threats. Neorealism proffers a rigorous and plausible way of analysing NCPF. Importantly, the theoretical context for the policy is characterised by competition for power, survival calculations and a host of threats, which are either state or non-state. Resende-Santos (2007:13) augments this argument by saying that the power of neorealist theory is that, “it predicts that state will emulate successful practices from other states.”

Cyberspace represents an economic, political, social and strategic domain for South Africa’s security. Reardon and Choucri (2012:6) contend that, ‘realist theories of deterrence, crisis management, and conflict may be used to understand whether cyberspace is stabilising or destabilising, whether cyber technologies will be a new source of conflict or of peace, and whether states will engage in cyber arms racing.’ In accordance to neorealism, a state needs to make rational choices in order to deal and position itself in the constraints of the security ecology (Nye, 1988:238; Brown, 2009:257). This helps the state to establish structures and coordinate institutions so that it addresses a challenge holistically. Unlike the classical realism approach, neorealism emphasises on a coordinated approach to security. This calls for an analysis of institutions and collaboration across layers of government. The theoretical approach therefore helps to assess the comprehensiveness of the policy in light of neorealism. Further, the theoretical approach is robust in its capacity to help come up with actionable recommendations for a strong policy. The neorealist approach can be further developed and refined for the analysis of cyber security policies. Thirdly,

and more importantly, neorealism is by no means absolute or comprehensive. Neorealism is thus best conceived as a framework for further inquiry, not as the end of inquiry.

1.7 METHODOLOGICAL FRAMEWORK

A methodological framework is a structure that puts in place the parameters for how the research study will be undertaken (Ravitch and Carl, 2016:24). In other words, it entails the rationale and justification for a particular methodology approach, methods and analysis. That is essentially the sequence of the methods.

1.7.1 Methodological approach

A qualitative approach was used in this study. Denzin and Lincoln (2011:8) say qualitative research emphasises on the qualities of entities, processes and meanings. In other words, a qualitative approach underscores the socially constructed nature of reality as well as the value-laden nature of inquiry. The main reason for adopting this approach was that policy, by nature, is value laden. On this account, this research focused on policy by unpacking the arguments, goals and implementation of the policy. The second reason for employing qualitative approach stemmed from the systematic data limitations in cyber security. Finally, notwithstanding some of the weaknesses of a qualitative approach, it provided an in-depth understanding of phenomena (Mahoney, 2010:128).

1.7.2 Data collection instruments

The study was a desktop-based research that utilizes available literature, published and unpublished. These articles include policies, scholarly studies, speeches, legislations and other reports on cyber security in South Africa. The North West University Library services was utilised to specify journal articles and databases that aid this particular study. Targeted electronic databases and research registers include;

- Ebscohost,
- Jstor
- Proquest Social Science Search that houses World Wide Political science abstracts, PAIS international, and International Bibliography of Social Sciences (IBSS).
- International security and terrorism reference centre.
- Sage
- Google Scholar
- Scopus
- Social Science Research Network
- Praeger Security International

Other sources encompassed government publications, official speeches by public officials, military publications and intelligence publications. Other publications such as International Institute of Strategic Studies (IISS) Cyber report and Institute for Security Studies (ISS) were also utilised.

1.7.3 Strategy for data analysis

Collected data was categorized using axial coding. Axial coding essentially entails disaggregating fundamental themes during a qualitative data analysis process (Klenke, 2016:100). The process included relating concepts, theoretical perspective, phenomena and relationships, using an amalgamation of both inductive and deductive reasoning. First, a comparison of policy frameworks and then juxtaposed with cyber security theory. Accordingly, this involves synthesising the components of the policy in a systematic manner. To a large degree, the use of procedures is highly focused, and is, "geared towards discovering and relating categories in terms of the paradigm model" (Corbin and Strauss, 1990:4). In particular, the researcher is better positioned to answer qualitative research questions pertaining to *what, when, why, where, how and with what* (Saldana, 2013:3; Theron, 2015:2). The end result is to answer the main research question, and thus, consequently address the objectives of this research study.

1.8 ETHICAL CONSIDERATIONS

Given this primacy of observing ethics in research, concerted attention is devoted toward making sure that this study is consonant with the basic ethical rules of the North West University. The study was reviewed by the North West Research Committee to adjudge its ethical fit. Plagiarism was avoided by acknowledging the sources of data used in this study. All literature used in the study such as journals articles, books, electronic sources, newspapers are duly acknowledged (Jordan and Hill*,* 2012). Accordingly, all the data sources used are found on the reference section at the end of the last chapter. Sources of literature include the NCPF document, comparable policy documents from other nation-states such as India, United Kingdom (UK) and US, as well as cognate scholarly literature.

In terms of data reporting, ethical principles of avoiding harm, upholding privacy and anonymity are upheld. Finally, the research strives to report the results honestly and objectively, and acknowledge all the external sources of information used for this research.

1.9 LIMITATIONS OF THE STUDY

1.9.1 Limited literature as a result of the sensitive and secretive nature of cyber security information from states is a matter of concern.

1.9.2 The fast-paced nature of cyber developments may compromise analysis process.

1.9.3 The study does not use classified material.

1.10 SIGNIFICANCE OF THE STUDY

There is no scholarly analysis on the NCPF from a security standpoint. This study is hence original and seeks to plausibly look at the issue from a security studies vantage point, thus it broadly adds to relevant academic literature. Against the background of mounting cyber security challenges this study is relevant to the discipline of political studies, specifically security studies specialisation within the North West University. Furthermore, the study is significant to international relations and security analysis, both in the government, private sector and in non-governmental organizations. The study is pertinent to law enforcement, military, intelligence and private security actors. It is of value to those interested in cyber security issues the world over, especially from the perspective of a developing country.

1.11 CHAPTER LAYOUT

The first chapter of the study covers research background and introduces key concepts underpinning this study. Chapter 2 discusses literature and the theoretical framework which undergirds this research study. Chapter 3 focuses on the South Africa Cyber Security Policy Framework. Chapter 4 analyses the cyber security in light of policy frameworks, proffers suggestions and recommendations that can be adopted in South Africa.

1.12 CONCLUSION

This chapter introduced the research background, described the problem statement and covered the key research questions undergirding the study. It went further to articulate the key objectives and the main theoretical standing. Ensuring sections described methodology to be employed as well as the data analysis considerations. Ethical issues regarding the study were also covered, the delimitation and significance of the study was equally spelt out. The next section discusses cyber security theoretical frameworks in detail.

CHAPTER 2: THEORETICAL FRAMEWORKS

2.1 INTRODUCTION

Questions of cyber security dimensions such as war, safety, espionage, intelligence, diplomacy, threats and attacks are anchored in theoretical foundations. This chapter discusses the theoretical basis for cyber security policies in a contemporary world. Given the wide expanse of theoretical approaches that could explain issues around cyber security this study primarily focused on three dominant approaches. It selects some of the dominant approaches in thinking about security and explains their persistence and relevance to this particular research study. These three are namely, realism (neo-realism), liberalism and constructivism. Specifically, the chapter addresses the foundational dimensions of cyber-security in a theoretical framework.

Theoretical approaches in security studies are equally contested and there is no unanimity on which one is supreme. Kallberg (2016:102) defines theory as, “an overarching way of combining ideas, phenomena, and facts, in a generalized form, to seek to explain specific outcomes.” Put otherwise, theory is a strong basis for making predictions, undergirds policies, explain phenomenon, and to understand social dynamics. Most security related theories emphasize on aspects such as power, ideological inclinations, material interests and the architecture of international affairs. At the heart of security studies are three foundational questions which theory ought to address in one way or the other (Hough *et al*., 2014:2), namely:

- What is the referent object of security?
- What are the threats it faces?
- How should the referent object be secured?

To a considerable degree the slant in the discussion of cyber security theories is on policies. As alluded to in the introductory chapter, states and non-state actors are developing cyber capabilities and engaging in cyber warfare, both offensively and defensively. The chapter delimits itself to three theoretical approaches, namely: realism, constructivism and liberalism. The rationale for discussing these is informed by the fact that they are perhaps the most widely used for state security rationale. It is crucial to underscore that theories of security studies are both externally and internally contested, as such the approach adopted can be plausibly challenged. Be that as it may, the first choice theoretical approach underpinning this study is neorealism, the rationale for adopting the approach is expounded broadly in the ensuing sections. In other words, the choice for neorealism does not preclude the positives of other alternative approaches, but rather it provides a great degree of efficacy to the analysis of this study.

2.2 REALISM AND CYBER SECURITY

Bevir (2010:1168) posit that realism is an international relations theory which has taken several forms over the past millennia. It is however not a single theory but is a constellation of various strands such as defensive realism, classical realism, offensive realism and neorealism (Kostagiannis, 2018:6). It also has several versions such as hegemonic stability theory, balance of threat theory, balance of power theory and power transition theory. It is an approach deeply influenced by rationality, individualism and materialism. Major realist thinkers include Sun Tzu, Thucydides, Hans Morgenthau, Nicollo Machiavelli, Thomas Hobbes and Mao Tse Tung. Essentially, its proponents, "describe themselves as dispassionate observers of the 'realities' of international life-as opposed to the imagined faith of their intellectual rivals, whom they designate 'idealists' (Bevir, 2010:1168).

At a micro level, realism emphasises rationality and individualism. Therefore, the nature of human thinking or the organisation of international politics is based on self-aggrandisement in a world without an effective mechanism for addressing competition. In the first instance human beings in any social setting desire power to control or master others as has been argued by the likes of Reinhold Niebuhr. The quest for power is considered 'insatiable and ineradicable' as it permits for one to become dominant over others (Donnelly, 2000:10). The human desire is driven by not only the offensive pursuit for power but also the defensive goal of avoiding being dictated to by others. In other words, human psychology has an *animus dominandi* which makes politics a contestation for power. In international affairs the pursuit for power is practised at the grandest scale and security issues become more of the practise of politics by other means.

At a macro level, contestations are mostly inter-state according to realism (Hobson, 2000:5). The second dimension of realists is at the macro level of the international system. This system is seen to be characterised by anarchy, meaning there is no single authority with the legitimate authority to use force. Put alternatively, the core view is that anarchy compels and locks states into unending security rivalry. Each state is regarded sovereign. As such, this is a self-help system in which states use all available instruments of power such as diplomacy, military, economic and intelligence to protect themselves when necessary. A state will seek to defend and advance its national interests. A state normally uses instruments of force as a last resort, as a way of exercising control over other actors on its territory. Externally, states do not voluntarily let other states or other international bodies to exercise control over them.

Since in the eyes of the realists, politics is based on the unquenchable pursuit of power it is thus difficult to have an international system which can govern the affairs of states (Kostagiannis: 2018:1). Put otherwise, even international institutions such as the United Nations can be subverted by powerful states that have *defacto* control over the agenda of these bodies. Arrangements in

international institutions favour powerful states, for example, the most powerful grouping in the UN Security council is the five permanent members Russia, United States of America, France, China and the United Kingdom. The agreements in such bodies can be used by dominant players to further their own agenda and harass those who do not conform to their demands. Accordingly, states without power in such bodies cannot expect much in terms of their cyber security concerns because most of the decisions would have been hammered out to favour the great powers. It is thus viewed as foolishness by the realists for states to completely throw their trust in international institutions as such doing is emasculating. Moreover, malevolent states or non-state players are likely to subvert the principles of international bodies in pursuit of their own affairs with little consequences to their actions. In other words, morality or sincerity is likely to be thrown out the window when it ceases to serve the interests of players.

For the realists the international system is characterised by fear, threat and suspicion (Waltz, 1979:102). Cooperation by states is vital only if it serves the interests of the concerned state. But states will have to be vigilant against a possible 'cyber-Pearl Harbour' as alluded to by former US Defense secretary Leon Panetta or "Cyber 9/11" (Nacita & Reith, 2018: 76). Sienkiewicz (2017:7) underscored that nation states leverage the cyber, predominantly the internet for military, espionage, political and economic reasons. They therefore cannot afford to leave the cyberspace to be used for activities which undermine state authority. He goes further to say, "there are hundreds of thousands of cyber actors" and the boundaries are both visible and invisible. In such a chaotic world, states are in a self-help situation.

Moving on, security is thus a political tool designed to serve the interests of the state or the groups which control the arms of the states. Components of security such as war, intelligence espionage, cyber security and diplomacy tend to be run by the executive in many states. States are worrisome of the destabilisation implications of cyber-attacks. One can give reference to the alleged interference by the Russians into the US electoral system. Cyber security according to realism is not a matter of morals or ethics, but goes to the heart of defending state sovereignty. For states to thrive in this unavoidably anarchic system they cannot rely on the benevolence of other actors. States also find themselves in an uncertain international system in which the future is difficult to forecast. The adverse activities in the cyber space are equally difficult to foretell. Moreover, states hardly can be certain of the intentions and actions of other states, even other non-state actors.

States are the main actors in the cyber space, with the United States Government having been at the heart of the development of the modern cyber system, via the internet. In addition, states are in control of infrastructures such as satellites, telecoms infrastructures, data centres, can spy on content and regulate communications protocol. Not only that, states are at the centre of defining the rules and regulations around the cyber space. A classic example of such is the General Data

Protection Regulation (GDPR) which was put forward by the European Union in 2018 (European Commission, 2018). This is particularly telling in powerful states such as the US and in China where the government has a firewall to monitor the internet. Considerably, states have the power to control the usage of the internet and other cognate elements of the cyber-physical systems.

The ways in which states are responding to cyber security issues is partly informed by realism. States now play a critical role in cyber security by themselves operating several units that operate the cyber space. For example, several states have cyber commands, cyber policing units, cyber armies, cyber defence agencies and cyber armies. Virtually every state is in the process of institutionalising cyber security via policy documents such as strategies and doctrines. Dipert (2010:384), underscores that cyber security issues are not amenable to present international cyber warfare. Cyber weapons expand the already available armouries in the hands of actors, thereby multiplying the possible harm that could be inflicted on rivalries or victims. According to Kello (2017:56) states are the cyber domain principal players as they possess the means to undertake sophisticated offensive attacks.

Whereas, power and security are considered as most valuable by states. Moreover, the cyber domains influence virtually every capability of the military (Brantly, 2016:1). Therefore, cyber can be viewed as an extension of traditional weaponry as well as traditional conflicts. For example, Russia can use the cyber to fight its wars against the United States.

The quest for power in the cyber space is heating up, with major powers being at the forefront of most recent salient spats (Sienkiewicz, 2017: 5). Large nation states such as US Russia and China have been leading the pack. Not only that, even small states such as Iran, Israel and North Korea have been involved in several contestations. It is therefore logically reasonable to contend that most of these states have, to a large degree, been informed by neorealism. The US leads as it has been at the very heart of the evolution of the cyber since the development of the telecommunications networks in the 19th century. Europe and North America play host to the densest and advanced telecommunications system and have more connectivity in terms of submarine fibre optics as well as wireless communications. Due to the industrialisation nature of advanced states, they have been at the forefront of cyber security.

The coming of the fourth industrial revolution is continuously exposing weaknesses in the cyber security dynamics (Valeriano & Maness, 2015:2). As such actors are on their own when it comes to defending themselves. Moreover, the cyberspace is also worsening the nature of the anarchic world as seen by realists. In other words, it cements the argument for states being more vigilant and less trusting to each other. One example to illustrate this point is on the question of attribution. In the other domains of warfare such as land, sea, and air, attribution is relatively easy to

apportion. But this is not the case with cyber, where anonymity is a major defining characteristic. Accordingly, the cyber space develops to be an enticing alternative for states or non-state actors to undertake aggressive actions against not only other states but non-state actors as well. Cyberspace by its nature makes the international system even more anarchic. Moreover, the cyber domain is relatively cheap to operate in, and the multiplicity of actors involved makes it an equivalent of the 'wild-west.' What worsens the situation is that there are no international police on cyber, neither is there international law on cyber conflicts or war in general. Some of the available laws such as the European Convention of Cybercrime are hardly universal and are mainly applicable within the boundaries of few states.

The anarchy in cyberspace is likened to, "swimming in a dirty pool" (Valeriano & Maness, 2015:2). It is reasonable to argue that the absence of cogent international cooperation on the cyber security front, states or even non-state actors have little confidence and trust in each other. In other words, one actor is not entirely sure of who is who in the cyber jungle and even the so called allies present credible threats. For example, WikiLeaks documents showed how European states were spied on by the US despite being allies. Furthermore, not all states have clear cyber security strategies, as most of their activities are deemed highly secretive and confidential. The opaque cyber strategies heighten the security dilemma.

Another vexing component which diminishes cooperation and festers tension amongst states is around lack of common definition as to what governance model to have in place (Jayawardane *et al*.,2015:5). Thus cyber security has to encompass physical components such as fibre networks, wires, routers, storage systems and data bases. The other component deals with securing flows of information. Cyber security in the military, the most critical security actor for the state, cyber agencies are manned by advanced computer and information technology (IT) specialists, programmers who design offensive and defensive tools (Harris, 2014:39). This component of cyber weaponry is also a factor which is necessitating states to engage in cyber arms race (Stadnik,2017: 31).

At the heart of cyber security is that technology is a tool for power as it encourages information dominance, political dominance, economic dominance as well as military power. As such, states are locked in cyber-technology battles in order to amass as much power as they can as it is a platform for being victorious against enemies. In the same regard, realists will be awake to the fact that cyber technologies are a fountain of threats against the state, society, peace, military and even industry. As such, several measures are taken to enhance both defensive and offensive capabilities. Moreover, the view is that a state ought to be well prepared especially in light of deepening dependency on cyberspace. Major states such as China and the United States of America possess credible defensive and offensive cyber capabilities (Stadnik, 2017:138).

2.2.1 Neorealism and cyber security

Neorealism borrows heavily from the basic assumptions of realism. Its main point of departure is that it argues that the systematic structure of the world influences international interactions. The main premise is that of anarchy, survival, uncertainty and effective offensive. Moreover, power maximisation is key in a self-help international system. As such, states are bound to be in defensive mode and the system is characterised by the bipolarity of major powers. But a bipolar system is regarded to be more stable relative to a multi-polar system. For neorealism to be particular, the uncertainty about the present and future interests of others, especially those driven by security motives lead a state to be security-seeking. In other words, should states be unprepared they risk being deceived by others and fall victim to several demanding security motives. Unlike realism which considers the state as the unit of analysis, for constructivism there can a number of units of analysis.

Essentially, for neorealism, cyber space is an important political instrument necessary for furthering the interests of the state. This means cyber war is only a means not necessarily the end for states. The glaring weakness of realism is that it considers non-state actors to be unimportant; as such they are not of relevance to cyber security. Realism does not however give much credence to the exercise of power by non-state actors in the international security system. Unlike in other domains of warfare, the role of non-state players in cyberspace is more pronounced and profound. Another shortcoming is the manner it discounts how security is constructed as well as how cooperation has helped to cut the levels of conflicts between states.

2.3 CONSTRUCTIVISM AND CYBER SECURITY

Constructivism is one of the key theories in international political subfields such as security (Weber, 2014: 68). It has been particularly influential in the 1990s to the turn of the 21st century but has its roots in Western thought of the likes of Emil Durkheim, George Hegel and Max Weber (Telo, 2009:117). It was later expounded by the likes of Nicholas Onuf (1989), Friedrich Kratochwil (2000) and Alexander Wandt (1992). It has been regarded a powerful approach in analysing events such as the collapse of the Soviet Republic (ibid: 9). It is essentially a portion of the interpretivist social theories (Guzzini, 2013:5). Thus in light of constructivism cyber security can be seen encompassing a ‘congress of disciplines’ to borrow from Kello (2017:27). As such the manner in which it is defined is mostly influenced by fields such as law, engineering, philosophy, political science, criminology and computer science. And the gallery of actors includes states, private companies, other non-state operators and quasi-states such as the Islamic State of Iraq and the Levante (ISIL).

Constructivism at its core argues that people act towards something based on the meaning they give to something, and, “the objects themselves do not determine meaning” Guzzini, 2013:5). The core concepts around constructivism are, “deliberation, discourses, norms, persuasion, identity, socialization, arguing” (Checkel, 2011:5).

There are three key elements of constructivism in theorising international politics (Copeland, 2006: 3). First, global politics is steered by intersubjective mutual norms, ideas and values held by actors. Second, the ideational structure has a constitutive effect on actors. This structure of ideas leads actors to define and redefine their identities and interests in the interacting process. Constructivism, therefore, considers how the ideational structure shapes how actors define their goals, whom they are and the role they must play. The third element is that the actors and ideational structure co-determine and co-constitute each other. That is, the structures are made up of actors in terms of their interests and identities. And the same structures also alter, produce and reproduce the practices of agents. Agents can change structures and vice-versa. By and large, the essence of constructivism is that the reality as defined by actors is historically assembled and contingent. That reality is a mere product of past social practices that influence interpretations, expectations and beliefs in international affairs thinking.

Principally, Barkin (2010:165) underscores that constructivism is “about the social, which is to say intersubjective, construction of international politics.” Decisions on security are based on the prospects of interactions between actors. Thus, it will be in line with Nye, (2010:19) that, “the cyber domain is likely to increase the diffusion of power to non-state actors, and illustrates the importance of networks as a key dimension of power in the 21st century.”

Far from an objective reality, international politics is ‘a world of our making’ (Onuf, 1989:36). For constructivism, ideas are potent drivers of political and social change, thus including questions around security. Cyber is therefore not just virtual-physical issues but something much more depending on whom and how it is viewed. To a greater degree, constructivism is able to show how politicians and security decision makers design cyber security policies and the reasons that inform their vantage points. It partly explains why cyber is being considered a security concern in numerous security related policy documents.

It essentially argues that the identities of states are not static, but they are dynamic. Alternatively expressed, identities and interests of states are always in a state of flux. It sees the views of the world by states as ‘what they make of it’. In other words, reality is all about how it is constructed. Put simply, the theory stresses the importance of subjectivity of the ideas that shape the behaviour and identities of various actors. One of the most vocal proponents of constructivism is Alexander Wendt (1992:394) who challenged the realist view that anarchy forces states to be in perpetual vigilance when it comes to security. His argument is that the so called anarchic state of the world is

a result of “shared culture created through discursive social practice” (Copeland, 2006:1). Thus, cultural manifestations are a result of one’s conception of ‘interest and identity’. The international system is therefore made-up of intersubjective culture, which can be altered over time. If applied to state security or cyber security to be specific, constructivism denotes the manner in which actors define what is to be secured, how it should be secured and with what means. In other words, the construction of security is mainly in the hands of key security actors, if it is the state such power resides in the hands of politicians and security leaders.

The constructivist approach to cyber security makes a strong contribution to the understanding of cyber security and related issues. First, it brings into light the debates around what ought to be secured, securitisation as argued by Buzan *et al*. (1998:5). Essentially, a securitisation process is used to justify policy making and to reinforce legitimacy of security policies. It therefore encompasses mainly the views of elites through their actions and speeches. A concern around cyber can in other words be moved into a national security concern by the elite. The threat(s) are identified and the referent object to be safeguarded is also identified. The audience is sold the idea of securitisation, which in many regards accepts the elite view. Moreover, the action that needs to be taken is also pronounced.

Securitisation of cyber is obtaining across virtually every state and it has substantive consequences. This securitisation process often gives birth to novel laws, security doctrines and new strategies around cyber. Moreover, many actors often create institutions that are geared towards addressing the identified security concerns. For example, this may see the establishment of new cyber security units, new cyber militaries and a broad reorganisation of the state security apparatus. The implications of securitisation are broad and deep, they encroach into issues of freedoms, privacy and liberties of citizens. In other words, securitisation may create tensions between players within a state.

Certain complicated questions arise with regard to securitisation pertaining to how, when and why something can be regarded a cyber-security issue. Put differently, how a particular issue is going to become an economic, security, political and societal issue. The securitisation of the cyber can be traced from way back in the second world war when computers were at the heart of security during the world war two. Computers were basically developed as a security tool aimed at aiding the winning of wars. As such from the 1950s funding was provided by the US agencies such as Central Intelligence Agency (CIA) and National Security Agency (NSA) to speed up computer research. Furthermore, the period around the Cold War (1947-1991) was characterised by states trying to defend their computer systems especially the nuclear components. By the turn of the 21st century the protection of computer systems has risen to be a major security issue for states, particularly major powers.

The global nature of computer systems has made cyber an international concern. This view is compounded by the number of actors with the capacity to launch global attacks, either directly or indirectly on states. These actors include individuals, organised groups, states and terrorists. In other words, in the view of macro-securitisation enemies are everywhere. Attacks in or on a state can be viewed in many ways, as attacks of value systems or attacks on an economic way of life. For the United States, marked enemies are those who pose a threat to the American value system as well as the traditional enemies such as Russia, Iran and China. Wendt (1995:73) aptly expresses this point by saying, “500 nuclear weapons in the hands of the British are less threatening to the US than 5 North Korean nuclear weapons.” In other words, North Korea is perceived to be an enemy and the British an ally.

The manner in which security actors perceive reality is likely to determine their actions in both cooperation and competition. Thus, states are more likely to cooperate should they view their counterparts to be doing so in goodwill and they are more likely to be hostile to those seen to be existential threats. A state or non-state actor perceived to be a key rival is most likely to be included in policy documents as such. For example, the US labels states such as Iran and Russia as rival in cyber security not just because there is a material basis for such, but because of perception as well. The manner in which polices frame cyber threats are mostly a result of perception, the constructivist will argue.

Stadnik (2017:141) posit that securitisation can be used to analyse the intentions of actors by looking at their discourse. Thus, how threats are represented by the various actors remains a key question in constructivism. As such, Stadnik (2017: 141) further underscores that cyber security discourse is particularly different in three countries China, Russia and US. Some commonalities are that these three states seek to mitigate against the adverse implications on national security however it is defined. China and Russia emphasise sovereignty in the cyber space as key *(ibid).*

According to constructivism the conceptual model for cybersecurity is contestable for it is historically and ideationally determined. By and large, the social reality of cyber security is subjective, and a human invention or interpretation. More importantly, the state is not the only actor in international affairs and norms of security are a product of interactions between various actors including states and non-state actors such as NGOs. Barkin (2010:154) contends that one of the weaknesses of constructivism is that it is conceptually overstretched. That is, it runs the risk of being meaningless. The constructivist view has however been criticised for failing to take into account the problem of uncertainty which is a reality in the contemporary world. Nonetheless, it is a strong theory for analysing cyber security policies for they are equally a socially constructed phenomena.

Cyber security threats have changed the social structures of security and conflicts, their norms and participation rules. In cyberspace, the social structure of violence is blurred and the lines between civilians and combatants are unclear. Hence, an interpretation of the current cyber security policy and its threats help us to better understand the events and actions from cyberspace. Constructivism may view the cyberspace in light of how it is being used to advance religious, ideological, cultural, political and social agenda. This explains the use of social media by terrorists' groups such as Boko Haram, ISIL and Al Qaeda. In closing, for constructivism, domestic security issues are integrated into international security. According to constructivism, states are the fundamental actors, but other non-state actors matter.

2.4 LIBERALISM AND CYBER SECURITY

The liberal approach has its roots in the 18th century in the enlightenment period, and was led by thinkers such as Jeremy Bentham and Immanuel Kant. Jackson and Sorensen (2007:97) posit that the liberal approach is convinced that international politics and relations can be 'cooperative rather than conflictual'; that human nature is positive and believes in a progressive politics. At the micro level, the liberal approach takes a more positive view concerning human nature and believes that humans can conflict but can share certain interests and can work cooperatively and collaboratively (Jackson & Sorensen, 2007:97). Actors, should they work in unison, can improve both the material and moral condition of the world. Some of the famous successes of liberalism is the formation of the League of Nations in 1919 and the Kellog-Briand Pact (1928). The liberal approach contends that domestic structures and actors influence the external behaviour and identities of states.

At a macro level, liberalism places emphasis on international institutions, "including international rules, norms, principles, and decision-making procedures". This can help to facilitate cooperation even in the face of a security dilemma (Stadnik, 2017:140). In particular, international institutions play a central role in restraining the behaviour of states and encourages cooperation. The argument for having international institutions which govern state affairs and encourage cooperation has the potential to constrain aggressive behaviour. In other words, liberalism sees itself as having the potential to address the "cyber security dilemma" dogging the international security system at present. Liberalism will also acknowledge and incorporate both state and non-state actors in this international institution (Stadnik, 2017:140). By joining the institutions actors will abide by its rules and tenets, and thus are liable to sanctions should they act outside the dictates of the agreements.

Liberalism is particularly strong in the sense that it takes into account the importance of non-state actors in international politics (Larenas, 2017:13). Admittedly, non-state actors such as private companies, particularly internet companies such as WeChat, Google, Facebook, Amazon and Twitter have become key cogs in modern cyber space. Not only that, the bulk of telecoms networks and computer firms are mostly in private hands. Put simply, non-state actors are a credible

component of the modern cyber domain. Because of this recognition, it has a more holistic perspective concerning the nature of threats and their impact to a referent object(s). Inescapably the cyber domain is a key element of the globalisation process which has reinforced interconnectedness and interdependence. A cyber challenge in one part of the world may have deleterious implications on others within the same system. Thus, vulnerabilities, sensitivities and shocks can flow easily to affect others. Security actors can, therefore, derive benefit from integrated cyber systems on the one hand, but they are equally vulnerable to the same intertwined system should something happen. Because a state is dependent on the system, it ought to work collaboratively with other states to enhance security.

The economic view of liberalism underscores that interdependence between states is likely to bring peace. This is because a disruption is most likely to disadvantage both parties. The cyber space can also be seen as improving cultural and ideational affinity between states, something which can be seen as a positive in terms of reducing friction. One weakness of this perspective is that interdependence does not automatically suppress conflict as it may render others vulnerable to exploitation. Basically, the many wars and conflicts which have been experienced despite the presence of international institutions have been recognised as a setback to the inherent optimism in liberalism.

Due to the relatively waning role of military power in current global order states have to lump on other tools to advance their interests. One such tool is cyber tools, which are notionally effective and less costly to deploy, compared to full-fledged boots on the ground contests. In other words, due to the growing complexity of interdependency military force is no longer a first choice for states (Gerace, 2004:56). The cyber domain without doubt expands non-physical threats to the security of an identified referent object.

A more palpable weakness to liberalism is that states, particularly the most powerful ones are unlikely to enjoy working in such institutional parameters because they may not want to reveal their capabilities to others. Importantly, by exposing their advanced capabilities states are most likely to cede some of their dominance.

2.5 SUMMARY OF THEORETICAL APPROACHES

This section summarises the key elements of the theories discussed in the previous sections. The key assumptions of realism: states are main actors and non-state actors are secondary actors; states are rationale actors; anarchic system; power is a key matter of pursuit and states act in their own interest. The key assumptions of constructivism are: Constructivism looks at how human agency and motivation shapes security thinking. In other words, actors shape and are shaped by circumstances for security approaches. Liberalism key tenet says that non-state actors are key

players in international systems. Cooperation and multilateralism is regarded as critical in achieving progress on matters of security. For liberalism, cyber security is a concern that goes beyond the nation-state boundaries.

2.6 CONCLUSION

Having discussed the three key approaches that illuminate cyber security thinking, the study will consider neorealism the main theoretical strand. It was important to provide a theoretical context in this chapter for several reasons. First, theories shape the manner in which security is viewed and what is currently being seen on the cyber security front. Second, they shape both what we see and how we see it. Third, theories provide a context for analysing the entire research by linking the concrete and abstract issues. The chapter essentially discussed the value of realism, constructivism and liberalism as tools for underpinning cyber security policies. This study finds realism to be more useful, logical and relevant to analysing the stance of states in cyber security. Its great strengths lie in emphasising the key role of the state in security, places less trust in morality, admitting to the anarchic nature of global polity and emphasises the role of power politics in security. The next chapter discusses NCPF and comparable policy frameworks.

CHAPTER 3: REVIEW OF CYBER POLICY FRAMEWORKS

3.1 INTRODUCTION

This chapter outlines the key security principles of South Africa's National Cyber Security Policy Framework. The chapter seeks to answer the second objective of this study and it views this NCPF in light of other comparable cyber security policies of states such as US and India. The main aim of the chapter is to describe the key components of the policy framework, which is a state's response for addressing cyber security concerns in an era of hyper connected socio-economic and political cyber dominant world. The chapter begins by outlining key components and ends with a conclusion.

3.2 KEY ELEMENTS OF A SECURITY POLICY FRAMEWORK

Literature is hardly expressive and clear when it comes to conceptualisation of what a security policy is. Part of the challenge stems from the fact that security is a contested concept which is viewed differently depending on vantage point and disciplines. As such, there is not much clarity when it comes to security policy regardless of virtually the term being used extensively. Be that as it may, this study argues for key elements that a security framework generally ought to have.

3.2.1 The difference between a policy and a framework

It is fundamental for this research study to unpack whether the NCPF is a policy or a framework. Or the NCPF is both a framework and a policy.

3.2.1.1 Policy conceptualisation

A policy instrument is defined as, "technique of governance that in one way or the other, involve the utilisation of state authority or its conscious limitation" (Howlett, 2005:31 as cited in Eliadis *et al*., 2005). Put alternatively, a policy essentially encapsulates what a government (or any entity) perceives as problems that need to be addressed and the way they are addressed. It speaks to choices about the intentions or purposes of government action, ends to be achieved, means for achieving the goals, approved programmes, specific actions to implement the programmes, and the measurable impact of the programs. A policy selects goals to pursue as well as the manner or way of pursuing those goals.

For Gyngell and Wesley (2003:20), a policy entails, "the promotion and protection of given social values within boundaries of state responsibilities by agents of the state." Policy thrusts generally reflect trade-offs among military, legal, ethical, economic, social and political values as well as goals. In other words, numerous institutions, organisations and individuals participate in the policy formulation, implementation and outcomes. Likewise, a policy is predominantly characterised by repetitiveness and consistency in the behaviours from the policy makers and implementers (Ealau

& Prewitt, 1973:34). For example, the statements of leading policy makers in the executive branch of government such as the president tend to communicate a policy stance of the state.

Others view a policy as a purposive course of action devised in response to a perceived problem (Cochrane & Malene, 2014:3). For this study a policy is a planned course of action determined and intended to influence actions, decisions and related matters. Thus, a group of actors select goals as well as the means of achieving those in a given situation. Passorns (1995:88) underlines that a policy has to, "be structured, located within a given place and given a name". In a nutshell, though there are variations to how policies are conceptualised, they nonetheless entail the following elements:

- Are authoritative decisions which have wide-ranging impact;
- Spells out goals and desired objectives;
- Identify the target or targets of the objectives;
- Determine the pathways, processes and actions to reach the objective;
- Spells out the action to take towards achieving the stated goals;
- It spells out what to do and what not to do; and
- Deliberative and conscious.

3.2.1.2 Conceptualising frameworks

In studying social phenomena frameworks come in different forms and guises such as theoretical frameworks (which are derived from theories and conceptual frameworks (are based on ideas and constructs), policy frameworks (focus on policies) and many other nuances. For this study, a framework provides the parameters for defining, understanding and interpreting social phenomena. It also integrates constructs with the aim of delineating what is important.

A framework seeks to crystallise different thoughts and activities of players into concerted focus. In this regard, a framework spells out the structure and mode via which cyber security will be delivered, overseen, and managed. Security deficits in the specific area are identified and means for addressing them are outlined. A security framework thus covers numerous issues, including compliance, risk and resilience, governance and regulation.

An example of a security framework is the National Institute for Standards and Technology (NIST) which basically sets standards for the protection of critical infrastructure in the USA. Essentially the NIST sets a benchmark to follow for government, industry and other actors. For cyber security, organisations follow the likes of International Organisation for Standards (ISO) 27001 and 27002 which are basically regarded as comprehensive frameworks for security controls for computer

security. The 27001 focuses on information security management systems, and 27002 on code of practice for information security controls (ISO, 2018).

There are numerous examples of industry specific security frameworks which include Centre for Information Security (CIS) framework for critical security controls across sectors such as power, finance, defence and transportation in the US. There is the Health Information Technology and Clinical Act of (2009) (HITECH) for the US health industry, the Payment Card Industry Data Security Standard (PCIDSS) for worldwide credit cards, and Defence Acquisition Regulatory System (DFARS) for US military contractors.

3.2.2 Security Policy

Having looked at policy in general, it is critical to shift attention specifically to security policies, which are arguably peculiar from other public policies. Security policies are geared towards addressing security related hazards, threats and risks to a single or a constellation of referent object/s (Mennen & van Tuly, 2014:15). At the state level, a security policy either is motivated by crises, or is geared towards fulfilling domestic and foreign interests (Morris, 2011:123). Because security is a fundamental need, every state has a security policy in one form or another. Security policies are sometimes encapsulated in a single document but can be ascertained from documents such as strategies, doctrines, plans and white papers. If such documentation is not publicly available, the actions and expressed statements of leaders and those in charge of high-level positions reveal the implied policy of the state. Security policies appear in different guises and inflections such as speeches, state behaviour and actions, and expressed statements.

Security policies are generally broader than defence policies. Defence policies that tend to be more militaristic and focus on “a plan of action regarding recruitment, training, organising, equipping, deployment and use of military force (Hays *et al*. 1997:9)”. A security policy, at minimum, needs to be economically feasible, understandable, realistic, consistent, procedurally tolerable, and provide reasonable protection relative to the stated goals and objectives of management. Security policies define the overall security and risk control objectives that actors endorse.

It is vital to underline that sometimes policy is informally formulated and implemented, depending on the political leadership of a given state. For example, one may not find the cyber security policy of North Korea, but this does not mean it is non-existent, but rather the policy is revealed in the activities of the state. Importantly, security policies come with a price tag, meaning financial resources are required to make them operational and functional. A key consideration in selecting a security policy is the context in which it operates (Hastedt, 2018:9). A critical caveat is that no

security policies are identical due to the varied differences between states and they vary over time as well.

If the two concepts are combined, a policy framework can therefore be seen as a blue print for formulating and imagining what is condensed in a policy. It entrenches the basic ideas, principles and approaches to the policy itself. In the case of cyber, a policy framework is the lense with which the state of South Africa purviews the cyber security world. Logically, the heart of a cyber-framework sets the tone for activities and expected outcomes. It is critical to delineate two closely related concepts, policy and framework. From the preceding articulation, it is therefore more plausible to refer to the NCPF as a framework for developing policies.

Borrowing from the Her Majesty Government (HMG) Security Policy Framework (SPF) (2011) a security policy framework, "describes the standards, practice guides and approaches that are required to protect assets (people, information and infrastructure)." It focuses on the outcomes that are required to achieve a proportionate and risk managed approach to security that enables an entity to function effectively, safely and securely. For this study, security policy frameworks are standards that can be followed to enhance and validate security posture or process by actors or agencies. In other words, they work as compliance or as guideposts for what is expected to be done towards providing security. Accordingly, a security policy framework acts as a map that shows possible directions to take, highlights areas of interest as well as what to avoid. Moreover, security frameworks enable effective communication between actors and agencies in a given setting. For example, in a state, a security policy framework improves coordination, communication and networking between the key security actors such as intelligence, police and military.

Security policy frameworks are contextualised, meaning they are informed by the peculiarities of a specific environment. They range in terms of focus and thrust with some concentrating on a specific referent object, a specific industry or sector and others being broad like national security frameworks. This means they have a focus as to what ought to be secured. Security policy frameworks can be industry based, meaning they are a designated set of rules and guidelines that allows for security architecture in that industry or sector. Further, security frameworks are designed to cover a broad range of industries and areas, and these can be national security frameworks which cover a slew of areas. The overarching features of a framework are that it speaks to cross-cutting issues in relation to cyber security.

3.3 COMPARING KEY ELEMENTS FROM SIMILAR POLICY FRAMEWORKS

This section reviews similar security policies to determine what other key elements they include. The examples are from relatively similar constitutional democracies, namely USA and India.

3.3.1 United States of America cyber security key elements

The USA is regarded as the leader in terms of cyber resources, military power, economic power, science, and technology (Adamsky, 2017). The current US cyber policy does not specify how or if cyber is an act of war (McNiel, 2017). There are several documents which cover cyber security policy in USA. Few of such documents include the National Security Strategy (2015), Cyberspace Policy Review (2009), the National Strategy to Secure Cyberspace (2003), Infrastructure Cybersecurity (2013), the Department of Defence (DoD) Cyber strategy (2015), International Strategy for Cyberspace, Draft Strategy for Improving Critical Infrastructure Cybersecurity (2014). The policy stance is further corroborated in national legislation which includes the National Cyber Protection Act (2014), Cybersecurity Enhancement Act (2014), and Cybersecurity Act (2015).

For the USA, internet is their creation and they have a strong grip over global internet governance (Bayuk *et al*, 2012:95). The USA remains the most dominant player in cyber security matters, especially given their dominance in aspects of cyber such as computing, networks and technologies. It pioneered internet naming and its addressing system (Kruger, 2016:20). In other words, a key imperative in a cyber-security policy is internet governance. Their cyber policy is more realistic, based on building robust defensive and offensive capabilities, cyber domination and advancing their hegemonic ambitions. The USA policy identifies a strategic risk as attacks with catastrophic impact on the homeland or to critical infrastructure.

Post September 11 (9/11) terrorist attacks on the US, the NSA was tasked with undertaking cyber offensive operations. USCYBERCOM manned with over 60 000 cyber warriors (Akdag, 2017:34). Further, the USA created a cyber-command under the auspices of the US military on 23 June 2009 by the then Secretary of Defence Robert Gates (Ibid). The Cyber command was aimed at defending the Department of Defence (DoD) networks against cyber-attacks and in developing offensive capabilities.

3.3.1.1 Rationale

The cyberspace is regarded by the USA as a fundamental pillar for advancing state interests, but can be a loophole for attacks. Thus enhancing security in this space is regarded as a *sine qua non* for, “protecting America’s national security and promoting the prosperity of the American people” according to the National Cyber Strategy of the US (2018). As an integral part of modern American life, the state is taking a leading role in making sure that private entities, public entities and individuals regarded as American are secure and are preserved from the harmful attacks. The increased dependence on the cyber has multiplied the probability and impact of risks.

3.3.1.2 Key elements

The USA cyber macro policy has four key pillars of priorities and several other specific areas of focus. These are the core elements of the USA security policy framework:

a. Defend the homeland by protecting networks, system, functions and data;
b. Promote American prosperity by nurturing a secure, thriving digital economy and fostering strong domestic innovation;
c. Preserve peace and security by strengthening the ability of the US in concert with allies and partners- to deter and, if necessary, punish those who use cyber tools for malicious purposes;
d. Expand American influence abroad to extend the key tenets of an open, interoperable, reliable, and secure internet.

Specific low policy plans include:

i. Securing networks and systems that fall under the Federal Government.
ii. Strengthening the security of critical infrastructure of both the state and the private sector. Examples of identified infrastructure include banking, energy, finance, transportation, health and communications.
iii. Prioritisation of investments, research and development on cyber security.
iv. Addressing cyber security for satellite, navigation and positioning systems.
v. Combating cyber crime
vi. Fostering a vibrant and resilient digital economy
vii. Incentivise and encourage innovation in security technologies.
viii. Collaborate with others to promote standards.
ix. Promote free flow of data across borders.
x. Maintain US dominance in emerging technologies.
xi. Build robust cyber human resources.
xii. Cooperation with other countries, industry and other actors.

3.3.1.3 Key Actors

According to Hunker (2010) the cyber policy of the USA internationally was to elevate cyber in the White House. In the Obama years (2008-2016), cyber security was regarded as a top priority in the National Security Council (NSC), and there was a dedicated post of a Cyber Security Coordinator. This position was however later scrapped with the coming of John Bolton as president Donald Trump's security advisor (Pelroth and Sanger, 2018). Though the White House takes a leading role, the actual capabilities to deal with cyber security concerns are distributed across various parts and agencies of the state (government). However, various security departments such as

Department of Defence (DoD), Department of Homeland Security (DHS), National Security Agency have various cyber security strategies.

In short, some of the key players as can be gleaned from various policy documents are:

i. The DoD entrusted with defending the United States of America and has a US Cyber Command that specifically looks at cyber security. One of their ambitions is to attain and maintain cyberspace superiority and different branches of the military have their cyber specialised units.
ii. The Department of Homeland Security (DHS) is entrusted with securing intra-state issues, meaning the prevention, mitigation and recovery from cyber-attacks.
iii. The Federal Bureau of Investigation (FBI) deals with domestic intelligence, particularly investigation and enforcement on cyber security concerns.
iv. Other intelligence arms such as the National Security Agency (NSA) deals with nation-wide intelligence on the cyber space and the Central Intelligence Agency (CIA) addresses the international component of cyber security.

3.3.1.4 Punishments

The USA has a plethora of means to deal with perpetrators of cybercrime, cyber terrorism, cyberwarfare and cyberespionage. One of the tools applicable is Cyber Sanctions that can be in the form of Executive Orders. Examples of such orders are Executive Order (EO) 13757 of 28 December 2016. This order described the steps to be undertaken against malicious actors. EO 13694 makes it possible for the state to block the property of persons believed to be involved in malicious cyber activities. The state can therefore impose sanctions on entities and individuals. Consequent to these EOs about 13 persons and 3 entities involved in elections meddling were added to a sanction list on 15 March 2018. Equally, 10 Iranians and a single entity were added on the sanction list on 23 March 2018.

The draft of the Active Cyber Defence Certainty Act (ACDC) in the USA which is before its Congress allows for limited hack back. For example, they help to clarify cyber criminality from cyber terrorism or cyber espionage. Technology companies such as Google, Facebook and Twitter had to attend several hearings in both the US Senate and House to give testimony on Russian activities in USA elections. To show this cooperation, for example, Peter Levashov, a Russian spammer was extradited from Spain to the USA to face justice there (Graff, 2017:1).

Other methods used include using the tools of power which the state possesses. These include intelligence (espionage and counter-intelligence), military operations (virtual and kinetic), diplomatic punishments (expelling diplomats) and economic sanctions as alluded to in the previous paragraph. The DoD in conjunction with the CIA is the institution prepared to fight cyber wars and

cyber terrorism world over. Other organs of the state are involved in fighting cyber money laundering.

On the domestic front several punitive measures can be instituted including being tried before the justice system, jailing, paying fines and in extreme circumstances, facing the court martial. An example is Chelsea Manning (also known as Bradley) who was given a 35-year sentence (was released in 2017) for releasing sensitive Wikileaks documents which included Afghan and Iraq war documents, diplomatic cables and Guantanamo Bay collections.

3.3.2 Indian National Cyber Security policy

The cyber policy stance of India is captured in the National Cyber Security Policy of 2013.

3.3.2.1 Rationale

For India, cyber security is considered a serious concern by the government, especially as the government was rolling out the Digital India Initiative which was made to narrow the digital divide. A central part of the Government of India's development policy is the 'Digital India' campaign, aimed at digitally empowering Indian citizens by boosting connectivity, expanding access, and improving electronic delivery of government services. However, as it makes progress on these goals, and as threats in cyberspace continue to grow, India needs to prioritize the security of the personal data of its citizens and update its Cyber Security Policy. Their policy enunciates a vision, mission, objectives, an institutional framework and statement principles. Moreover, the policy statement takes into cognisance the broader security environment in which India finds itself in terms of cyber security and it proposes ways to address the challenges confronting the country.

3.3.2.2 Key elements of the NCSP of India

Some of the main objectives of the Indian National Cyber Security Policy (2013) are namely to;

- create a secure cyber ecosystem in the country, generate adequate trust and confidence in IT system and transactions in cyberspace and thereby enhance adoption of IT in all sectors of the economy;
- create an assurance framework for the design of security policies and promotion and enabling actions for compliance to global security standards and best practices by way of conformity assessment (Product, process, technology and people);
- strengthen the Regulatory Framework for ensuring a secure cyber space;
- enhance and create National and Sectoral level mechanisms for obtaining strategic information regarding threats to ICT infrastructure, creating scenarios for response, resolution and crisis management through effective predictive, preventive, protective response and recovery actions;

- improve visibility of integrity of ICT products and services by establishing infrastructure for testing and validation of security of such product;
- create workforce of 500,000 skilled professionals in the next 5 years through capacity building, skill development and training;
- provide fiscal benefit to businesses for adoption of standard security practices and processes;
- enable Protection of information while in process, handling, storage & transit to safeguard privacy of citizen's data and reducing economic losses due to cyber-crime or data theft; and
- enable effective prevention, investigation and prosecution of cybercrime and enhancement of law enforcement capabilities through appropriate legislative intervention.

More importantly the outlined strategies focus on the following:

- create a secure cyber ecosystem;
- Create an assurance framework;
- Encourage open standards;
- Strengthening a regulatory framework;
- Creating mechanisms for security threat early warning;
- vulnerability management and response to security threats;
- Securing e-governance;
- Protection and resilience of critical infrastructure;
- Promotion of research and development;
- Reduction of supply chain risk;
- Human resources development;
- Create cyber security awareness;
- Development of effective public private partnerships; and
- Information sharing and cooperation.

3.2.3.2 Key actors in India National Security Policy

India is one state with an explicit National Cyber Security Policy (2013) which was produced by the nation's Department of Electronics and Information Technology. The Indian National Security Council Secretariat works as the nodal agency for cyber security. The country however has a National Cyber-Security Coordinator who works from the office of the Prime Minister. In this sense, it can be seen that cyber security is regarded as a top priority in which the executive is highly interested. Under the India cyber policy, the following institutional arrangements are instituted:

i. National Critical Information Infrastructure Protection Centre (NCIIPC) is set up to deal with protection of critical infrastructure from cyber-attacks. The identified infrastructure includes finance system, payments, telecommunications and geo-spatial systems.
ii. Indian Computer Emergency Response Team (CERT-In): This entity functions as the nerve to dealing with cyber security incidents. In other words, it gathers, analyses and distributes information pertaining to cyber incidents. The same unit coordinates all other agencies by providing guidance, alerts and advisory services.
iii. Cyber Swachhta Kendra which is considered as the Malware analysis and Botnet cleaning centre. It specifically aims to deal with malware and botnets which compromise network systems.
iv. National Cybercrime Coordination Centre (NCCC) deals with online monitoring and reporting. It also establishes units that deal with cyber forensic activities, cybercrime handling and assisting the prosecution and aiding the judiciary. It also seeks to promote Research and Development on cyber security.

3.3.2.4 Punishments

The state can take several measures to deal with identified perpetrators of four cyber concerns namely cybercrime, cyber terrorism, cyber warfare and cyber espionage. Normally states use four measures to deal with state actors by using economic punishments such as sanctions, quotas and blockades. Diplomatic measures that can be evoked to expel diplomats and freezing the assets of suspects. Undertaking espionage sabotaging tactics in the case of how the USA and Israel was involved in sabotaging the Iran nuclear facilities. The state can use military operations, mostly as a measure of last resort and the Indian army will be called to fight either in the cyber space or to engage in kinetic warfare. On the domestic front, suspects may have to face justice, be fined, jailed or extradited.

On the legal side, India possesses legislation to deal with various cyber related security challenges. For example, it has the Information Technology Act, 2000 (IT Act) which specifies in section 66F how cyber terrorism is considered and addressed. Moreover, the Indian cyber policy permits its India Computer Emergency Response Team (CERT-In) to undertake emergency measures when handling matters of cyber emergency.

3.4 KEY ELEMENTS IN AMERICAN AND INDIAN CYBER SECURITY POLICIES

It is important to provide a constellation of a combined feature of key elements of cyber security policies by gleaning from USA and India. This section covers some of these core elements in a detailed manner.

3.4.1 Security actors and institutions

Actors and institutions are key players in security policy formulation and implementation (Lake, 2001:129). Each state tends to have key actors on the state security front which maybe formal or informal actors. Similarly, actors carry their own goals, interests, and values in policy formulation and implementation process. Depending with the type of state, main security actors include head of state, security advisors, parliament, judiciary, military, intelligence, police and prison services. The effect and influence of a policy, particularly a security policy largely expands beyond the confines of security actors to encompass private security agencies, civil society and the supranational actors. Some of the important issues that influence a policy range from structural factors, institutional arrangement, complex interrelationships, and other varied instruments. The formulation and implementation of policy rest on the shoulders of institutions. It would be logical to expect a security policy to provide sufficient guidance to the institutions mandated for cyber security.

Internal security largely demands a strong and functional criminal justice system, effective intelligence entities, civil defence capabilities and emergency preparedness (Morris, 2011:127). On the external front, institutions such as diplomatic postures, military and foreign intelligence are vital.

3.4.2 Security environment and strategy

Cyber policies are not formulated in a vacuum, invariably they reflect the broad security environment, both domestic and international. Thus, it is of critical importance to have a cyber-policy informed by a national security assessment exercise which looks at short-term and long-term security concerns. Different security related theoretical framework poses different explanations to the importance and influence of the security environment (Hastedt, 2018:27). The strategic environment takes into consideration rising threats from the other nation's policies and the 'policies' of non-state actors. Notably, the prevailing security environment is complex as non-state actors such as criminal and terrorist organisations add to the ambiguity, volatility and uncertainty. Other critical markers for a security policy take into cognisance of the economic, political, development, cultural and safety issues. Arguably, the prevailing the cyber security environment is anarchic as it precludes binding accepted norms for governance and international cooperation. Put differently there is an apparent lack of agreements, institutions, norms, international institutions, laws and societal values at the global level.

This essentially requires taking into cognisance the values and interests, require governance structures as well as the decision-making processes. Arguably, actors who lack robust coercive means to achieve their goals may rely heavily on non-coercive means such as cyber activities to achieve foreign policy goals. Put differently, cyber tools incentivises weak powers to fight asymmetrical warfare. The external factors that have been taken into cognisance in various cyber

policies include strategic interests, international law, cyber capacity and the foreign policy goals of rival states and other non-state actors. Other considerations include economic conditions, non-state actor behaviours, competing values, coalitions and alliances. It also takes note of the technology and software companies as well as private security contractors who are intimately involved in cyber security. This may partly explain the uneasy relationship between the American government and the dominant Chinese telecom hardware equipment and smartphone manufacturers like ZTE Corporation and Huawei.

3.4.3 Risk perception

Threat and risk perceptions constitute a critical variable to how security policies are formulated (Pertersen, 2011:694). Most security thinking tends to take the worst-case scenario approach as the policy makers seek to minimise the devastating impact from threats (Smith, 2017:78). Threat perception also leads to politicisation of security policies, leading to security policies conferring political status on certain actors. Some of the influencers of threat perception are the personalities involved in policy making, the nature of institutions and historical factors. For example, during the Cold War period the risk perception of dominant was mainly influenced by nuclear threat, hence security policies of states such as US gave nuclear deterrence the highest priority. In other terms, threats which are perceived high tend to garner increased attention from key security decision makers; hence they tend to influence the development of policies and strategies.

Inarguably, risk mitigation strategies are closely related to perceived consequences or probabilities of outcomes. According to Sjoberg (2001) perceived risk is important for policy related attitudes (as cited from Eriksson, 2001:1). To a great degree, the state must combine military and non-military concerns into a security policy. These may include military, economic, diplomatic, political, intelligence tools to help a country to achieve desired security objectives. This further permeates into conceptual understanding, structural and personnel levels of the state.

3.4.4 Capability analysis

What a state possesses and what it needs to possess to advance its security objectives is a vital component to factor in a cyber-policy. Security policies of states differ, and the difference is more pronounced between small and large states; which points to capability differences. The main reason for that difference is in their relative political power within the international political system. As such, a state looks at what is required to fulfil its objectives of reducing incidences and impact of cyber crisis, threats and hazards. According to Mennen and van Tuly (2015:863) in a review of the Netherlands Security Strategy, capabilities help to, “translate policy options for prevention, preparation, response and recovery”. In other words, small states tend to have limited political, economic, cultural and military ambition as well as power relative to big states.

Moreover, smaller states tend to be small players in global polity, unless they are having a rivalry with a major power or are engaged in existential battles in the case of Israel and North Korea (Bracken, 1993:138; David, 2012: 503). That said, to a considerable degree, the cyber security policy stances of the USA are largely about shaping international strategic environment to their favour unlike for many small states such as Chad or Zimbabwe whose ambitions might be materially constrained. In other words, the size and stature of power instruments at the disposal of the US *vis-à-vis* what Malawi has, unsurprisingly influence how they factor certain issues for their cyber policies. Moreover, many small states are mostly focused on internal security concerns.

3.4.5 Alliances and international diplomacy

Cooperation and alliances are a key component of many security policies in the contemporary modern-state (Cavelty *et al*, 2014:4). Alliances and partnership on the security front have been a critical element in enhancing security for nation states (Morris, 2011:132). Alliances have been traditionally seen as state-to-state agreements which are mainly intended to endure from a security standpoint. In the contemporary world, alliances are not only purely military, but entail cooperation in other domains. Some of the notable alliances include the European Union (EU), Commonwealth and North Atlantic Treaty Organisation (NATO). This declaration was regarded as the biggest cyber security cooperation, as it sought to enable member countries to build cyber security capabilities and to enhance international cooperation on this matter. Moreover, the fact that NATO has a Cooperative Cyber defence centre and possesses the Tallinn Manual which defines the legal framework for cyber warfare, is also proof of what alliances may deliver.

Cyber policies also address partnerships and working with other nations. The role of regional bodies looms large, and the European Union is the most active organisation. In October 2017 there was a report about mobile devices belonging to NATO troops being hacked to steal critical information (IISS, 2018). The USA and China has had various engagements and meetings to enhance bilateral law enforcement on cyber activities.

3.4.6 Norms, regulations and laws

Norms, regulations and laws play a vital role in establishing a cyber-security framework both within and between nation states. For any policy to be practical it needs to be in conformity with constitutional and related legal instruments. Companies may be regulated so that they put robust systems to secure private information and protect unauthorised access to computer systems. In the USA for example, different legislations have been passed to help engender cyber security. These legislations include Cybersecurity Information Sharing Act (CISA) 2015, Cybersecurity Enhancement Act of 2014, Federal Exchange Data Breach Notification Act of 2015 and National Cybersecurity Protection Advancement Act of 2015. Overall, policies provide a basis upon which various players in the security sector as well as private enterprise can work within. Legislative

actions taken by jurisdictions such as the US include the prohibition of the sale of Huawei and ZTE mobile phones on US military bases (IISS, 2018). Another broad regulation from EU member states is the General Data Protection Regulation (GDPR) which seeks to protect people's data privacy. Generally, laws carry penalties for those who fail to comply.

3.4.7 Human resources and capacity building

Humans are at the heart of security because they are a core element which defines the very nature of a state. As such, the power of states is partly seen by the number of people it can raise for security purposes, and this is not far from being true when it comes to cyber security. Accordingly, states require a contingent of people with high level skills to develop cyber weaponry, defend and launch attacks against rivals. Just like a state developing nuclear armoury needs specialised skills in areas such as nuclear physics and engineering the same can be said for cyber. High level skills in Science, Technology, Engineering and Mathematics (STEM), particularly in engineering, cryptography, network engineering, mathematical modelling, and computer science are considered critical in growing a cyber-security skills base. The growing sophistication in information technologies, associated attacks and crime call for a corresponding level and amount of skills to meet such challenges. As such, states which seek to be up the curve of cyber need to train and have a pool of highly skilled individuals.

Human resources development is a critical component of a cyber-security policy as it empowers a state for asymmetrical warfare. The personnel are necessary in the police service, intelligence, military and government. Basically, capacity building includes the endeavours geared towards fostering a vibrant cyber ecosystem within a state. This may entail stimulating research and development, within and without private entities, state sponsored research and personnel building in civilian areas as well as in the military. Generally, the US and Indian cyber policies emphasise the importance of skills and technology.

3.4.8 Resilience against breaches

Breaches in government and private entities are becoming a common feature that may result in loss if data, assets and financial losses on the part of government. Not only does this have severe effects but also creates high levels of distrust within a given state. Some of the cyber weaknesses are as a result of a lack of awareness of the need for cyber security on the part of government bureaucracy. Moreover, a policy may have to look at how the government prepares for and responds to data breaches and put in place laws in support of this.

3.4.9 Privacy and rights

One of the most contentious issues on cyber security is the question of striking a balance between constraining rights and providing security. In other words, the internet has been regarded as a tool

for expanding human rights, freedom of expression and privacy. Yet, such privacy and human rights issues can and have been abused by elements who seek to cause harm to states. Equally so, states are grappling for more powers to censor and monitor cyber space the way in which institutions such as the NSA have been doing as exposed by Edward Snowden, Bradley Manning and Julian Assange's WikiLeaks. Not only that, private companies, particularly data companies such as Facebook have been at the forefront of losing people's private data to Cambridge Analyitca (Persily, 2017:65). Nefarious governments seeking to bolster regime security have taken the route of using cyber policies to clampdown on local opposition voices and to infiltrate foreign audiences.

3.4.10 Military and cyber warfare

The military in virtually any state is primarily entrusted with the responsibility of defending the state against external and internal aggression (Barrett, 2013:4). Thus, its role in the cyber domain cannot be understated. Cyber warfare has equally become a critical feature in the modern militaries world over and has become a means for offensive and defensive actions of militaries. Equally so, military doctrines have evolved with states demonstrating cyber force on the global level. For example, Russia carry out cyber-attacks on Georgia, Ukraine and Estonia (Nocetti, 2015:114). Stand-alone units have been formed to act as cyber guerrillas within the militaries, with the United States having a Cyber Command which was established in 2010.This USCYBERCOM has different elements from the army, fleet, air force and marines. Ashton Carter former US once said in February 2016, that his county was using cyber as a weapon of war (Szoldra, 2016:1).

Similarly, the Department of Defence Law of Armed Conflict (Department of Defense, 2015) outlined three ways in which cyber weapons can be used to achieve mass casualties. These are:

- Trigger nuclear plant meltdown;
- Open a dam in a populated area causing destruction; and
- Disable air traffic control system resulting in airplane crashes.

The service elements of the USCYBERCOM are the Army Cyber Command, the Fleet Cyber Command, the Air Force Cyber Command and the Marine Forces Cyber Command.

3.4.11 Critical infrastructure

According to Futter (2016:1), sophisticated cyber-attacks on national infrastructure and critical infrastructure such as nuclear facilities may necessitate a national response. Critical infrastructure includes banking, communication, industrial systems, energy, health, water and transportation which the nation depends on. Most of this critical infrastructure has moved from being analogue to

digital, making it intimately interwoven in the cyber realm. Connectivity has revolutionised the way we travel, communicate and do business.

Such attacks will lead to substantial destruction, disruption and loss of life. Thus, deterring such kind of attacks is of strategic importance to the state. Cyber-attacks on such infrastructure can be strategic and tactical as they offer asymmetric benefit over strong states or opponents. The growing threat of destructive cyber weapons in future has potential devastating effects. Batch (2018) notes that the maturing cyber warfare tools deserve concerted attention of policy makers. They include cyber offensive capabilities such as Computer Networks Exploitation (CNE) and Computer Networks Attacks (CNA). Defensive capabilities include computer networks defence.

3.4.12 Cyber intelligence

According to Carr (2012:42), cyber espionage is more prevalent than other forms of war and he pointed to China as the dominant actor in this regard. The global intelligence entities are playing a big role in cyber intelligence, espionage, deception and surveillance activities. To a great extent, a cyber-policy reflects the role of the intelligence community in undertaking operations that seek to defend the interests of the state. Activities that are alleged to have been undertaken by the states are operations some as Stuxnet against Iran nuclear enrichment facility (Lindsay, 2013:365). New tools for undertaking these activities are being developed. Thus, many states, if not all states carry out state driven cyber espionage operations at a high frequency than in the past. This brings into light the operations of agencies such as NSA, CIA and Canadian Security Intelligence Service.

3.4.13 Partnerships

Germano (2014:1) posits that a thriving cyber security environment cannot be achieved by one actor, but a combination of actors especially institutions of the states and private sector. In most states in the contemporary world, it is the private sector which owns, operates and controls the biggest volume cyber related information systems. They have more resources at their disposal to attract high-quality talent for cyber security positions. Not only that, the private sector is also a victim of cyber related attacks, one can provide the example of the 2016 hack on Sony Entertainment allegedly by North Kore, and wiped about half of the company's network (Ismail, 2017:3). The government has strengths in being able to investigate, arrest, and prosecute cyber criminals and terrorists. Moreover, it can collect intelligence on threats. In other words, an effective working partnership between the private and public partnership is critical in the modern world system where cyber security challenges are fast-evolving, multifaceted, nuanced and complex in nature. Numerous cyber policy documents speak to the value of this kind of partnership.

3.5 KEY ELEMENTS OF SOUTH AFRICA'S NCPF

South Africa's NCPF was a follow up to electronic security related legislation and policy stance with regard to cyber security. These measures, regarded as incomprehensive in the NCPF included:

- Chapter XIII of the Electronic Communications and Transactions Act. 2002 (No.25 of 2002) provided tho first statutory provisions on cybcrcrime in South African jurisprudence.
- Regulation of Interception of Communications and Provision of Communication related Information Act No. 70 of 2002
- Protection of Constitutional Democracy against Terrorist and Related Activities Act, 2004

South Africa's NCPF was conceived by the State Security Department and was approved by the South African cabinet on the 8th of March 2012. The document remained classified until 2015 when it was officially published in Government Gazette no. 39475 on the 5th of December 2015. On the 15th of October 2013 a National Cyber Security Advisory Council (NCAC) was established in accordance with the terms of the policy framework and was announced by the then Minister of Communications Yunus Carrim. The NCPF was released at the end of 2015 (SSA, 2015), specifically being regarded as a comprehensive approach for addressing the burgeoning cyber security threats in South Africa. Regionally, the SADC 2012 Model Law on Computer Crime and Cybercrime is a guide development of cyber security laws in SADC Member States.

South Africa's NCPF is said to incorporate bits of inputs from other states such as the EU, NATO and the US (Sutherland, 2017). The first NCPF draft came in 2010, and later formally published in 2015 with the Ministry of State Security being in charge. The State Security Agency was tasked with its implementation and strategizing. The remainder of the responsibility was left to the Department of Communications (DOC) which succeeded the Department of Telecommunications and Postal Services (DTPS).

In light of the growing role of cyber and the impending fourth industrial revolution South Africa has sought to come up with a security framework in that regard. The NCPF framework is premised on four identified problems with regard to cyber security:

- inadequate regulatory framework;
- uncoordinated and siloes approaches;
- lack of awareness by the public; and
- lack of skills, capacity and resources.

To address the identified challenges above, the NCPF's ten core elements are as follows:

a) The development and implementation of a Government led, coherent and integrated Cybersecurity approach to address Cybersecurity threats;

b) Establishing a dedicated policy, strategy and decision making body to be known as the Justice Crime Prevention & Security (JCPS to identify and prioritise areas of intervention and focussed attention regarding Cybersecurity related threats. The Cybersecurity Response Committee will be chaired by the State Security Agency (SSA) and will be situated at the SSA;
c) The capability to effectively coordinate departmental resources in the achievement of common Cybersecurity safety and security objectives (including the planning, response coordination and monitoring and evaluation);
d) Fighting cybercrime effectively through the promotion of coordinated approaches and planning and the creation of required staffing and infrastructure;
e) Coordination of the promotion of Cybersecurity measures by all role players (State, public, private sector, and civil society and special interest groups) in relation to Cybersecurity threats, through interaction with and in conjunction with the Hub (to be established within the Department of Telecommunications and Postal Services);
f) Strengthening of intelligence collection, investigation, prosecution and judicial processes, in respect of preventing and addressing cybercrime, cyber terrorism and cyber warfare;
g) Ensuring of the protection of national critical information infrastructure;
h) The promotion of a Cybersecurity culture and compliance with minimum security standards;
i) The establishment of public-private partnerships for national and action plans in line with the NCPF; and
j) Ensuring a comprehensive legal framework governing cyberspace.

The NCPF emphasises coordination across government in the implementation of NCPF. Clusters such as Justice, Crime Prevention and Security are cited to take a leading role in the implementation of the policy framework. The Director General of State Security chairs the Cybersecurity Response Committee (CRC) and liaises with heads of other cognate agencies and departments. The CRC is tasked with decision making, strategic thinking, as well as to prioritize areas for threat identification, intervention and assessment.

Some of the key institutions dealing specifically with cyber-security matters in South Africa include the Department of Telecommunications and Postal Services (DTPS), Centre for Scientific and Industrial Research (CSIR), State Security Agency (SSA), Special Investigative Unit (Hawks), South African Police Service (SAPS) and State Information Technology Agency (SITA). For example, the DTPS launched the National Cyber Security Hub. CSIR was involved with sharpening technical skills and technologies to address cyber threats in South Africa. In addition, SSA engages in cyber intelligence and counter-intelligence for South Africa and it oversees the Computer Security Incident Response Teams (CSIRTs), SAPS polices cyber issues specifically

with regard to Electronic Crime Unit and the Hawks can undertake cyber investigative work. SITA advises the government on cyber material procurements.

This NCPF therefore provides for:

- Measures to address national security in terms of cyberspace;
- Measures to combat cyber warfare, cybercrime and other cyber ills;
- The development, review and updating of existing substantive and procedural laws to ensure alignment; and
- Measures to build confidence and trust in the secure use of ICT.

The provisions of the NCPF as mentioned above have a lot in common with other cyber policies, particularly that of India and the US. The security of ICT systems is largely deemed a fundamental constituent of cyber policies. Overall, from the above objectives, it can be deduced that, the NCPF's objectives seem to be in accord with what other cyber security policy documents emphasise. In other words, the difference with Russia is that it emphasises much on information security and playing a role in shaping the global cyber arena. To a significant degree, the objectives are much in line with other policy documents.

3.5.1 Discussion of key elements of National Cyber Security Framework

The NCPF is explicit when it comes to identifying the following items to be protected: critical infrastructure (hardware, networks and software components), defence capabilities, economic security, national security, public confidence and social life. Another constituent is that the NCPF identifies several sources as potential sources of cyber threats in South Africa. Some of the identified threats revolve around the following sources: extremism (terrorism), criminals, espionage, foreign nationals, foreign states, and accidents. From this, the NCPF shares much with the Indian and US policy on threat identification as well as covering what needs to be secured.

The NCPF also refers to two technical layers of cyber which are the physical layer and the logical layer. The physical layer refers to the hardware such as routers, cables, switches, and the logics include aspects such as software and codes of communication. The third layer is social, which is, the interactions of humans and machines. The NCPF emphasises detection, prevention and recovery. This includes harmonisation of security standards. However, engagement and commitment to the framework, if done on voluntary basis, may be problematic. Virtually all cyber security policies underline protection of cyber-physical components, software and logical components.

It can be deduced that departments and units will be formed within the main security actors in South Africa, particularly in the military and police. India and the USA are examples of states which have moved towards institutionalisation of cyber security. Moreover, this is in line with some practices in other states such as the USA where security agencies possess dedicated units to address cyber security gaps. NCPF also underscores that intellectual cyber theft poses a security threat to South Africa, a factor other states such as the US has been accusing other states such as China for doing. In other words, commercial intellectual property is regarded as key to state economic security for now and the future. Despite having agreements not to use cyber-attacks on each other, China and the USA have continued to accuse each other of the persistence of the problem.

Though the NCPF underscores the development of cyber defence and offensive capabilities, it seems as if South Africa is not a salient offensive player on the global stage. Notable attacks include the NotPetya virus attacks on Ukraine's infrastructure, cyber-attacks on Georgia and attacks on the USA Democratic National Committee (Connell & Vogler, 2017:6). In other words, NCPF praxis seem not to be the same as that of USA and Russia which have been saliently engaged in carrying substantial state on state cyber-attacks.

Just like the Indian and USA policy, there is strong emphasis in the NCPF to improve the cyber security culture in South Africa. Perhaps the framework could have been more detailed regarding how it addresses data protection, especially its storage, transmission and sharing. Further, the question of the collection of data by private sector seem not well attended to by the NCPF. Should the private sector lose valuable personal information of citizens what will be the consequence of that? Several South African based firms such as Liberty life which lost personal data of millions of South Africans in an attack in June 2018 (Shapshak, 2018:1). How will the state address the issue of data stolen from the government by external actors such as quasi-state groups?

3.5.2 Summary of elements not included in the National Cyber Security Framework

The main difference between the NCPF is that the USA's approach is premised on being a dominant player in the global security, and on cyber security to be specific. In other words, the cyber is meant to be a domain in which the USA has to be the leading player. Moreover, cyberspace is a conduit for advancing the diplomatic, intelligence, military and economic dominance. The second issue missing from the NCPF is the emphasis that US places on its 'intra-states.' The USA is a federal republic rather than a unitary state in the manner in which South Africa is, as such the US policy emphasises states to also have their policies to advance respective cyber security concerns.

The NCPF is different to the USA approach because the US has several supporting doctrines and strategic documents about cyber security for virtually all security agencies. Additionally, the number of security agencies and departments involved in the US approach is quite large. The South African approach therefore resembles the Indian approach.

3.6 CONCLUSION

South Africa's NCPF stitches together complex interactions between domestic and foreign factors, with a slant on state security peppered with a tinge of human security. The NCPF is essentially illustrative of this national security posture as it outlines objectives, partnerships and resilience of critical infrastructure. More importantly, it speaks to social, economic, political and technical defence of cyber space within South Africa *vis-à-vis* external and internal cyber security threats. The NCPF also highlights both politically and apolitically motivated threats in the cyberspace. To a large degree the NCPF is more of a framework than a policy, arguably it is a framework for thinking and making cyber policies particularly for the various agencies of the state security architecture. The next chapter which is an analysis section of the research provides an in-depth critique and examination of the NCPF.

CHAPTER 4: CRITICAL ANALYSIS AND CONCLUSION

4.1 INTRODUCTION

The rise to prominence of cyber as a frontier for security, both offensively and defensively gave rise to state cyber security policies. These policies are geared towards dealing with small and big, both state and non-state actors on the confluence of domestic and international politics. This study specifically sought to undertake a critical analysis of South Africa's NCPF, looking at how it was meant to enhance security in a changing international and local strategic landscape. This chapter builds upon previous chapters and strives to make a critical analysis, summarisation, proffer recommendations and suggestions for avenues for cognate research studies. In particular, it seeks to answer two questions: How effective has the NCPF been since being introduced to achieve its self-stated aims? Is the NCPF a sufficient policy framework for cyber security in South Africa?

The study has thus far covered three chapters. Chapter 1 describes the outline of the research study, the background, problem statement and research objectives. It also attends to the contributions of the study, conceptual discussions and research ethics issues. More broadly, it lays the foundation for the entire study. The first chapter focused on backgrounding the basis for this research study, enunciating the direction for the study. Key components covered in the chapter include articulating the problem statement, research questions and research objectives. Even more important was to underscore that this is the first of such academic studies to specifically undertake a critical analysis of the NCPF. Though the differences between a policy and framework are subtle, the NCPF has more characteristics of a framework than it is a policy. In other words, the NCPF is more of a framework for drafting cyber security policies of security actors and the government at large. The chapter also addressed the question of the key elements of a cyber-security framework and discussed such using comparative examples of the United States and India. The chapter concludes by summarising key elements of a cyber-security framework.

Chapter 2 targets discussion on theoretical frameworks applicable to cyber security. In specific terms, Chapter 2 attended to theoretical framework discussions. Particular attention was riveted on three theoretical approaches namely, neorealism, constructivism and liberalism. The discussion focused on the insights of such theories to cyber security policies and how they illuminate discussions with regard to how relevant they are to the study. The chapter walks through several cyber security scenarios that are linked to each theoretical approach and specifically realism, liberalism and constructivism. Following this discussion, neorealism was considered a plausible approach key to critique the NCPF.

In Chapter 3 several cybersecurity related concerns were discussed, while looking at the intricacies that are between policies and frameworks. It is important to note that the NCPF was found to be more reminiscent of a “security framework” than a “policy” as it did not clearly articulate the key elements of a typical security policy, namely that it should clearly:

- Make reference to specific referent object/s (what is to be secured);
- Outline how the identified referent object/s will be secured;
- Pinpoint the actual and potential threats to the referent object/s; and
- Spell out the institutions key in terms of securing the referent object.

The next section provides an overall critique of NCPF to address the last two research questions. It accepts that it is a security framework and several recommendations are also made to strengthen the NCPF in line with comparable frameworks of other countries.

4.2 POLICY CRITIQUE

This section provides a critique of the NCPF, with particular attention given to answering the third objective of the study: To assess the effectiveness of the NCPF against its stated aims.

4.2.1 Strong points of National Cyber Security Policy Framework

On the positive side, the NCPF covers a plethora of areas which are at the heart of cyber security. Cyber is not confined to state boundaries, which makes striving for international cooperation a critical component. It is therefore commendable that the NCPF will try in a more challenging world to negotiate bilaterally and multilaterally for some international norms in cyber (NCPF section 11.3). Exploring international cooperation also helps to put in place some form of sanity which may lower cyber security risks as it has done in nuclear weapons for example. International overtures have the potential to improve international law and cooperation amongst security players. South Africa may push for the UN Security council to address concerns around cyber hostilities between states, deal with cyber weapons proliferation, transnational cybercrimes and terrorism. This means pushing for the UN to expand the definition of security to encompass the cyber component. A realist view in the short term is that it is highly unlikely that multilateral agreements will improve South Africa’s cyber security standing. As such, a unilateral approach is more reasonable and plausible to guarantee that South Africa is better secured. This unilateral action gives the state some assurance to do damage limitation.

One of the NCPF’s upside is its emphasis on promoting a cyber-security culture (NCPF section 14). A security culture need to be promoted and implemented across the entire state, government, citizens and private sector. The question that lingers is perhaps how this will be implemented, the specifics about how this is being carried out. This is because at present it seems as if little headway has been made towards implementing a security culture. In other words, the government,

private sector and public sector need to be build a conducive environment for cyber security culture. This means proper regulatory requirements and organisational policies must be supportive of this move. Components that aid to growing cyber security include training, awareness initiatives and continuous risk assessments. “Culture”, in this context, includes beliefs, values, attitudes, norms and assumptions that relate to security.

The NCPF takes cognisance of the fact that cyber threats and attacks disregard state political boundaries (NCPF section11.3). In other words, states cannot only win by acting within their borders because attackers can act internationally. NCPF is cognisant of the political inevitability and the practical possibilities of a state being compromised from the cyber domain (NCPF section 3.1). One can refer to the previous connections between technological developments and the horrors of war. The relentless enlargement of and integration of cyber technologies and systems fundamentally expands the risk and cost of cyber damage. In some way, it is folly to predict in the immediate future the world coming together to establish an international body that will transcend state power in governing cyber security.

Another strong point of the NCPF is the manner it emphasises coordination (NCPF section 4.1.1). This comes after the realisation that a scattered and individualistic approach may fail to mitigate threats which can emanate from varied sources. The level of sophistication of some of the actors and technologies involved justifies the need by security actors and the private sector to work collaboratively. The major difference between the NCPF and the US cyber policy is that the main coordinator of cyber security is the White House. In South Africa the NCPF hardly mentions the Presidency as a key authority.

The success in security cooperation and partnerships generally rest on trust between the various actors and institutions (Rathbaum, 2011:245; Vlaander, 2013: 7). NCPF underscores the importance of partnerships (NCPF sections 4.1.2; 4.1.3). Naturally the private sector will be wary or reluctant to share much of its data and information with the government as it has been the case in the US (Bhatia, 2016:2). As such collaboration with academic institutions, private sector and government agencies towards enhancing skills and knowledge about cyber is critical, something the NCPF should be applauded for (NCPF section 12). Perhaps a good reference to educational institutions at the forefront in South Africa is the University of Johannesburg’s Centre for Cyber Security. This means, there is need by the state to assuage the hesitations of other actors to enhance cooperation especially regarding risk management and information sharing. One considerable concern that require critique is around the silence by the NCPF regarding how the partnerships between actors will be designed and practiced. This is critical in the sense that the private sector, particularly the telecoms sector, is largely owned by the private sector, meaning that

the bulk of network infrastructure, logics of servers, computers, and fibre are not in the hands of the state. Put differently, the methodology of engagement will need to be clearer.

Further, the USA and India knowledge-based economies (as mentioned NCPF Executive summary) are built on cyber, making its protection a critical aspect. Moreover, as with India's cyber policy, it seeks to converge investigation, intelligence collection and the justice system in strengthening cyber security. This is underlined as critical in fighting all forms of cyber terrorism, cyber-crimes and other related concerns. The Department of Justice is part of the JCPS cyber security implementation culture as alluded to in the NCPF. On the same note, the NCPF underlines the importance of regulating cryptograph and online identity issues. The NCPF is meant to be a guide for developing and improving laws, regulations, policies and decision-making processes about cyber security in South Africa. It emphasises collective security for South Africa's cyber systems and crisis management having acknowledged how cyber threats transcend institutional, sector and state boundaries. Cooperation within the state boundaries is deemed vital especially across government, private sector, and the academia. Such an emphasis on cooperation is found in both the cyber policies of India and the USA.

It is noble that the NCPF underlines technical and operational standards (NCPF section 15) and verification of information security products and systems (NCPF section 7). These two areas are vital for improving the resilience of the cyberspace. South Africa will however remain particularly vulnerable because of its high dependency on telecoms, network and computing technologies. In other words, without a strong emphasis on developing and encouraging the development of local technologies, regulating their usage will hardly be effective. This factor was not prominently highlighted in the NCPF, that is, to provide a proper analysis of the state *vis-a-vis* other actors on the global arena. Foreign firms also operate and own significant infrastructure in South Africa, for example data centres.

It can be deduced that the departments and units which will be formed as the main security actors in South Africa will fall within the ambit of the Justice, Crime Prevention and Security (JCPS) cluster (NCPF section 1.1; 5.2; 5.3). This is in line with some practices in other states such as the US and India where security agencies possess dedicated units to address cyber security gaps. Another commendable component of the NCPF is the way it targets awareness and education as critical pillars to cyber security. Because of the human factor, small firms, state employees and individuals might not appreciate the real security threats in the cyberspace. The NCPF further acknowledges the importance of knowledge, innovation and expertise on cyber as a state. Expertise is at the heart of developing cyber defensive and offensive weapons.

4.2.2 Shortcomings in National Cyber Security Policy Framework

The study has identified several contentious elements with regard to NCPF, which can potentially weaken its effectiveness toward addressing the stated aims and objectives. Such shortcomings are discussed in the ensuing sub-sections.

4.2.2.1 Complications of semantics and conceptual clarity

Clarity in terms of the meaning to terms matters in the interpretation, analysis and implantation of policies. One of the main contention around NCPF is on a semantic level, particularly its conflation of state, nation and country. The namesake 'national' is problematic considering that South Africa is not composed of people of the same identity. One therefore, has to grapple with whether the term is meant to mean 'state' or country. The explicit reference is, "national cyber security is a broad term encompassing many aspects of electronic information, data, and media services that affect a country's security, economy and wellbeing" (as stated in the NCPF executive summary). Moreover, it is not clear whether the term "nation" on NCPF is symbolic or it means a geographic setting? The term national is regarded as a country; this could be viewed as causing conceptual confusion to the NCPF. A confusing issue is that the concept of national security is ill-defined, thus its inclusion in NCPF is controversial. Is "nation" meant to mean an ideology, institutions and material (borders, physical security and integrity of individual? Or, is it the security of a nation "an identity" or the state 'institutions and a geographical space?' Thus, striving for the security of the state as the main referent object may cause the insecurity of other sub-referent objects such as civilians.

The NCPF conflates threats to the state with threats to society, individuals and business. Despite pointing towards several sub-referent objects, one can plausibly contend whether the main referent object is the state or nation. Furthermore, the NCPF refers to several endangerments to South Africa, ranging from economic, political, social, and institutional and endangerments to democracy. In this sense the NCPF is unspecific regarding what is being endangered (main referent object), a factor which may weaken efforts to bolster cyber security. Van Brunschot and Kennedy (2008: 51) posit that failure to capture the referent objects undermines the effectiveness of security interventions. Security requires a referent object with regard to what is being threatened (Van Brunschot & Kennedy, 2008: 51). The NCPF makes references to several sub-referent objects such as, information, critical infrastructure, economic well-being and human safety. It is to underscore that all these referent objects are interconnected.

4.2.2.2 Contradictory issues

Trade-offs are unavoidable in security making, and prioritisation is fundamental. This brings to fore concerns over how NCPF will reconcile issues pertaining to balancing encryption (cryptography) (NCPF section 9) of privacy (NCPF section 3.2) *vis-à-vis* public safety. Thus, on the competing

priorities of either focusing on human security or state security, the NCPF sounds more of a state-security centric approach though it acknowledges covering human security aspects. Though achieving cyber security and ensuring privacy is theoretically achievable, it is rather a fact that malevolent actors can exploit the privacy loophole to operate. As such, pronouncements which are too restrictive on intelligence and security information collection my pose even greater threats to the republic.

The NCPF looks quite similar to the Indian cyber policy that seeks to improve collaboration and harmonization among government, civil society and private sector including ensuring that South Africa becomes a critical contributor to international cooperation on cyber security matters (NCPF section 11). Similarities abound in the discussed cyber policies regarding emphasising the need to secure critical infrastructure. In other words, critical infrastructure is currently regarded as vulnerable and if compromised the damage to the state is seen as massive. Just like the Indian cyber policy, the NCPF makes oblique mentioning to, 'public-private partnerships' without expanding on how it will be realised. Moreover, regarding devastating attacks on civil infrastructure the NCPF does not mention how liable will be the private owners of that infrastructure. Further, the obligations on the private sector to secure their system look flimsy and creates a legal loophole should the state want to charge a private actor of disruptive attacks on their systems.

4.2.2.3 Slow implementation by the state

The NCPF makes clear reference to the role of the military in cyber security (sections 13; 16. 5). The national cyber defence strategy from the South African National Defence Force (SANDF) is yet to be finalised and be published. The Cyber Command Centre is not yet established due to lack of financial resources by the Department of Defence (DoD) (DefenceWeb, 2018). The DoD annual report 2016/17 refers to the department having to develop and establish a cyber-warfare strategy which was to be submitted to the Justice, Crime Prevention and Security (JCPS) cluster. As such, one of the shortcomings of the NCPF is that there are no requisite financial resources to expedite the formation of units as planned. In other words, in the absence of financial support and political will to augment the financial resources to DoD, the cyber security thrust in South Africa is most likely to remain precarious. Moreover, the DoD is still working to establish a cyber-defence office within SANDF as of September 2018, something many other states such US and Israel accomplished to do many years back.

Mitrovic (2018:1) notes that components of the NCPF, as touted in the cybercrime and cyber security bill such as the National Cybersecurity Hub, are not yet fully established. This is indicative of the fact that either NCPF was not well thought through or there is lack of political will to operationalise it. South Africa cannot effectively undertake proactive measures to reduce cyber security risks and organise awareness campaigns in the absence of supporting financial resources.

Accordingly, this pokes holes into the robustness of the NCFP as a whole. The state seems not to be acting decisively when it comes to cyber security. Moreover, there are no cyber security strategies yet for key security institutions such as police, intelligence and military as is the case for the USA cyber security.

4.2.2.4 Limited details

Critical infrastructure protection is a theme emphasised in the cyber policies of the United States and India (NCPF, 8). The NCPF is however not expressive as to how the state will ensure that critical infrastructure which is in the hands of the private sector will be secured. Critical infrastructure such as financial systems, telecommunications and computing networks and logics lie in the hands of the private sector. If the private sector is to use its own discretion to secure the system, it may jeopardise the entire state in general. As such, it may be prudent to have vibrant measures that are obligatory on the part of the private sector so that it is vigilant to cyber threats and attacks.

The NCPF sounds more like a framework than a policy mainly because it lacks details. It took a considerable time for South Africa to realise they need a policy thrust and even longer time to formulate and implement it. Given the pace of technological evolutions, it may not be far-fetched to consider the NCPF to be lagging. In other words, its implementation has been slow and the changes in technologies and other social changes can make some of its aspects not cogent enough. The NCPF, for example, does not spell out the kind of action that the state will take against those who gain access to private information, like what happened when Cambridge Analytica harvested data from Facebook.

The NCPF calls for a whole-of-government approach to cyber security (NCPF point 9 of the executive summary). This may be regarded as problematic given that governments are conceptually short-term administrators of the state. As such, a whole-of-government approach may not aptly capture the kind of attention with a whole-of-state approach. A government is a component of the state and thinking in terms of a whole of government approach may mislead to mean the government of the day may be the target to be secured (referent object). Arguably, a whole of the state approach can help engender better interagency coordination and facilitate a shared vision for cyber security for both government (administratively) arms and arms of the state. This helps departments not to be siloed on their goals and objectives but think more broadly about state goals.

A whole of the government approach may be misleading. The state cyber security structure better functions as a system not merely its disparate components. Thus, cyber security planning, budgeting and programming demands all units not just of the government but of the whole state to

capitalise on available resources. The key word is a 'holistic approach'. In other words, budgeting for cyber security may need not to be conducted on the usual departmental or agency approach, which means harmonisation and synchronisation of efforts. Moreover, a whole of the state approach helps the state to speak its position clearly to external non-state and state actors.

In order to provide immediate assistance in the wake of an offence, the Cyber Bill provides for the establishment of a point of contact to be available on a 24 hour, 7 days a week basis. This includes the following teams that should be able to assist and facilitate with enforcement and compliance issues: Cyber Response Committee, Cyber Security Centre, Government Security Incident Response Teams, National Cybercrime Centre, Cyber Command, Cyber Security Hub, and Private Sector Security Incident Response Teams. However, the activities of these entities are hardly known to the corporate and wider public. These activities are largely unknown even to researchers who can help in shaping and furthering our cyber security strategies and policies.

The fact that South Africa's defence cyber strategy is not yet pronounced is another indicator that even military systems are still vulnerable to cyber-attacks. Of note is that urgency is required to secure mission critical systems that connect combat vehicles, satellites and aircraft from vulnerabilities before South Africa suffers from being underprepared. South Africa's weapon systems can be compromised via cyber-attacks by other adversaries that may include state and non-state actors. The framework then could have been clearer in proposing or mandating frequent vulnerability assessments to government systems, voting systems, military systems and critical infrastructure in order to identify and fix loopholes before they are exploited.

The NCPF is somehow 'securitising' issues such as cybercrime (identity theft, fraud and phishing) as a matter of state security. Stated otherwise, the NCPF expands the range of threats to the state to include matters that are generally regarded as civil threats. This has partly caused an uproar with the Cybercrime and Cybersecurity Bill 2017 which was meant to magnify the state's surveillance of threats in South Africa. Enhancing cyber security within a state such as South Africa requires an all-of-the-state approach in which the cyber security posture of the individuals, non-state entities and state entities is improved. To its credit the NCPF makes a strong statement towards collaboration and coordination on four fronts: between government agencies, private sector and government, state and international actors and the state with civil society and the citizenry. The fourth leg of this engagement with the public is however not well articulated. The citizenry and civil society are not only consumers of security but can play a fundamental role in bolstering cyber security in South Africa. This is because the activities and practices of the citizens can create threats or can be exploited in a manner which hurts the entire state. In this case, the state will have to respond. Put alternatively the citizenry can be the weakest link to cyber security. As such, underscoring public awareness and engendering public participation in cyber security is

critical. In this way ensuring cyber security need to be seen as a civic duty of the society as a whole.

4.2.2.5 Lack of a balanced approach

It may be plausibly argued that the NCPF can be viewed as using an intelligence framework. Though the process of drafting NCPF is complex, the process was largely driven by the South African intelligence, SSA. As such, the language and thrust in NCPF reveals that most of measures to address cyber security concerns bear the imprint of the SSA along with the Ministry of Communications. It is thus not farfetched to argue that the competencies of various other security actors and civil society have not been central to this NCPF. The policy framework is deficient of the necessary balance that view resisting cyber threats in a unison manner. Rather, the SSA might have played a key role as arguably, a means for putting itself in a prominent role for getting security resources over other security actors. The strength of a security policy lies in its ability to consider the perspectives of key stakeholders.

One glaring miss in the NCPF is mention of a critical institution such as the Independent Communications Authority of South Africa (ICASA), a key regulator in communications. The role of this regulatory body is not specified which therefore challenges concerns around information regulation or privacy concerns *vis-à-vis* national security. Furthermore, the NCPF stipulates that South Africa's public private partnerships will be coordinated through a national computer incidence response team (CERT). This is perhaps unclear because at present South Africa does not have its own CERT. However, South Africa subscribes to the Ghana based AfricaCert. It is thus questionable as to whether this is the CERT that is being referred to in the NCPF or it is yet to be formally established. If it is, then how is it going to aid cyber security in the country and even more important is how private-public partnership will be meaningfully realised in the absence of the touted body.

Though comparing US and India policies is apt, South Africa has unique characteristics to these nations. Firstly, South Africa is not as big population wise, meaning its security expenditure and cyber connectivity is relatively low. Secondly, South Africa is in a different geopolitical space in which it does not clearly mention its enemies the manner in which the USA does. Thirdly, South Africa seem not to have known enemies the manner in which the USA refers to Iran, North Korea and Russia as threats. Neither does it in the same way India considers Pakistan to be a threat. Further, South Africa has not faced substantial terrorist related attacks, both direct and on the cyber front compared to these two states. Fourthly, South Africa is not a major producer and influencer of cyber products such as hardware, software and networks the manner in which the other states are. Nonetheless, the three states view themselves as democracies.

Another challenge pertains to how to assure private entities that their trust will not be abused by the state. The assumption by the NCPF that non-state actors and the private sector can make substantial commitment without a binding sanction and incentives is highly impracticable. Consequently, complete commitment requires that legal obligations are put in place to specify situations, actions and decisions that are prescribed and proscribed. Even more important is that such obligations ought to be enforceable via the legal system. More broadly, all this helps to improve commitment both from government agencies and from the private actors.

The NCPF grapples with whether other issues such as partnerships are voluntary or mandatory (NCPF section 11.3). It uses the lexicon 'promote' cooperation and partnerships. In other words, it will be confusing to see how it is going to select what is going to be mandatory and what will be voluntary. For example, the NIST in the US is voluntary because the private sector was not comfortable with mandatory provisions. In my view a voluntary framework leaves security gaps which may make the state more insecure as other actors may choose not to abide by the provided standards. As such, the state should play a leading role in coordinating reduction, management and responses to threats on critical infrastructure by stipulating some mandatory standards. Alternatively, it is more prudent for the NCPF to put in place a baseline for all stakeholders who operate in South Africa.

As with many other state security documents, state interest seems to be a key priority for NCPF with common interests being a secondary concern. In other words, national interests mean that in as much as concerns of liberty and privacy are key, they are regarded not as equally important as the security of the state itself. This also identifies the policy with neorealism in the sense that in as much as international cooperation is touted to be important, it is the state which is a key priority. Put alternatively, it is the primary interests of the state which need to inform international cooperation and cyber diplomacy.

4.2.2.6 Privacy concerns

One of the supporting policies to NCPF is The Cybercrime and Cybersecurity Bill 2017, which was criticised by the private sector and civil society (SHRC, 2017). Problematic areas were on copyrights, state investigative powers, freedom of speech and handling cyber terrorism. The state in South Africa is equally sceptical of sovereignty issues as it has not supported the African Union Convention to harmonise cybercrime laws and has not yet consented to the Budapest Convention. South Africa has not placed trust on multilateral approaches and places some trust on bilateral approaches to addressing cyber security concerns. Outcry over the Cyber Bill in South Africa raised concerns over how the state security is overriding citizen liberties and privacy concerns. Concerns are that surveillance can be used to track political opponents and to clamp down on dissent. The researcher's view is that the NCPF underlines that there are no unlimited rights to

liberties and privacy if society values security. In other words, security and privacy cannot balance equally at the same time.

Some of the concerns about Cybercrime and Security Bill (here after the CSB) of 2017, yet to be passed into law, is that it can be used to stifle liberties and free speech in South Africa and allow government to preside over private information in the name of security. The CSB vows to establish a Cyber Response Committee, which is chaired by the intelligence department. Moreover, the bill states that the Ministry of State Security is obliged to establish and run the Computer Security Incident Response Team (CSIRT) for the South African government. The SANDF is also required in the bill to develop offensive and defensive cyber capabilities, and the Ministry of Telecommunications and Postal Services is to establish and run a Cyber Security Hub. Further, the CSB provides for the Ministry of Justice to make regulations pertaining to information sharing.

4.2.2.7 Other concerns

South Africa can equally take a cue from the USA policy by striving to make its security establishment attractive to cyber-skilled personnel. This is fundamental because, inarguably cyber is the foundation of current and future strategic and tactical security thrust. The USA is also taking measures to recruit cyber skilled personnel to the national army by extending pay (Williams, 2018:42). This comes in light of realising that the military and Defence Department had been experiencing challenges in attracting and retaining cyber workers. The salaries in the private sector were making the security sector unattractive to those with cyber skills.

It is still to be seen if the military cyber defence strategy which compliments NCPF will be robust enough. It however requires political will towards making the policy strong and to realise its implementation. Moreover, resources will need to follow the framework to make it operationally practical. Thus, in the backdrop of continuously evolving cyber technologies and thinking, the NCPF will equally need to be reviewed and improved. In other words, the undercurrent of cyber security is the security of technological systems and the awareness of the potential harm by the users.

The NCPF does not put major emphasis on the power of South Africa vis-à-vis other states in the global international system. South Africa has slipped from being a hegemonic power on the African continent. Moreover, the role of South Africa in providing security on the continent has been waning. Like many developing economies, South Africa lags behind in terms of technological innovations and is not much of a producer of cyber products. In other words, much of the computing and telecoms equipment which can compromise security in South Africa are imported from external vendors. Explained differently, the policy framework hardly mentions how the state regulates equipment standards for they are a possible conduit for launching attacks. An example

for this is how the US expressed concern over telecoms equipment from Chinese firms, particularly Huawei and ZTE as a threat to their country's security (Raud, 2016:6). In other words, as a consumer of technologies, South Africa is always at a significantly threatened position which the NCPF must pay attention to, specifically regarding standards and proper due diligence in terms of procurement.

Other critical security agencies have not been central in the production of the framework. The intelligence community in South Africa could however counter argue by saying intelligence is a crucial component of security policy making as underscored by Best (2015:450) in his prognosis of US strategies on nuclear weapons and the control of armaments. Put simply, intelligence has played a pervasive role in the construction of US security policies (Best, 2015:450). However, overemphasis on intelligence might have side-lined the contributions of the civil society, private sector and the police as key players on the cyber security front. Perhaps to the credence of SSA, the cyberspace is at the heart of building an information society in which the intelligence community is inundated with information which is challenging to gather, analyse and share. As such, they have been keen to be at the heart of developing the security policy framework. In other words, the data deluge makes intelligence gathering challenging and have acknowledged the centrality of information in waging war and electronic attacks.

The success of a cyber-security policy lies not in over regulating or over controlling the private sector but by having an environment which equally permits the growth of industry and the economy. Inarguably, economic security is inextricably linked to long term security of the state. As such, adopting a policy which gives leeway for industry to experiment and thrive is important for South Africa. The US policy is comparatively more advanced as it has allowed the state to be a leader in cyber technologies and it does not constrain the growth of the fourth industrial revolution which has spawned world dominant firms such as Microsoft, Google, Facebook and Amazon. Not only that, but the leading academic institutions collaborate with industry and the state in the development of cyber defensive and offensive capabilities.

4.2.3 Theoretical critique

As alluded to in the second chapter that there are several competing theoretical approaches applicable to analysing state security policies. This part of the chapter reflects upon the study findings in light of the theoretical approaches covered in Chapter 2. First, the conflation of terms, particularly state security and human security highlights that the NCPF might have been informed by different theoretical positions. For example, the policy document places huge emphasis on cooperation and coordination between South Africa and other external institutions. This reflects more how this thinking is informed by liberalism. Not only that, the manner in which the current and future economic wellbeing of the state is premised on cyber also underlines liberalism. The hyper

interconnected nature of systems and people via the cyber can been viewed as important to bridge social cohesion, thereby lessen conflicts. However, the same cyber space can be used by states to limit freedom of expression, engage in cyber repression and fuel cyber wars. Importantly, liberalism acknowledges that the state is not the only actor, as such it has to be considerate of other players and work collaboratively where necessary.

Constructivism has substantial significance in analysing the findings of the study. Security policies involve value judgements and social construction of phenomenon particularly with regard to threats. Threat perception and 'securitising' the cyber as is in the case of NCPF can be astutely viewed in light of constructivism. This partly explains there were reservations from civil society on the Cybercrime and Cybersecurity Bill 2015. They argued that the construction of security was such that it permits the state to override individual freedoms and liberties.

For neorealism the state is at the heart of security and international security in general. Arguably, cyber security in South Africa depends much on what the state does or does not do simply because it the most powerful and influential actor in society. The practice of the state to a large extend determines domestic security and the role of non-state actors. As such, that is why the NCPF is an effort by the state to coordinate all other actors to play their role in enhancing cyber security in South Africa. The state is also the main unit of analysis for seeks to bolster defensive and offensive cyber posture.

Neorealism is reasonably illuminating given that all the other domains and armouries of warfare and security in this age can be influenced by cyber. All domains of warfare can be exploited by the cyber and it expands vulnerabilities to the entire state. Cyber devices are multiplying and are connected to critical infrastructures and weapons systems which both civilian and militaries depend on. Hence, if the South Africa's military is not prepared, any form of interruptions to command and control systems in times of war pose a serious threat to military communication, resource deployment and errors. Further, disruptions in critical civilian infrastructure such as transportation, financial systems, water and electricity can equally compromise military operations. Given this scenario, the NCPF can be lauded for underscoring the development of offensive and defensive cyber capabilities. However, thinking about offensive capabilities raises questions around the technical capacity, international legal constraints (rules of engagement) and state preparedness.

Though the NCPF can be applauded for underlining cooperation (NCPF section 11), one need to caution that overdependence on cooperation may increase vulnerability which has the potential to cause serious security challenges caused by interstate competition. The apparent weakness in cooperation is the fact that allies of today can be enemies in the future and *vice-versa*. This is not to say cooperation and partnerships are not important, but it emphasises the need to be cautious

when exploring such. Thus, South Africa must be prepared to avoid the unpleasant surprises fraught on the international security terrain. Partnerships are only as strong as their weakest member, and all nations can agree on norms to cyber security. The rise of non-state actors in the cyber domain means interstate cooperation is not enough in itself. The international cyber system is a self-help mechanism which motivates South Africa to act for its own survival and states habitually fail to collaborate in international politics and as such agreements sometimes break down. As such, interstate cooperation has its own limits, and developing states (South Africa included) hardly have their input heard at international security forums. In fact, many less powerful states are compelled to bandwagon with major powers when making decisions on security out of fear of reprisals.

Neorealism is more convincing as it views cyber weaponry control as utopian and precarious at worst for states such as South Africa. Thus, preparing to fight a cyber-war is perhaps a plausible way to prevent it. The state ought to have deterrence and responsive capabilities to undertake punitive retaliation, damage limitation and war fighting. Relying on mere defensive capabilities is insufficient to guarantee long-term security to South Africa because of the fast-evolving nature of cyber technologies. NCPF should therefore have been more articulate in the manner in which it enhances South Africa's war fighting position. From this perspective, the state requires an ever-ready cyber weaponry arsenal that is employable in worst case scenarios.

Neorealism places more value in security over privacy and freedoms concerns, something the NCPF seem to emphasise. Consequently, cyber security is central to the attainment, upkeep and use of state power in South Africa and the state cannot afford to be too dependent on other states or a group of states for its cyber security requirements. Cyberspace brings other advantages that traditional weapons and boots on the ground approach cannot achieve. In other words, they can be used to carry out precision attacks as compared to bombs which may have substantial collateral damage. Put alternatively, for cyber-attacks cyber can be used selectively without placing substantial cost on the state. For the military and intelligence, cyber weaponry can be able to do the job of soldiers and intelligence officials. When used externally it does not violate territorial integrity and sovereignty in the same magnitude as troops.

4.3 OVERALL REMARKS

It is important to note that the four issues that underpin cyber security concerns in this age will not go away in totality. These are namely, the presence of malicious actors, increased reliance on cyber technologies, human fallibility and inherent vulnerabilities in cyber virtual and physical technologies. As such, a neorealism approach is arguably the most relevant to address these inherent shortcomings pertaining to the cyber domain. Stated otherwise, cyber security is an endless battle in which there can hardly be a permanent solution or decision for it to go away. The

cyber threat landscape is ever-evolving and as such a cybersecurity policy or framework should not be judged on how it solves challenges, but rather how it can effectively manage them.

The neorealist camp acknowledges that states need cyber offensive and defensive capabilities because of fundamental security concerns. Put alternatively, NCPF will be seen as strong on this aspect because the anarchic international system justifies the need to address attacks from potential adversaries. It is however questionable if South Africa has the capability to develop its own defensive and offensive capabilities due to certain deficiencies around technologies and cyber preparedness. In other words, most of the effective capabilities may need to be sourced from outside South Africa, in the same way other security hardware and software are imported.

Established models of deterrence may not work effectively because of the agility and speed of technological evolutions in the cyberspace. Thus, NCPF must be flexible to adapt to changes, especially in the face of artificial intelligence and related technologies now being at the heart of cyber security. Therefore, NCPF ought to be alive to changes on the cyber security front and respond accordingly. The state in NCPF is concerned by the diffusion of power to the private sector when it comes to responsibility to secure cyber systems. This is because according to the Westphalia system the primary role of the state is to provide security to its citizens.

Given the fast alteration of the cyber terrain since 2012 and the palpable need to give flesh to the NCPF to strengthen its security posture. Overall, the effectiveness of the NCPF is much dependent on the level of commitment the state and its various units has in operationalising it. As of now, there seem to be flimsy commitment regarding not only implementing NCPF but in terms of understanding the magnitude of the dangers of being cyber-insecure as a state. For example, Telkom, one of South Africa's largest operators of critical infrastructure was a victim of the WannaCry Ransomware in May 2017. These kind of attacks show how South Africa is susceptible to attacks, and there is a possibility of much larger and devastating attacks should the state not implement and improve the NCPF. This therefore means the NCPF is in many dimensions commendable, but in its current format it is not sufficient to guarantee South Africa security. In other words, the state and the sub-referent objects identified in the NCPF will remain vulnerable if the implementation process is piecemeal and the broad framework is underspecified.

Overall, the NCPF in my view melds together strands from several theoretical viewpoints such as liberalism (in emphasising the importance of cooperation and economic security), neorealism (in emphasising the state taking a leading role in ensuring security) and constructivism (in shaping the narrative about the cyberspace as a security concern). Neorealism is more privileged in emphasising building deterrence capabilities, enhancing resilience, focus on cyber offensive and defensive capabilities. Put otherwise, NCPF underscores that when necessary South Africa will

take unilateral actions to safeguard its interests against cyber threats of all kinds and the SANDF is a core pillar in this regard.

4.3.1 Recommendations

In light of the above concerns this study proposes the following recommendations for enhancing cyber security in South Africa. The recommendations cover the following categories: political, institutions, technical, operational and financial component of cyber:

- Put it place minimum mandatory requirements for both the private and government entities as a way of enhancing cyber security.
- Enhancing political so that implementation of NCPF is expedited and the various organs of security are well-resourced. The strength of a policy is as solid if it can be supported by implementing mechanisms.
- Put in place legal mechanisms to enable the prosecution of cyber terrorism, criminal and other related offenses. The state need to outline the punitive measures for offenses regarding cybercrime, cyber terrorism, cyber espionage and cyber warfare.
- Implement complementing policies or strategy documents to further elaborate on some of the broad areas which are not expounded on.
- Though the NCPF underscores the need to produce human capital, it must tap into a variety of disciplines. This is because cyber security is complex and fields such as economics, political science, engineering, law, sociology, computer science and psychology need to be part of the development of the skills gap. In other words, a mere focus on technical matters is inadequate.
- The state need to give due attention to placing measures that address the concern for insider threats.
- Finally, the NCPF may need to be updated, considering it was developed in 2012, the cyber threat landscape has changed significantly. This means it may need to be improved with something which outlines the specifics of implementing the broad principles outlined by the NCPF. For example, there is need for specific details about how the cyber human resource will be trained and what the timelines are.

4.3.2 Directions for further research

Scholarship can be enriched by extending it in several trajectories that were not in scope of this study. First, the study can be undertaken in a methodologically different fashion, particularly by engaging an empirical study in how the NCPF is being implemented by the agencies of the state. Second, scholarly work can explore the nature of security actors (military, intelligence, police and justice) coordination in dealing with cyber security. The third possible avenue for further research on cyber security is to consider the regional implications of the NCPF. This was not investigated in

this study and it will be more important given the importance of geopolitics in security policy formulation.

4.4 CONCLUSION

The chapter concluded on a study which sought to provide a critical analysis to South Africa's main cyber security framework, the NCPF. The study was done using a qualitative paradigm, which utilised secondary data and some theories to attain four research objectives and answer the four research questions. Essentially, the illuminating theoretical strand adopted is neorealism, which has enabled the researcher to identify the strengths and weaknesses of the NCPF. The identified strong points in the NCPF includes its emphasis on a coordinated approach to security, stressing the need for and instituting cooperation via the JCPS, articulating the role of the state, promotion of human resources development, and research and development on cyber security and the developing of cyber offensive and defensive capabilities. Its weaknesses include emphasising on promoting security, ambiguities on the referent object, conceptual clashes and being underspecified. This chapter was specifically aimed at providing a critique of the NCPF, summarise and conclude the entire study. This research provided a critical analysis of South Africa's (NCPF) which is a state-centric approach which however considers other actors as critical to enhancing cyber security. Overall, from the synthesis of the theory, comparison with comparable policies and critique, several recommendations were proposed. It is based on a comprehensive analysis of the text, content and implications and demonstrates that NCPF is more of a framework than a policy. The framework is the tool upon which policy thinking and direction is set and it reinforces the stance of the state about cyber security. The chapter wrapped up by suggestion recommendations and areas for possible further studies.

5. BIBLIOGRAPHY

Adamson, F.B. 2016. Spaces of global security: beyond methodological nationalism. *Journal of Global Security Studies*, 1(1):19-35.

Akdag, Y. 2017. Cyber deterrence against cyberwar between the US and China: A power transition theory perspective. Masters thesis-University of South Florida, Florida.

Barkin, S.J. 2010. realist constructivism: rethinking international relations theory. Cambridge: Cambridge University Press.

Barrett, E.T. 2013. Warfare in a new domain: the ethics of military cyber-operations. *Journal of Military Ethics,* 12 (1): 4-17.

Barzashka, I. 2013. Are Cyber-Weapons Effective? *The RUSI Journal*, 158 (2):48-56

Bayuk, J.L. 2012. Cyber security policy guidebook. New Jersey: John Wiles and Sons.

Beach, D. 2012. Analysing foreign policy. Hampshire: Palgrave Macmillan.

Bendiek, A. & Metzger, T. 2015. Deterrence theory in the cyber-century: lessons from state-of-the-art literature review. Working Paper RD EU/Europe, 2015/02, May 2015 SWP Berlin.

Betz, D.J and Stevens, T. Cyberspace and the state: towards a strategy for cyber power. Alpha Series, IISS.

Bevir, M (ed). 2010. Encyclopaedia of political theory. Vol 1. California: Sage.

Bodmer, S et al. 2014. Hacking back: offensive cyber intelligence. McGraw: New York.

Bhatia et al. 2016. Privacy risk in cyber security data sharing. 3rd ACM Workshop on Information Sharing and Collaborative Security. November 2016.

Bracken, P.1993. Nuclear weapons and state survival in North Korea. *Survival*, 35 (3): 137-153.

Brantly, A.F. 2016. Decision to attack: military and intelligence cyber decision making. Georgia: University of Georgia Press.

Brown, C. 2009. Structural realism, classical realism and human nature. *International Relations*, 23 (2):257-270.

Buzan, B., Waever, O., & Wilde, J. 1990. Security: A security analysis framework. Colorado. Lynn Rienner Publishers.

Buzan, B., Waever, O. & Wilde, J. D. 1998. Security - A new Framework for Analysis, Colorado,USA: Lynne Rienner Publishers. Inc. p. 239

Carr, M. Public–private partnerships in national cyber-security strategies. *International Affairs*, 92(1): 43–62.

Cavelty, M.D. 2014. Breaking the cybersecurity dilemma: aligning security needs and removing vulnerabilities. *Scie Eng Ethics.*

Checkel, J.T. 2011. The social dynamics of civil war: insights from constructivist theory. Simons papers in security and development, 11:3-24.

Choucri, N.2012. Cyber politics in international relations. Cambridge: MIT Press.

Cochrane, C.L., & Malone. E.F. 2014. Public Policy: Perspectives and Choices. 5th ed. Boulder: Lynne Rienner Publishers.

Connell, M & Vogler, S. 2017. Russia's Approach to Cyber Warfare. CNA Analysis and Solutions.

Considine, M. 1994. Public Policy: a critical approach. Melbourne: Macmillan.

Copeland, D.C. 2006. The constructivist challenge to structural realism: A review Essay. (In Constructivism and International Relations Ed Guzzini and Leander). Oxon: Routledge.

Corbin, J & Strauss, A. 1990. Grounded theory research: procedures, canons, and evaluative criteria. *Qualitative Sociology,* 13(1):3-21.

David, S.R. 2012.Existential threats to Israel: learning from the ancient past. *Israel Affairs*, 18 (4): 503-525

Defence Web, 2018. SANDF outlines threats, priorities. Written by defenceWeb, Tuesday, 12 June 2018.

DefenceWed, 2018. Work on South Africa's cyber defence strategy in process. Written by defenceWeb, Tuesday, 18 September 2018.

Denzin, N.K & Lincoln, Y.S. 2011. The discipline and practice of qualitative research. In Denzin, N.K & Lincoln Y.S, *eds Qualitative Research,* California: Sage Publications Inc.

Department of Justice. 2017. Cybercrime and Cybersecurity Bill 2017. http://www.justice.gov.za/legislation/bills/CyberCrimesBill2017.pdf accessed 01 May 2017

Diez, T., von Lucke, F & Wellman, Z. 2016. The securitisation of climate change: actors, processes and consequences. Oxon: Routledge.

Dipert, R.R.2010. The Ethics of Cyberwarfare. *Journal of Military Ethics*, 9(4):384-410.

Donnelly, J. 2000. Realism and international relations. Cambridge: Cambridge university press.

Elau, H & Prewitt, K. 1973. Labyrinth of democracy. Indiana: Bobbs-Merill Co. US.

Eliadis, P., Hill, M.M., & Howlett, M (ed). 2005. Designing government: from instruments to governance. Montreal: McGill Queen's University Press.

Eriksson, J, ed. 2001. Threat politics: new perspective on security, risk and crisis management. London: Routledge.

Even, S. & Siman-Tov, D.2012. Cyber warfare: concepts and strategic trends. Tel Aviv: Institute for National Security Studies.

Futter, A. 2016. The Dangers of Using Cyberattacks to Counter Nuclear Threats. Arms Control Today.

Germano, J.H. 2014. Cybersecurity Partnerships: A New Era of Public-Private Collaboration. New York: New York University.

Gerace. M.P.2004. Military power, conflict and trade. London: Franck Cass Publishers.

Government Gazette. State Security Agency, National Cybersecurity Framework for South Africa, Government Gazette, 4 December 2015. No 39475 http://www.gov.za/sites/www.gov.za/files/39475_gon609.pdf.

Graff, G.M. 2017. How The FBI Took Down Russia's Spam King—And His Massive Botnet, Wired 4 November 2017.

Guitton, C. 2013. Cyber insecurity as a national threat: overreaction from Germany, France and the UK? *European Security*, 22 (1): 21-35.

Guzzini, S.2013. Power, realism and constructivism. Oxon: Routledge.

Hare, F. 2010. The cyber threat to national security: why can't we agree? Conference on cyber conflict proceedings 2010.CCD COE Publications, 2010, Tallinn, Estonia.

Harris, S. 2014. War: the rise of the military-internet complex. Boston: Houghton miffling Harcourt publishing.

Hart, C., Jin, D.Y & Feeberg, A. 2014. The insecurity of innovation: a critical analysis of cybersecurity in the United States. *International Journal of Communication*, 8:2860–2878

Hastedt, G.P. 2018. American foreign policy: past, present and future. London: Rowman and Littleman.

Hays, P.L., Vallance, B.J., and Van Tussel, R (ed). 1997. American defense policy. Maryland: John Hopkins University Press.

Hobson, J.M. 2000. The state and international relations. Cambridge: Cambridge University press.

HMG Security Policy Framework, 2011. Understanding the Security Policy Framework. Version 2.0 October 2011.

HM Government 2016. National Cyber Security strategy 2016-2021.

Hough, P., MaliK, S., Moran, A., & Pilbeam B. 2015. International Security Studies: theory and practice. Oxon: Routledge.

IISS Cyber Report: 29 June to 5 July. https://www.iiss.org/blogs/cyber-report/2017/07/cyber-report-29-june-to-5-july accessed 30 October 2017.

IISS Cyber Report: 8 to 14 February. https://www.iiss.org/blogs/cyber-report/2018/02/15-to-22-february accessed 5 April 2018.

Ismail, M. 2017. Sony pictures and the US. Federal government: a case study analysis of the sony pictures entertainment hack crisis using normal accidents theory. Master's thesis-The University of Southern Mississippi, Mississippi.

Jackson, R.H & Sorensen, G. 2007. Introduction to international relations: theories and approaches. Oxford: Oxford University Press.

Jayawardane, S., Larik, J., and Jackson, E. 2015. Cyber governance: challenges, solutions, and lessons for effective global governance. Hague institute for global justice.

Jetschke, A. 2011. Human rights and state security: Indonesia and Philippines. Pennsylvania: University of Pennsylvania Press.

Jordan, S.R., & Hill, K, Q. 2012. Ethical assurance statements in political science journals. *Journal of Academic Ethics*, 10 (3): 243-250.

Kallberg, J. 2016. Strategic Cyberwar Theory -A Foundation for Designing Decisive Strategic Cyber Operations. *The Cyber Defense Review*,101-116.

Kaiser, R. 2015. The birth of cyberwar. *Political Geography* (46):11-20.

Kello, L. 2017. The virtual weapon and International Order. Yale University Press.

Klenke, K. 2016. Qualitative research in the study of leadership. 2nd ed. Bingley: Emerald Group Publishing Limited.

Kostagiannis, K. 2018. Realist thought and the nation-state: politics in the age of nationalism. Cham: Palgrave McMillan.

Lake, D.A. 2001.Beyond anarchy: importance of security institutions. *International security*, 26 (1):129-169.

Larenas, M.J.A. 2017. What are states' strategic responses to cyberattacks? Impacts in international relations. Master's thesis: Universitat Wien.

Lindsay, J.R. 2013. Stuxnet and the limits of cyber warfare. *Security Studies,* 22(3): 365-404.

Mahoney, J. 2010. After KKV: The new methodology of qualitative research. *World Politics,*62 (1): 120-147.

Mennen, M.G & van Tuyll, M.C (2015) Dealing with future risks in the Netherlands: the National Security Strategy and the National Risk Assessment. *Journal of Risk Research*, 18 (7): 860-876.

Morris, T. 2011. Achieving national security: comparing four state security models. Police practice and Research, 13 (2): 121-137.

Nacita, I & Reith, M. 2018. Cyber War and Deterrence Applying a General Theoretical Framework. *Air & Space Power Journal*, 74-83.

Nocetti, J. 2015. Contest and conquest: Russia and global internet governance. International Affairs, 91 (1): 111-130.

Nojeim, G.T.2010. Cybersecurity and freedom on the internet. *Journal of National Security Law & Policy*, 119-137.

Nye, J. 1988. Neorealism and Neoliberalism. *World Politics*, 40 (2): 235-251.

Nye, J. 2010. Cyber Power. http://belfercenter.ksg.harvard.edu/files/cyber-power.pdf (accessed August 2, 2018).

Onuf, N.G. 1912. World of our making. Columbia: University of South Carolina.

Paalman, M. 2013. The Copenhagen school in the fifth domain: successful securitising the cyberspace? Uppsala: Uppsala Universitet. (Thesis-Masters).

Persily, N. 2017. Can democracy survive the internet? *Journal of democracy*, 28 (2): 63-76.

Pertersen, K.L. 2011. Risk Analysis-a field within security studies. *European Journal of International Relations,* 18 (4): 693-717.

Radu, R. 2014. Power technology and powerful technologies: global governmentality and security in the cyberspace. (In Kremer, J.F. & B. Müller, *eds*. *Cyberspace and International Relations* Berlin, Heidelberg: Springer-Verlag.

Rathbun, B.C. 2011. Before Hegemony: Generalized Trust and the Creation and Design of International Security Organizations. *International Organization*, 65 (2):243-273.

Raud, M. 2016. China and cyber: attitudes, strategies and organisation. NATO Cooperative Cyber Defence Centre of Excellence (the Centre).

Ravitch, S.M., and Carl, N.M.2016. Qualitative Research: bridging the conceptual, theoretical and methodological. Sage, Singapore.

Readon, R and Choucri, N. 2012. The Role of Cyberspace in International Relations: A View of the Literature. Paper Prepared for the 2012 ISA Annual Convention San Diego, CA April 1, 2012.

Resende-Santos, J. 2007. Neorealism, states, and the modern mass army. New York: Cambridge University Press.

Rigoglioso, M. 2014. Civil liberties and law in the era of surveillance. *Stanford Lawyer*. 91

Saldaña, J.2013. *The coding manual for qualitative researchers*. 2nd ed. London: Sage.

Santos, O. 2018. Developing cybersecurity programs and policies. Pearson.

Segal, A. 2016. The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age. New York: Public Affairs.

Shapshak, T. 2018. Liberty hack the 'biggest breach yet, Financial Mail, 21 June 2018.10.30.

Sienkiewicz, H.J. 2017. The art of cyber conflict. Virginia: Dog Ear Publishing.

Singer, P W., & Friedman, A. 2014. *Cybersecurity and Cyberwar: What Everyone Needs to Know*? What Everyone Needs to Know. Oxford: Oxford University Press.

Slack, C. 2016. Wired yet Disconnected: The governance of International Cyber Relations. *Global Policy*, 7 (1):69-78.

Smith, M.E. 2017. Security: politics, policy and prospects. 2nd ed. London: Palgrave.

South African Human Rights Commission. 2017. Submission on the cybercrimes and cybersecurity bill [B6-2017]. August 2017.

Stadnik, I. 2017. What is an international cybersecurity regime and how we can achieve it? *Masaryk University Journal of Law and Technology*, 11 (1):129-154.

Stevens, T. 2016. Cybersecurity and the politics of time. Cambridge: Cambridge University Press.

Szoldra, P. How the US military is beating hackers at their own game? Business Insider 24 May 2016.

Tang, S. 2009.The security dilemma: a conceptual analysis. *Security Studies*, 18(3):587-623.

Telo, M. 2009. International relations: a European perspective. Surrey: Ashgate publishing limited.

Theron, P.M. 2015. Coding and data analysis during qualitative empirical research in Practical Theology. *In die Skriflig,* 49(3):1-9.

Tuthill, D.P. 2012. Reimagining Waltz in a Digital World: Neorealism in the Analysis of Cyber Security Threats and Policy. Masters Dissertation-University of Kent.

U.S National Security Council. 2010. Cyber Space Policy Review: securing America's digital future. New York, NY. Cosimo Reports.

Van Brunschot, E.G., & Kennedy, L.W. 2008. Risk balance and security. California: Sage Publications Inc.

Vlaander E.M. 2013. Constructing security partnership between China and Asean. Master's Thesis- Universiteit Utrecht.

Waltz, K.N 1979. Theory of international politics. Illinois: Waveland Press.

Weber, C. 2014. International relations theory: a critical introduction. 4th edition. Oxon: Routledge.

Wendt, A. 1992. Anarchy is what States Make of it: The Social Construction of Power. *International Organization*, 46, (2): 391-425.

Wendt, A. 1995. Constructing international politics. *International Security*, 20: 71–81.

Wiliams, P. D. ed. 2008. Security studies and introduction. Routledge: Oxon.

Valeriano, B and Maness, R.C. 2015. Cyber war versus cyber realities: Cyber conflict in the international system. New York. Oxford University Press.