

https://dspace.org/

Government and private sector cooperation on security of critical information infrastructures

Mshunqane, Zoyisile

2017

https://hdl.handle.net/10539/26268

Mshunqane, Zoyisile (2017) Government and private sector cooperation on security of critical information infrastructures, University of the Witwatersrand, Johannesburg, <http://hdl.handle.net/10539/26268>

Downloaded from a DSpace repository. https://dspace.org/

GOVERNMENT AND PRIVATE SECTOR COOPERATION ON SECURITY OF CRITICAL INFORMATION INFRASTRUCTURES.

ZOYISILE MSHUNQANE: **9207314W**

SUPERVISOR: PROF ANTHONI VAN NIEUWKERK

A Research Report submitted to the Faculty of Management, University of the Witwatersrand, in 50% fulfilment of the requirements for the Degree of Master of Management in Public Policy (in the field of Security).

SEPTEMBER- 2017

Contact details: **0828967137/0784570662**

Email address: **zmshunqane@gmail.com**

1 DECLARATION

I, **ZOYISILE MSHUNQANE**, declare that this Research Report is my own work. It is submitted in partial fulfilment of the requirements for the Degree of Master of Management in Public Policy (in the field of Security) at the University of the Witwatersrand. It has not been submitted before for any degree or examination at this or any other university.

JOHANNESBURG

SEPTEMBER 2017

TABLE OF CONTENTS

1 DECLARATION 2

2 GLOSSARY 4

3 ABSTRACT 10

4 CHAPTER 1- INTRODUCTION 12

4.1 Background 12

4.2 Problem statement 16

4.3 Purpose statement 18

4.4 Research questions 18

5 CHAPTER 2- LITERATURE REVIEW 19

5.1 Introduction 19

5.2 CIIs and cybercrime 21

5.3 Methods for identifying CIIs and PPS: the South African approach 30

5.4 Secrecy, transparency and accountability 37

5.5 CIIs and information security standards 40

6 CHAPTER 3- RESEARCH METHODOLOGY 49

6.1 Conceptual framework 49

6.2 Research approach 50

6.3 Research design 50

6.4 Validity and reliability 51

6.5 Research constraints 52

7 CHAPTER 4-DATA PRESENTATION 53

7.1 Introduction 53

7.2 Primary data: interviews of government officials 53

7.3 Private sector perspectives 60

8 CHAPTER 5-DATA ANALYSIS 65

8.1 International practice 65

8.2 The South African policy and legal framework 67

9 CHAPTER 6- FINDINGS 72

9.1 International cooperation 72

9.2 RECOMMENDATIONS 75

10 REFERENCES 77

2 GLOSSARY

Access the ability or opportunity to gain knowledge of classified information

Access control the process by which access to a particular area is controlled or restricted to authorized personnel only;

Accreditation the official authorization by management of the organisation for the operation of an Information Technology (IT) system, and acceptance by that management of the associated residual risk.

Asset anything that has value for the organisation and includes hardware, software, people, infrastructure, data, suppliers and partners;

Availability the timely availability of information technology resources in line with organisational requirements;

BCP business continuity planning which entails the development of plans, measures, procedures and arrangements to ensure minimal or no interruption of the availability of critical information services and assets;

Budapest Convention the Council of Europe Convention on Cybercrime;

Classification the process by which state information is placed into categories for purposes of classifying such information in accordance with their level of security measures required in securing such information.

CERT Computer Emergency Response Team

Certification the process to certify that a comprehensive evaluation of the technical and non-technical security features of an Information and Communication Technology system and its related safeguards has

	been undertaken and that it was established that its design and implementation meets a specific set of security requirements;
CI	critical infrastructures whose unlawful alteration, destruction or loss is likely to deny the public or individuals of a service or benefit to which they are entitled;
CIIS	critical information infrastructures which is physical and computer based systems and assets, which are so vital to a country and whose incapacity, malfunction or destruction would have a debilitating impact on the provision of essential social, economic and national security;
CIIP	Critical Information Infrastructure Protection.
Confidentiality	the principle that information is not made available or disclosed to unauthorised individuals, entities or processes.
Comsec Act	the repealed Electronic Communications Security (Pty) Ltd Act no 68 of 2002;
Configuration	refers to changes made to a system's hardware, software, firmware and documentation throughout the development and operational life-cycle of the system;
CRC	the Cyber Response Committee responsible for the coordination of Cybersecurity activities in South Africa;
Cyberspace	a physical and non-physical terrain created by and/or composed of some or all of, amongst others, data, computers, electronic systems, networks, and end users;
Cybersecurity	the tools, policies, security concepts, security safeguards, guidelines and best practices approaches that can be used to protect the

	cyber environment as well as the cyber assets of an organization and/or users;
Cryptography	the art and science concerning the principles, means, and methods for rendering plain information unintelligible and for restoring encrypted information to intelligible form;
CSIRT	a computer security incident response team, a team of dedicated information security specialists that prepares for and responds to Cybersecurity incidents;
DTPS	the department of State responsible for Telecommunications and Postal Services;
ECT Act	Electronic Communications and Transactions Act no 25 of 2002;
ECS	Electronic Communications Services;
ECNS	Electronic Communications network Services;
ECSP	Electronic Communications Service Providers;
ENISA	European Union Agency for Network and Information Security
FICA	Financial Intelligence Centre Act
GLACY	Global Action against Cybercrime, a cybercrime technical capacity building project of the members of the Budapest convention funded by the European Union and implemented by the Council of Europe.
ICTS	information and communications technologies that are used to store, communicate and manipulate data.
Integrity	the inherent quality of protection that maintains the accuracy of entities of an information system and ensures that the entities are not altered or destroyed in an unauthorised manner;

Internet governance	the development and application of shared principles, norms, rules, decision-making procedures, and programs that shape the evolution and use of the Internet**.**
ISO	International Organisation for Standardisation, a non-Governmental Organisation responsible for, amongst others, the development of international standards for Information security;
ISPA	the Internet Service providers Association of South Africa;
ITU	the International Telecommunications Union
Majoritarianism	a political belief that simple numerical majority of citizens should rule a country the way it wants with total disregard of the views of other citizens outside of that numerical majority;
Mobile device	any portable device that can perform the same function as computer equipment including laptops, tablet PCs, cellular telephones and data cards;
NCII	National Critical Information Infrastructures which are all the ICT systems, data systems, data bases, networks including physical infrastructure, that are fundamental to the effective operation of the Republic;
NCPF	the National Cybersecurity Policy Framework, is a policy statement of South Africa outlining the policy approach of government in addressing cyber security related matters;
NGOs	Non-Governmental Organizations.
Network	a system of two or more computers that can exchange data or information;
NKP Act	the National Key Points Act, 1980 (Act No. 102 of 1980);

NKPs	the National Key Points declared as such in terms of the National Key Points Act;
Organ of State	an Organ of the State as defined in the Constitution of the Republic of South Africa;
OWASP	the Open Web Applications Security Project, a non-governmental organisation that educates information security experts on common Web application vulnerabilities;
Phishing	a fraudulent way of acquiring sensitive information such as usernames, passwords and credit card details by someone pretending to be a trustworthy entity in an electronic communication to lure the unsuspecting person.
POPIA	the Protection of Personal Information Act no 4 of 2013;
PPP	Public Private Partnerships.
Risk	the likelihood of a threat materialising by exploitation of vulnerability;
R2K	the Right to Know Campaign, a non-governmental organisation that campaign for freedom of expression and access to information.
SABRIC	South African Banking Risk Information Centre, a section 21 company whose key focus is to combat organised crime.
Server	a computer used to run programs that provide services to multiple users;
Standard	an essential requirement for the implementation of a specific policy, procedure or technology;

SOPs	standard operating procedures which are instructions to all system users, administrators and managers on the procedures required to ensure the correct operation of a system;
SSA	the State Security Agency, a department of State responsible for State Security.
System integrity	the ability of a system to prevent the circumvention or bypassing of its security mechanisms;
System Owner	a Manager ultimately accountable for the performance of the business process executed via a particular ICT system. The System owner is ultimately responsible for the functionality of the system;
TCY	the Cybercrime committee of the Council of Europe responsible for the implementation of the Budapest convention.
Threat	any potential event or act, deliberate or accidental, that could cause injury to persons, compromise the integrity of information or could cause the loss or damage of assets;
UNODC	the United Nations Office on Drugs and Crime
RICA	the Regulation of Interception of Communications and Provision of Communication-related Information Act, 2002
User	Anyone with authorised access to an ICT system;
Verification	activities related to the identification of the origin or the integrity of an electronic communications product, system or service;
Vulnerability	a deficiency related to security that could permit a threat to materialise.

3 ABSTRACT

Information and Communications Technologies (ICTs), in particular interconnected computer and related digital systems, create opportunities for innovation, competitiveness and economic growth. These technologies also expose key sectors of the economy such as banking, telecommunications, manufacturing, emergency services, transportation, energy, and social services to new security risks and threats.

This security challenge has given rise to a need for the adoption of appropriate strategies to secure critical information systems commonly referred to as Critical Information Infrastructures or CIIs. The European Union defines CIIs as ICT systems that are critical and essential for the operation of Critical Infrastructures, such as telecommunications, computers, the internet, and communications satellites. The African Union has defined CIIs as the cyber infrastructures essential to vital services for public safety, economic stability, national security, international stability, and the sustainability and restoration of critical cyberspace.

Given their complexity and sophistication, CIIs are increasingly owned or operated by the private sector, and governments generally purchase these services on behalf of the general public. This interdependence between the public and private sectors calls for structured co-operation aimed at ensuring the security and uninterrupted availability of CIIs.

This study examines the extent to which South Africa's public policies for securing CIIs promote co-operation between the government and the private sector. It includes a literature review which shows that policy aimed at promoting and regulating public-private cooperation is a key element of efforts to secure CIIs and combat cybercrime in Europe, the Americas and Asia.

The report also shows that the Council of Europe, through the Budapest Convention, has played a central role in creating a legal framework for combating cybercrime and promoting public- private cooperation on cybersecurity.

Government and private sector cooperation on security of Critical information Infrastructures

Research also shows that not much has been done in Africa to combat cybercrime. Some initiatives have been undertaken by Senegal, Morocco, South Africa and Mauritius. These countries are members of the Budapest Convention, and participated in initiatives of the Council of Europe in their capacity as members of the Convention.

In 2014, the AU adopted the AU Convention on Cyber Security and Personal Data Protection. This convention has only been signed by eight of 54 African countries, and has not entered into force because it has not been ratified by the required number of countries. This means that there is no valid instrument for promoting cooperation on cyber security in Africa.

Since 2002, the South African government has adopted various policies and laws aimed at promoting cooperation with the private sector. However, there is no evidence of these policies or legislation being implemented. The research also shows that the government has failed to develop a consistent strategy for implementing policy in this field.

In 2015, the government approved the National Cybersecurity Policy Framework (NCPF), which calls for public–private partnerships and cooperation. However, the research shows that it has not adopted a strategy that will allow this approach to succeed. In this regard, the research report points to the 5C protocol as a useful guide to successful policy implementation.

In interviews conducted for this study, senior government officials acknowledge that, as in many other areas of governance, good policy has been made, but implementation is lagging.

The study concludes with recommendations for improving cyber security in South Africa. These include fast-tracking the Cybersecurity and Cybercrimes Bill, which has been tabled in Parliament; developing and institutionalising a policy implementation framework in line with the 5C protocol; and developing the required skills and capacity to institutionalise and structure cooperation between the government the private sector in identifying and protecting CIIs, and pursuing a regional approach to cybersecurity.

4 CHAPTER 1- INTRODUCTION

4.1 Background

Rapidly development of Information and Communications Technologies (ICTs) continue to have a positive impact on the provision of social services as well as economic development throughout the world. While this is welcome, rapid technological changes are also presenting public policy as well as regulatory and legal frameworks with unprecedented challenges, notably by requiring more structured partnerships between government and the private sector.

These partnerships are needed because most of these systems, which form the backbone of contemporary social services, are owned or operated by the private sector. Like all major computer systems, they are vulnerable to cyber-attacks. These services are also highly sensitive, and disruptions could have far-reaching social and financial consequences. Therefore, a key aspect of public-private collaboration involves identifying and protecting what has become known as Critical Information Infrastructures (CIIs).

This study investigates the extent to which South Africa's public policies, laws and regulations aimed at identifying and securing CIIs are promoting cooperation between the government and the private sector.

As noted by Timothy Shaw (2004), the resurgence of civic protest in virtually all sub-Saharan African countries since the late 1980s has resulted in the transformation of the continent's governance and political systems, with civic groups in most of these countries demanding that their governments be democratic, transparent and accountable. While much has been achieved, much remains to be done in this regard for Africa to have an effective and vibrant civil society which plays a meaningful role in governance.

Ndlangisa (2009) and Assaf (2008) point out that most successful policies for securing CIIs involve collaboration between the public and private sectors. The need to transform and adapt governance and political systems has been accelerated by technological innovations and developments which have influenced the provision of essential services such as electricity, emergency services, health care, water, food, communications, fi-

nancial services and social security. This has forced governments to introduce more inclusive processes for managing these processes and their security, involving both the private sector and civil society.

Globally interconnected technology has introduced a new public policy dimension, requiring collaboration with the private sector and civil society about the provision of essential services. This is because the ICT systems that are central to providing these services are often owned or operated by the private sector.

Citizens do not always concern themselves with the processes involved in providing essential services, but want their governments to ensure that they are available and accessible. Any government which fails to ensure that these services are provided in an efficient and effective way is likely to lose the confidence of voters.

At the same time, government relies on the private sector to provide these services, because the information systems that provide access to essential services are either owned or operated on a commercial basis by the private sector. For government to provide these services efficiently, it has to have some working relationship with the private sector.

Pasquale (2011) points to the need for greater transparency following the global financial crises from 2007 onwards, marked by undisclosed risks to financial institutions, and argues that this has raised the need for an appropriate balance between transparency and secrecy in relation to securing CIIs. Kirtley (2006) also argues that government's desire to prevail over its adversaries must not be achieved at the expense of transparency and accountability.

As a result of technological innovations and developments, these services now rely on the effective functioning of a range of ICT systems, from generation through storage to transmission to the end user. This has led to governments intensifying their efforts to develop public policies and regulatory frameworks for ensuring that CIIs are protected against illegal or unauthorised access or intrusion.

Government and private sector cooperation on security of Critical information Infrastructures

According to Dunn-Cavelty and Suter (2009), there is general consensus, at least in the developed world, that these technological innovations have improved access to essential services, but have also created a public policy and national security challenge in that they expose society to a range of cyber threats. According to the Right to Know Campaign (2015), while technological innovations are forcing governments to establish structured relations with the private sector, the latter is sceptical about working with government as it is not very transparent about national security matters. As a result, the private sector is demanding greater transparency and accountability from government. However, many governments remain committed to the traditional approach of blanket secrecy about all matters involving national security, including CIIs.

Public comments on South Africa's Protection of State Information Bill show clearly that both the private sector and civil society are opposed to blanket secrecy, and see this as a tool for advancing or concealing undemocratic governance (Corruption Watch, 2012; HESA, 2012). The conflict between government and the private sector about these issues is further complicated by the South African Constitution (Act 108 of 1996), which entrenches the rights of freedom of expression, privacy, and access to information held by the state, and requires the security services to be subject to civilian authority and the rule of law. These sections provide the private sector, civil society and individual citizens with a legal framework for resisting government interference, and demanding more transparent and accountable government.

In this digital age, partnerships between government and the private sector are vital for protecting the accessibility and integrity of social services. Governments, globally, are preoccupied with making and implementing policy for combating cybercrime directed at national CIIs. Clark (1999) argues that CIIs in the private sector, including those used in managing banking, finance, railways, aviation, electricity, and gas and fuel pipelines, involve computer networks that are also not secured against cyber-attacks. He further notes that those networks are penetrated on a regular basis by hackers and sometimes by foreign powers, and that protecting them also requires a partnership between government and the private sector. This view is supported by various experts, including Suter (2007), Muhaya (2010) and Kyoung-Sik Min (2015).

Government and private sector cooperation on security of Critical information Infrastructures

South Africa has taken various steps to develop a policy and regulatory framework for securing its CIIs. The National Strategic Intelligence Act (no 39 of 1994) defines CIIs as electronic communications held by organs of state which are necessary for the protection of the national security of the Republic, and defines 'critical electronic communications infrastructure' as electronic communications products or systems used to transmit and store or transmit or store critical electronic communications.

Policy and regulatory initiatives include the Electronic and Transactions Act (no 25 of 2002), which provide for the registration of cryptographic service providers, an accreditation authority, the accreditation of authenticated products and services, and the identification and security of critical state databases (Act no 25 of 2002). More recently, the government has approved a National Cybersecurity Policy Framework (NCPF), which was published in December 2015. Inter alia, it deals with the identification and security of the CIIs.

In 2015, the government published a Critical Infrastructure Protection Bill for public comment, and this Bill has not been introduced in Parliament as yet. Its contents are not clear on the issue of Government and private sector cooperation. The NCPF notes that significant proportions of South Africa's CIIs are in private hands, or are operated on a commercial basis. This creates a need for institutionalised and entrenched cooperation between the public and private sectors about identifying and securing those infrastructures. The policy framework further outlines a strategy for protecting national CIIs, which, it says, should include clear information security procedures, access control and authentication, measures for the secure storage and archiving of critical databases, incident monitoring, and physical security measures.

The NCPF also calls for the adoption of international standards for securing CIIs. Mohammed (2015), among others, emphasises the importance of adopting such standards. He states that they help states and business to protect CIIs, and respond to and recover from cyber-attacks. The International Organisation for Standardisation (ISO) has developed standards for information security which deal with information security policies, risk management, human resource security, cryptography, access control, compliance, and business continuity measures (ISO 27001). Some of these standards have been in-

corporated into the NCPF. They provide a basis for cooperation between government and the private sector on information security.

In 2016, the South African government also tabled the Cybercrimes and Cybersecurity Bill, which provides a framework for identifying and adopting measures for securing CIIs. This Bill has been introduced in the National Assembly, but has not yet been passed or promulgated into law.

These policy and legislative processes have allowed the private sector to state its views about the proposed identification and protection of national CIIs. Among other things, it has allowed the major private sector entities which are likely to be declared NCIIs in terms of pending legislation to comment on the extent to which they are prepared to co-operate with government in identifying and securing NCIIs.

This researcher has consulted government and private sector role players in this regard. As noted earlier, developing policy and legislative framework on identifying and securing NCIIs rests on a cooperative model. However, there is no current evidence of structured cooperation, and the model is still being contested, with government still following the traditional national security approach, while the private sector is demanding greater transparency and accountability

Inter alia, the private sector regards government policies on secrecy as an attempt to conceal government inefficiency and protect corrupt officials. Numerous private sector entities have objected to the Protection of State Information Bill. This centres on opposition to what is regarded as government attempts to protect all state information, including information with little or no impact on national security.

4.2 Problem statement

Government has an overarching responsibility for ensuring the uninterrupted provision of essential services such as water, health, food, emergency, energy, telecommunications, transport and financial services. This responsibility is often expressed in constitutions and in subsequent policy, legislation and regulations.

Government and private sector cooperation on security of Critical information Infrastructures

As in many other areas, ICTs play a growing role in providing essential services. For this reason, these systems have become known as Critical Information Infrastructures (CIIs). Due to their increasing complexity and sophistication, many CIIs are owned and operated by the private sector. Government's growing dependence on these systems has introduced a new public policy dimension in that it needs to collaborate with the private sector as well as civil society to secure and protect these CIIs. The development of such policy and legislative framework in South Africa rests on such a cooperative model.

However, the private sector and civil society are contesting aspects of this framework, and there is no evidence of current collaboration between government and the private sector. Instead, relations are marked by hostility and a lack of trust. This lack of cooperation is not building confidence in the secure use of CIIs.

In 2014, a SABRIC report stated that cybercrime was costing South Africa approximately R1 billion a year. Reported cybercrimes and their negative impact on the provision of essential services provide additional evidence of the need for structured cooperation between the government and the private sector. Cybercrimes include phishing, a fraudulent way of acquiring sensitive information such as usernames, passwords and credit card details, and card skimming, aimed at capturing data from the magnetic stripe on the back of ATM cards. Hacking, gaining unauthorised access to computer systems and data, is also reported to be on the rise. Some cybercrime are non-financial and are aimed at giving hostile nations a competitive advantage. This includes the theft of intellectual property, and cyber espionage.

The current lack of cooperation between the government and the private sector is compromising the security of South Africa's NCIIs, including those involved in providing essential services. This poses a social, economic and national security threat to the constitutional order of the Republic. Hostile nations or other elements could exploit this situation to their own advantage. The private sector views the state's involvement in information security as censorship (Radu 2015), an attempt to prevent the free flow of information (HESA, 2012) or an attempt to restrict access to information (Cosatu, 2012; Helen Suzman Foundation, 2012).

Among other things, private sector and civil society role players argue that the government should not become involved in internet security, including limiting access to the internet, and that internet security should be a shared responsibility involving a range of stakeholders.

4.3 Purpose statement

The purpose of this study is to examine the need for structured cooperation between the South African government and the private sector as an effective tool for the implementation of public policy on the identification and security of the CIIs. It also seeks to identify some of the underlying causes of the lack of structured cooperation between the government and the private sector.

It will seek to make a case for structured cooperation on two main grounds. The first is that a failure to secure South Africa's CIIs poses a serious threat to national security, and may undermine national welfare and socio-economic development. Given this, every South African citizen has a role to play in ensuring the security of NCIIs.

In this context, the study examines the current policy and legislative framework to assess whether it provides an effective model for structured cooperation between government and private sector.

4.4 Research questions

The research addresses the following questions:

1. What are the existing policies, laws and regulations for protecting and securing South Africa's CIIs? Do they promote structured cooperation between the government and the private sector, and are they being implemented?

2. What should be done to achieve an appropriate balance between secrecy, transparency and accountability in securing CIIs?

3. Could the adoption of relevant ISO standards assist in promoting closer cooperation between the government and the private sector?

5 CHAPTER 2- LITERATURE REVIEW

5.1 Introduction

This report discusses government policy and legislation on securing and protecting CIIs, and the extent to which it adopts structured cooperation between the government and the private sector as a viable model for the implementation of the public policy on security of the CIIs. It specifically examines the extent to which government may have promoted cooperation between itself and the private sector in view of the fact the most CIIs are either owned or operated on a commercial basis by the private sector (Van Solms and Van Niekerk, 2013). Given that the protection of CIIs is a growing global issue, the research also compares the dispensation in South Africa with those in other countries.

This study acknowledges that this is a complex subject in that it involves values held by the state and society that are traditionally regarded as inimical, but have become intertwined due to technological developments. CIIs are physical and cyber based systems essential for the minimum operation of key economic and government sectors in a given country (Council of Europe, 2001).

They are regarded as critical because they ensure that all infrastructures which provide essential social services operate effectively and efficiently. Any vulnerability, unavailability, incapacity or destruction of these infrastructures can have a severe and even disastrous impact on the wellbeing of a nation. Essential services such as financial services, emergency services, transport, social welfare, energy, food processing, water, sanitation and electricity now rely on ICTs.

The South African government regards the protection of CIIs as an integral part of its national security mandate. As a result, it views this as the exclusive preserve of the executive arm of the state, particularly those agencies with the authority to deal with matters of security. While it may allow the private sector to persuade it otherwise, it will not be easy to convince state security policy-makers of the need for broad stakeholder consultation on matters of national security. In the past, when technology was less connected, it was easier to maintain linkages between technologies viewed as serving national

security interests and those that created linkages between the government and the private sector.

Given higher levels of connectivity, it has become practically impossible to retain the boundary between technologies used by government and the private sector in the course of providing essential services, and protecting them against unauthorized access. Today, they are commonly embedded in one device that is commercially available. This has created a new public policy challenge surrounding the provision of services that are vital to the socio-economic order and national security of the Republic.

Making policy for securing CIIs is more difficult in countries with no existing cooperation between government and the private sector, because most of the relevant information systems are owned and operated by the latter. This situation becomes even more difficult in the case of companies with a global footprint, or companies based elsewhere. Concerns are often expressed about the security of the technologies they provide to countries with which they only have a commercial relationship, and whether they can be trusted not to provide their countries of origin with a competitive advantage in this regard.

A national interest debate also arises around the issue of whether structured cooperation between a government and a multinational company does not amount to exposing the technical abilities of the country in question to a foreign entity whose commitment to its national development can be questioned. Despite this, engaging with a range of stakeholders has become a key element of policies for identifying and securing CIIs. Brynard (2007) argues that public policy development and implementation is no longer the exclusive preserve of government, with the private sector and civil society playing little or no role. He further states that public policy implementation is a complex process affected by a range of variables deriving from different perspectives, political systems and economic capacities.

In this perspective, successful policy implementation becomes less about the number of votes captured by a ruling party, and more about capacity, commitment, and coalitions of interest (Brynard, 2005). The ability to build alliances and share political power

among a range of stakeholders differs from country to country, and depends upon the abilities of different governments to rise above political differences for the greater good of the country. In this regard, this report analyses the different approaches adopted by various countries in building public and private sector alliances for implementing policies such as securing CIIs.

5.2 CIIs and cybercrime

According to the NCPF, the borderless nature of cyberspace and the interconnectivity of information networks offer vast opportunities for innovation, competitiveness and economic growth, but also provide unprecedented scope for cyber-attacks on countries, organisations and individuals, particularly attacks directed at NCIIs.

According to SABRIC (2016), there has been a significant increase in reported incidents of cybercrime directed at South African Intellectual Property Rights (IPR) and strategic installations, as well as cyber espionage attacks. While South Africa is in the process of developing a policy and legislative framework for identifying and protecting CIIs, it is still not being implemented, and elements of the proposed framework are still being contested by important stakeholders.

Experts generally agree that the bulk of criminal activity has shifted to cyberspace. In recent years, cybercrime, particularly those directed at CIIs, has escalated. Global cybercrimes are mainly crimes directed at national CIIs, requiring nation-states to take appropriate policy, regulatory and technical steps to protect and secure their CIIs. The borderless and transnational nature of cybercrime complicates attempts by nation-states to secure their CIIs, forcing them to seek bilateral and multilateral agreements that promote international cooperation in the fight against cybercrime. Put differently, it has become vital for nation states to seek international cooperation on combating cybercrime.

The leading international instrument for combating cybercrime is the Convention on Cybercrime, developed by the Council of Europe. Also known as the Budapest Convention, it provides guidelines for developing national responses to cybercrime, as well as a framework for international cooperation.

Government and private sector cooperation on security of Critical information Infrastructures

The Council of Europe is an international organisation aimed at upholding human rights, democracy and the rule of law in Europe, and promoting European culture. It works mainly by drafting conventions or treaties which set common legal standards for its member states. However, several of its conventions have been opened to non-member states. This includes the Convention on Cybercrime, which has also been signed by Canada, Japan, South Africa and the United States.

The Convention was adopted in 2001, and entered into force in 2004. By December 2016, 52 states had ratified the convention, while a further four states had signed the convention but not ratified it. South Africa was one of the first non-European countries to sign the convention, and has been participating in its implementation. Membership of the Convention is open to all nations of the world. The Council of Europe is actively marketing the Convention, and providing technical support and funding to new members.

The United Nations, through the UNODC, is also engaged in initiatives to develop an international instrument for promoting cybersecurity. One of the outcomes of this process is a comprehensive global report on country initiatives to build legislative and technical capacity to fight cybercrime (UNODC, 2013). Besides this, no other significant activity by the UN has been reported, and the Budapest Convention remains the only binding international instrument on this issue.

Members of the cybercrime committee of the Council of Europe are reluctant to support the UN initiatives on the grounds that it took the Council almost 10 years to negotiate the convention, and another 10 years to start implementing it. Given this, they argue it would be pointless for the UN to negotiate a similar convention rather promoting the existing one. They argue that a UN convention may be dictated by political considerations rather than focusing on defeating cybercrime, which remains a major security threat to global peace and economic development. They also argue that it is more important to build the technical capacity of member states to implement the existing convention than to develop new international instruments (TCY Report, 2016)

Government and private sector cooperation on security of Critical information Infrastructures

South Africa is one of few African countries that have participated in the Council of Europe convention capacity-building initiatives. Importantly, the Budapest Convention promotes cooperation between national governments and the private sector in combating cybercrime and ensuring the secure use of ICT. It also commits its members to helping to develop international criminal policy on cybercrime, and fostering international cooperation.

South Africa has also benefited from GLACY (Global Action on Cybercrime), a joint project of the European Union and the Council of Europe aimed at assisting countries worldwide to implement the Budapest Convention. Its specific objective was to 'enable criminal justice authorities to engage in international cooperation on cybercrime and electronic evidence on the basis of the Budapest Convention on Cybercrime'.

The project ran from November 2013 to October 2016. It has been succeeded by GLACY+, an extension project for supporting seven priority countries in Africa and the Asia-Pacific region, namely Mauritius, Morocco, Philippines, Senegal, South Africa, Sri Lanka and Tonga. The idea is that countries should also serve as hubs for sharing their experiences in their respective regions. Countries in Latin America and the Caribbean are also benefiting from project support.

Under the GLACY project, South Africa was assisted to develop various legal and institutional measures for combating cybercrime, including the Cybersecurity and Cybercrimes Bill, the Standard Operating Procedures for cybercrime investigation and prosecution, and the training of prosecutors and judges (GLACY, 2016). Glacy+ was due to start at the beginning of 2017 and continue for four years until 2020. It is aimed at further building the capacity of member states to combat cybercrime. The other notable achievement of the capacity building initiatives of the Budapest convention is the public-private cooperation in the implementation of the various training initiatives. Most of the different delegations from the member states consisted of experts on cybersecurity matters both from the Public and private sector entities in those countries.

As noted, the Budapest Convention and GLACY emphasise the importance of cooperation between the public and private sectors for dealing with cybercrime. Cooperation is

not limited to nation states only but is broadened to include global cooperation against cybercrime.

At its plenary meeting in 2013, the Cybercrime Committee adopted guidance notes to member states for implementing the provisions of the Budapest convention relevant to the protection of CII. They provide member states with advice on defining offences, gathering evidence, instituting prosecutions and imping penalties.

The Budapest Convention defines CIIs as those systems and assets, 'whether physical or virtual, so vital to a country that their improper functioning, incapacity or destruction would have a debilitating impact on national security and defence, economic security, public health or safety or any combination of those matters'. It notes that, while countries may define CIIs in different ways, member states generally accept that they involve services such as food, water, energy, transport, communications, finance, industry and defence, in both the public and private sectors.

The guidance notes deal with illegal access (Article 2), illegal interception (Article 3), data interference (Article 4), systems interference (Article 5), computer-related forgery (Article 7), computer-related fraud (Article 8), aiding and abetting (Article 11), and sanctions (Article 13). According to the guidance notes, these articles should be used to combat cybercrime directed at CIIs, and inform international cooperation. In addition, members of the Budapest Convention may develop laws and procedures for combating crimes directed at CIIs guided by these articles.

In 2014, the European Union Agency for Network and Information Security (ENISA) published a benchmark report entitled *Methodologies for the Identification of Critical Information Infrastructure Assets and Services.* Based on a survey of current practice in European countries, the study was aimed at providing guidelines for charting electronic data communication networks prior to improving their security.

The report demonstrates the extent to which public-private partnerships (PPPs) have drastically improved the legal and technical capacity of member states to fight cybercrime. Most European countries had established structures comprising both government and private sector role players to develop systems for identifying and protecting CIIs.

The report provides a summary of the methods adopted by European countries for identifying and protecting CIIs. It also notes that CIIs are increasingly dependent on computer systems for a variety of information management, communications and control functions, and that effective public-private collaboration is vital for identifying and protecting CII assets and services. Common methods used to identify CIIs include the following:

Identifying critical sectors of the economy: This process entails defining critical sectors, subsectors and services that are essential for the health, safety, security, and economic and social well-being of a nation. A risk assessment is performed to determine the impact of the unavailability, destruction or impairment of a given service on economic wellbeing and national security.

Identifying the critical and severity impact of services in the economy: This process takes into account the extended unavailability, impairment or malfunctioning of a CII, and its impact on any or all of the listed vital services.

Rating the extent of the impact: Severity levels are used to rate the extent of the impact. Maximum severity reflects grave damage to services critical to the socio-economic order and national security. Moderate severity reflects a higher level of tolerance and therefore lower costs of interruption, provided the functions in question are restored within a certain time frame. Moderate severity would cause 'serious damage' to vital services. Minimum severity means that specific functions of the electronic communications system can be performed manually, at a tolerable cost and for an extended period of time. Minimum severity will 'cause damage' or 'be prejudicial' to vital services.

Assessing the roles of owners or operators: The owners and operators of CIIs are responsible for determining the core processes, applications, and network assets and services used to operate the systems in question. The report summarises the initiatives undertaken by European countries to develop national cybersecurity strategies, notably those featuring public-private collaboration. These initiatives are summarised in Table 1.

Table 1: Sample of European countries with PPP arrangements in respect of CIIs

COUNTRY	POLICY/LAW	STRUCTURES	PUBLIC/PRIVATE COOPERATION
SLOVENIA	National Cyber Security strategy	Slovenian Ministry of defence (responsible for critical infrastructure in Slovenia) National Cyber Security Authority National CERT Intelligence agency/agencies Academia R&D organisations	Trust relationship between critical infrastructure owners/operators, National Cyber Security Authority and also Intelligence agency/agencies. Mixed ownership of CIIs. Public ownership is 15 % of sub-sectors. Adopted sectorial criteria in determining the critical infrastructures.
SPAIN	Spanish Law 8/2011 EU legislation on protection of CIIs Royal Decree 704/2011 National Cyber Security Strategy	Secretary of State - Ministry for Home Affairs National Security Council. Cyber Coordination Office Industry (CERTS) CERT for Security	National Plan for Critical Infrastructure Protection, strategic approach and State responsibility includes both the Public and private sector focus. Sectorial Strategic Plans for all sectors of the economy. Critical operators have to develop Operator Security Plans and Operator Specific Protection Plans.
LITHUANIA	Law on Cyber Security	Ministry of Interior (to develop CII identification methodology) Cyber Security Council (consists of public, private sectors and academia) National Cyber Security Centre (NCSC) State Data Protection Inspectorate Contact points for cyber security (designated by CI owners)	National Cyber Security Centre (NCSC) as the authority responsible for CIIP. CII owners shall inform National Cybersecurity centre, State data protection inspectorate, police about cyber incidents. CII owners shall designate contact points responsible for cyber security CII owners shall develop, implement and exercise their cyber incident management plans.
ESTONIA	Emergency Act 2009. Cyber Security Strategy.	Ministry of Interior (overall national coordinator). Cyber Security centre (monitor cybersecurity threats and advise CIIs) Information System Authority (law enforcement authority).	CII to conduct annual risk assessments, operational plan for critical services and report security incidents. CII operators monitored by the Ministry of Interior in the implementation of the security operation plan for CIIs.
HUNGARY	Critical Infrastructure Protection Act (166/2012)	Directorate for disaster Management (responsible for identification and protection of CIIs) CIP Network Safety Centre acting as the national security authority. CIP CSIRT.	The National Directorate General for Disaster Management plays a monitoring, controlling and coordination role, and includes the CIP CSIRT. The CIP Network Safety Centre was established to provide safety and to help the CII operator companies to protect themselves against network and cyber security incidents.
POLAND	National Critical Infrastructure Protection Program established in terms of the Crisis Management Act	Government Centre for Security responsible for CIP coordination and cooperation between government ministry responsible for security and CII operators or owners.	CIP programme created the PPP forum for private and public owners of CIP. It develops national priorities, objectives, and standards for effective functioning of critical infrastructure and development of detailed criteria for identification of CIIS.

Source: ENISA (2014)

As noted earlier, the cybercrime committee of the Council of Europe has undertaken a number of initiatives for global action against cybercrime, including training and capacity-building (GLACY, 2014). Under GLACY, cooperation between law enforcement agencies, service providers, and other private sector entities is regarded as essential for protecting the rights of Internet users and protecting them against crime. Strategies for promoting cooperation between public and private sector entities include:

- Establishing clear rules and procedures for access by law enforcement agencies to data held by service providers and other private sector entities.

- Fostering a culture of cooperation between law enforcement agencies and service providers as well as other private sector entities.

- Facilitating public--private information sharing across borders. In this regard, governments are advised to consider legal mechanisms for establishing structured public—private information sharing as well as trans-border measures for access to data, including the promotion of more efficient regional and international cooperation.

- Establishing continuous points of contact through adequate resourcing, training, legal powers and support for proactive cooperation domestically and with foreign counterparts, as well as emergency procedures for access to and disclosure of data in situations related to risks to life and similar circumstances.

This clearly demonstrates that cooperation between governments and the private sector entities has greatly helped European countries to develop the legal strategies, capacity and skills needed to fight cybercrime and secure their CIIs.

The UNODC global survey on cybercrime and cybersecurity (UNDOC. 2013) agrees with the need to identify strategic priorities in the fight against cybercrime. It concludes that there is a degree of fragmentation at the international level which does not provide a good foundation for international cooperation, caused by different multilateral or bilateral interests which, in some instances, hamper agreements about global instruments for combating cybercrime.

The report notes that a lack of uniformity among cybercrime laws has a negative impact on interstate cooperation, compounded by a lack of uniformity among bilateral or multilateral agreements on various matters relating to cybercrime. In this regard, the report notes that the Budapest Convention remains the only international instrument for promoting a common approach to cybercrime. It further argues that while divergent instruments legitimately reflect socio-cultural and regional differences, they could lead to the emergence of country 'clusters' that may not be well matched to the global nature of cybercrime. It also argues that traditional methods of international cooperation may not provide the timely responses needed to respond to cybercrime, and obtain volatile electronic evidence. As an increasing number of crimes involve geo-distributed electronic evidence, this will become an issue not only for cybercrime, but crimes in general.

The report raises the issue of trans-border access to data, regarded as a strategic priority in implementing the Budapest Convention, and states that the role of evidence 'location' needs to be reconceptualised, inter alia to obtain consensus on issues surrounding direct access to extra-territorial data by law enforcement agencies.

The report also refers to the need to provide law enforcement agencies, prosecutors, and the judiciary in developing countries with the technical capacity they need to investigate and combat cybercrime. An analysis of current national legal frameworks points to insufficient harmonisation of cybercrime offences, investigative powers, and the admissibility of electronic evidence.

The issues raised in the UNODC report are being addressed by the Council of Europe in the course of its capacity-building project. In fact, the UNODC report appears to confirm the Council of Europe argument that developing a new UN convention on cybercrime is unlikely to produce a different result to the Budapest Convention and the GLACY initiative.

A cause for concern is that as long as global multilateral institutions do not adopt a common approach to the fight against cybercrime, cybercriminals will continue to take advantage of these divergent approaches and the resultant fragmentation of international efforts to combat cybercrime. Therefore, a united approach to the fight against global cybercrime is vital.

Given this, and the continued growth in cybercrime, the UN and the Council of Europe should agree on an acceptable international mechanism for implementing existing international instruments such as the Budapest and African Union conventions, with a focus on building the capacity of member states. Waiting for a UN instrument is unlikely to be a better solution to the current global challenge than to involve as many countries as possible in implementing the existing instruments. Cybercrime is increasing at an alarming rate, particularly targeting countries with little or no capacity to respond to cybercrime, and with weak economies and security systems that are vulnerable to attack. Given this, the capacity-building initiatives of the Council of Europe is a welcome intervention.

5.3 Methods for identifying CIIs and public-private partnerships: the South African approach

The initiatives referred to above demonstrate that public-private partnerships (PPPs) are an effective strategy for combating cybercrime. Added to this, countries should participate in global initiatives against cybercrime via international instruments that promote cooperation on this matter as well as on information-sharing.

Adeleke (2014) argues that public-private cooperation is often very complicated, largely because of the different political interests of those involved. He believes it is a form of participatory democracy in which those who are governed play a significant role in holding government accountable, not only by being given access to information, but also by being given a stake in the exercise of state power. In essence, he argues that those with the authority to exercise power must agree to the notion that power should be shared with the people, in the course of addressing the needs of society.

As noted previously, approaches to cybersecurity vary, with some countries regarding this as an issue involving information systems security only, and others as a matter of national security. These approaches determine the extent to which governments involve the private sector in their approach to cybersecurity. Governments in the former category tend to focus on building the technical capacity needed to secure its critical systems against unauthorised access. This would include the adoption of appropriate information

security standards. In countries in the latter category, it becomes very difficult for the state to learn and share information about best practices with other jurisdictions due to the focus on secrecy.

International initiatives promoting public-private cooperation on securing CIIs against cybercrime have been described above. Those initiatives have had a direct impact on South Africa, not only due to the escalation of cybercrime, but also because it is a significant global economic player. This status and its implications for CII are reflected in its membership of the Budapest Convention. Initiatives under the Convention have had a direct impact on South Africa's legislative, regulatory and technical capacity-building initiatives, particularly in respect of public-private partnerships.

This report assesses the policy and regulatory choices by policy-makers in preparing South Africa to become a global player in the technology security space. It will also look at lessons that may have been learnt by successive South African governments in dealing with public-private cooperation in view of the international approach discussed above, and taking into account that South Africa is part of the international initiatives to promote cybersecurity.

Public-private cooperation creates an enabling framework for more inclusive governance and the sharing of the resources. While governments often experience a scarcity of skills, they need to develop and implement policies that have far-reaching implications for social, economic and national security. Connectivity also had a direct impact on the ability of a country to attract foreign direct investments, which are critical for national development. All these matters require public-private cooperation aimed at ensuring that the country in question is able to attract much-needed foreign direct investment, thereby ensuring economic growth. Given this, the NCPF seeks to enhance cybersecurity, but also accepts that South African cyberspace is vulnerable to attack by global cybercriminals targeting the proper functioning of the CIIs that are vital to the provision of essential services.

In this regard, the NCPF emphasises the importance of balancing measures for promoting cybersecurity with measures aimed at preventing cybercrime. The NCPF states that there is a need to find an appropriate balance between the risks associated with the use

of information systems and accepting the reality that the use of information technology has become a central aspect of service provision in modern societies. The NCPF further states that the growing threat of cybercrime due to the vulnerability of CIIs should not impede the role of ICTs in stimulating economic growth and national development. It goes on to prescribe measures for securing CIIs and protecting them against cybercrime.

As noted earlier, the global connectivity of information systems requires a paradigm shift in dealing with the security of CIIs as most are either owned or operated on a commercial basis by private sector entities. Historical data shows that public policy on protecting CIIs in South Africa has evolved over time. It was initially dealt with as a purely physical infrastructural matter in terms of the National Key Points Act (No 102 of 1980). The main objective of the Act was to provide for the declaration and security of National Key Points. It focused on physical infrastructure rather than on information security. In terms of this Act, if the Minister was of the view that any place or area was so important that its loss, damage, disruption or immobilization might prejudice the Republic, or whenever he considered it necessary or expedient for the safety of the Republic or in the public interest, it could be declared a National Key Point. The owner would then be advised of this in writing.

He / she would then be required to take appropriate steps to secure the National Key point. If the owner refused to do so, or failed to provide the specified protection, the Minister could either order him or her to do so, or provide the required protection, or require the owner to reimburse the state for the costs involved. The Act did not envisage collaboration between the state and the private sector. The state played all the key roles, thereby creating the impression that security was the exclusive preserve of government, and the Minister in particular. Even the list of National Key Points was kept secret. This changed recently when this secrecy was challenged and the courts ordered that the list of National Key Points be disclosed, in line with the constitutional right of access to information held by the state. The application was brought against the Minister of Police by the Right to Know Campaign (Right 2 Know and another versus the Minister of Police, 2014).

The National Key Points Act is old order legislation which is now subject to the South African constitution of 1996. This means that all the provisions of this Act which are inconsistent with the constitution are invalid and unenforceable.

After the transition to democracy in 1994, South Africa adopted ICT policies that created conducive conditions for innovation and development. Due to these technological innovations, critical services such as financial services, emergency services, transport services, social welfare services, energy generation, food processing, water, sanitation and electricity generation, transmission and distribution are now dependent on ICTs. Criminals took advantage of the vulnerability of some electronic systems to launch attacks against countries, organisations or individuals in order to achieve their objectives, and South Africa was also a victim of these crimes. Rising cybercrime forced the government to enable law enforcement institutions to deal with cyber related threats, including those directed at CIIs. In view of escalating incidents of electronic crimes and soon after signing the Budapest Convention in 2001, South Africa initiated a review of legislation impacting on cybersecurity, and dealing with the criminalisation of cyber-related acts.

This process enabled South Africa to respond to the challenge of cybercrime, and to comply with the requirements of the Budapest Convention. This included the adoption of the Electronic Communications Transactions Act (No 25 of 2002), aimed at creating a legal framework for electronic transactions and related security matters. Specifically, the Act empowered the relevant Minister of Communications to 'declare certain classes of information which is of importance to the protection of the national security of the Republic or the economic and social well-being of its citizens to be critical data', and to establish procedures to be followed for identifying and registering critical databases (Sections 53 and 54). The Act also introduced the notion of cybercrime, defined as unauthorised access to, interception of or interference with data (Section 86), computer related extortion, fraud and forgery (Section 87), and aiding and abetting (Section 88). The procedures to be followed in declaring certain classes of information as critical data is consistent with those followed by the European countries reflected in Table 1. How-

ever, it does not refer to the private sector, although it was well known at the time that most CIIs were owned or operated by the private sector, and it remains unclear how the government intended to deal with CIIs in private ownership. In the event, this clause has not been invoked since 2002.

Also in 2002, the government passed the Electronic Communications Security (Pty) Ltd Act (No 68 of 2002). This Act established a government entity responsible for securing the critical electronic communications of organs of state. It has since been repealed, but it is important to mention that it contained mandates similar to those provided for in the ECT Act, but to a different entity. Not much progress was made with the intended process of identifying and protecting critical electronic communications and critical electronic communications infrastructures of organs of state. The other limitation of this Act was that it confined the identification of CIIs to Organs of State. This mean that it did not cover the bulk of CIIs, which are owned or operated by the private sector. This Act was later repealed by the General Intelligence Laws Amendment Act (No 11 of 2013) and the National Strategic Intelligence Act (No 39 of 1994). This legislation requires the Minister of State Security to issue regulations prescribing the processes for protecting critical electronic communications against unauthorised access or any technical or related threat.

These regulations have not been published, and it is therefore difficult to assess the extent to which the Minister will seek to cooperate with the private sector in identifying and securing CIIs. Prior to approval of this amendment in 2013, the government initiated a process for developing a National Cybersecurity Policy Framework (2012). The NCPF acknowledges that South Africa, like many other countries, has become dependent on the Internet for governance and other purposes, that the Internet has become indispensable to many South Africans, and will become even more so as more and more people access the information highway. Taking into consideration the increase in national and international bandwidth in South Africa, it notes, cybercrimes and threats will continue to increase. These cybercrimes and threats have the potential to impact on national security and economy. In response, the NCPF seeks to establish public-private

partnerships for national and international action plans, ensure the protection of NCIIs, and promote a comprehensive legal framework for governing cyberspace.

To these ends, the NCPF requires the development of a National Critical Information Infrastructure Policy dealing with third-party access to NCIIs, access to and authentication of NCIIs, storage and archiving of critical databases, incident management and business continuity, and the physical and technical protection of NCIIs (NCPF, 2012). While the private sector has generally accepted most of the proposals in the NCPF, it has not supported the proposals for identifying and securing CIIs. Some private sector entities have declared their intention to have this proposal declared legally invalid on the grounds that it contravenes the constitutional right to privacy. The Banking Council of South Africa, which represents most South African banks, argues that the inclusion of the private sector within the overly broad definition of state-managed/controlled National Critical Information Infrastructures provides cause for concern, as this would result in significant regulatory, bureaucratic and security overlaps, and potential systemic risk to the private sector, let alone significant and potentially unwarranted compliance costs (Banking Council of South Africa 2016). It has also recommended that the private sector should be removed from this section of the proposed legislation.

The Association of Fraud Examiners, one of the private sector organisations which commented on the Cybercrimes and Cybersecurity Bill of 2015, suggested that no private sector infrastructure should be designated as NCIIs, as this would be 'tantamount to the nationalisation of these infrastructures' (Association of Fraud Examiners, 2016). Taking these and other private sector views into account, it will be important for the government to ensure that cyber policy complies with the constitution. It would be difficult or impossible for the government to build a productive partnership with the private sector if the latter feels that its policies and strategies infringe the constitutional rights of private sector entities. Any policy that seeks to promote public-private cooperation should conform to the constitution. It is not immediately clear whether the government failed to implement the 2002 laws because it realised that it would have to negotiate the implementation of these policies from a position of weakness.

The other major problem is the government's approach to policy development and implementation. It appears to approach this from a 'big brother' position, using its majoritarian authority to compel the private sector to comply with policies that may be difficult to implement, or when private sector procedures would have been a better option. This approach reduces the role of the private sector to that of commenting on government plans, with the latter having the right to decide whether to agree with these comments or dismiss them outright. Ultimately, this approach does not benefit the government, but weakens its ability to involve the private sector in policy implementation. As argued by Adeleke (2014), effective participatory democracy strengthens government even in cases where its proposals could be legally challenged on the grounds that they conflict with private and individual rights.

From a narrow perspective, the current proposals for state-private collaboration in identifying and securing CIIs may be seen as interfering with the rights of the owners of the private sector entities in question. From a broader perspective, these entities may be regarded as providing a vital service which, if compromised, altered or destroyed, would have grave national consequences. It becomes very difficult for the government to seek the support of private sector or non-government entities when its approach is not guided by some form of participatory democracy that is guided by a desire to serve the broader national interest rather than a narrow majoritarian one. Once a government becomes technical in its interpretation of its right to majoritarianism, it loses credibility among members of society who did not necessary vote for it but were prepared to accept it as a legitimate authority. In such a case, private sector or non-governmental entities tend to rely on the courts to reinterpret government policy. This not only delays policy implementation, but deprives the government of vital technical support that may be in the hands of the private sector.

Brynard (2005) concurs with this view, and submits that the government should consider observing the so-called 5C protocol in implementing policy, namely content, context, commitment, capacity and clients/coalitions. It may be argued that the content and context of the NCPF policy is responding to the needs of the stakeholders in so far as the

need for a policy mechanism to deal with Cybersecurity issues in South Africa. Issues of the means and measures adopted to achieve the policy objectives are informed by content. Mtshali (2014) also argues that context provides institutional understanding on where and how the policy operates or travels and therefore the implementation of policy may also depends on whether the policy is consistent with applicable laws and the constitutional arrangements.

She submits that all of these matters become very relevant in the implementation of the policy. Commitment addresses issues of implementers and their attitude (willingness and ability) towards implementation. Capacity informs on the existence or non-existence of administrative and other capabilities for doing the job. It therefore becomes important to ensure that for policy implementers to take into account that importance of the support or lack thereof of clients and coalition in the implementation of public policy and how such support or lack thereof affects actors in promoting or frustrating implementation.

Despite the policy requirement for government and private sector cooperation in the identification and security of the CIIs, government has not been able to implement this policy because of lack of stakeholder participatory approach due in part to government failure to consider broader views of all stakeholders. This has made it impossible to implement this policy on the security of the CIIs. There is no guarantee that the section on the security of the CIIs in the current Cybersecurity and Cybercrimes Bill (2016) will be successfully implemented taking into account the comments of some of the members of the private sector referred to above. It is likely that these policy provisions will be challenged in Court by the private sector because a culture of national unity and common national interests has not created by the relevant authorities.

5.4 Secrecy, transparency and accountability

The credibility of those with the authority to govern depends on how they exercise the power given to them by the governed, and their willingness to share this power with citizens. This lies at the heart of participatory democracy. Those in power who rely on majoritarianism in exercising their powers will be constantly challenged in the courts be-

cause of the breakdown of trust between the governing and the governed (Cosatu, 2012). Issues of secrecy, accountability and transparency become areas of disagreement between the government, the private sector and civil society, with the latter two fighting for more transparent and accountable policy implementation, while the government would prefer to maintain secrecy, particularly in respect of issues related to national security. As noted earlier, private sector and non-government entities have contested aspects of government policy relating to information security (Helen Suzman Foundation, 2012). Issues of national security and right of access to information have been central to the recent mistrust and contestation between government and the private sector.

The government has not undertaken any visible initiatives to reach out to the private sector and civil society in order to achieve a common understanding of issues relating to national security. Parties have repeatedly gone to court in an effort to resolve this impasse, which is tantamount to asking the courts to resolve issues what should really be dealt with by the executive. Majoritarianism leads to a credibility deficit among other social role players. While it would have been ideal for government and the private sector to cooperate and secure identified CIIs for the greater good of citizens, this does not seem possible in the current climate in which trust between the two key stakeholders seems to have broken down.

This has happened despite the fact that it is vital for these two parties to agree on an appropriate balance between secrecy and transparency in respect of identifying and securing CIIs. The interests of both stakeholders will be best served by secured CIIs able to deliver essential services without interruption. In the case of the Right 2 know Campaign versus Minister of Police (December, 2014), the Right to Know campaign succeeded in getting a court order to compel the Minster of Police to disclose the list of declared National Key Points under the National Key Points Act. In a judgment handed down in December 2014, Judge Roland Sutherland ruled that the refusal by the Minister of Police to release the demanded list of the declared National Key points was unlawful and unconstitutional. He further stated that 'It is wholly unsatisfactory that political office bearers and senior civil servants should have to perform their duties under a cloud of suspicion of incompetence or dishonesty. Transparency about all the facts is neces-

sary to either repair the rot, if any exists, or dispel the lack of confidence which the citizenry will continue to nurse if the facts are concealed.'

Even though transparency is an important democratic tool for enforcing accountability, it also creates 'political winners and losers' (Berliner, 2015). It creates political winners within the groups in power, and the groups outside power. Those in power would ordinarily want to have a controlled transparency so as to avoid a situation where the shortcomings of government are laid bare in the public. This would be political suicide in that the government would have given ammunition to its opposition to campaign for its removal from power.

Berliner (2015) further argues that limited transparency allows groups in power to maintain privileged control over government information for themselves and their allies, thereby monopolising opportunities. By contrast, full transparency gives all groups and individuals equal access to government information, thereby creating a level playing field for monitoring officials and holding them accountable. Even in cases where governments would benefit from private sector assistance, they often refuse to bring the private sector on board, mainly due to political considerations. This is often due to suspicions that the private sector entities in question may be aligned to opposition parties, and provide them with access to sensitive information. Opposition parties are also politically opportunistic, because they tend to use the private sector in order to gain an insight into government inefficiency for their own political benefit.

This political contest is problematic when it touches on matters with social, economic and national security consequences. Members of the public would prefer politicians to bury their political differences in these instances, for the greater good of the nation. Adeleke (2014) contests the idea that transparency and access to information promotes trust between the government, the private sector and civil society. According to him, this narrative assumes that the 'distrust of government arises firstly as a result of lack of information, and when such information is disseminated, such information is devoid of manipulation by the discloser and that disseminated information is used in a particular form of rational way to formulate a particular public opinion that constitutes a form of

democratic surveillance' This view is consistent with what really happens when protests continue for an indefinite period despite government releasing information to justify its inability to meet the obligations of civil society and the same applies more frequently when negotiations over salary increases break down between government and employee representatives on the grounds of mistrust between the negotiators, regardless of how much information would have been given to the employee representatives to show the government's inability to meet their demands.

Adeleke (2014) further argues that the development of participatory democracy cannot be judged only on the basis of access to information and transparency, but also on the relations of trust built when those in power are willing to share power with those who are governed, particularly on matters that define the national interests of a country.

While the government has introduced various policies and laws since 2002, they have not been implemented, largely because the 5C protocol has not been observed. Government needs to accept that the owners/operators of CIIs should themselves address the security of their assets and the continuity of their business (Australia-New Zealand Counter Terrorism Committee, 2015). The survey of successful European approaches to securing CIIs reflected in Table 1 shows that public-private cooperation has played a central role. This explains why South Africa has struggled to implement its policies.

5.5 CIIs and information security standards

Information security is governed by international standards such as ISO (ISO/IEC 27000) that are adopted on a continuous basis by the relevant international bodies. National information security policies or laws should comply with these standards. Institutions that have adopted these standards generally require their trading partners to be certified as compliant. This is because information security is a pillar of essential services and economic development. Chia (2012) notes that that confidentiality of information refers to information protected from disclosure to unauthorised parties; integrity of information refers to protecting information from being modified by unauthorised parties; and availability refers to information that authorised parties are able to access when needed. These principles guide information security in order to assure end users that all

reasonable steps have been taken to ensure the confidentiality of information, to prevent it from being compromised or degraded, and ensure that it has retained the required level of accuracy, completeness and dependability.

The following text refers to ISO standards that are vital for securing CIIs, and would promote public-private cooperation. The government could also use them as a basis for compliance with security requirements.

5.5.1 Confidentiality, integrity and availability

Availability seeks to ensure that the owner of the information has taken all the necessary steps to ensure that information is available to and accessible by those with the necessary authorisation to access such information. These principles are very important as they provide end users with confidence and trust in the secure use of ICT. Policies, laws and regulations are intended to ensure that that the principles of confidentiality, integrity and availability are realised. Consistent with the above, the NCPF (2012) emphasises the need for government, the private sector and civil society to enjoy the full benefits of a safe and secure cyberspace. In order to achieve this objective, its stated purpose is to create a secure, dependable, reliable and trustworthy cyber environment that facilitates the protection of CIIs while strengthening the national security interests of the Republic.

The NCPF also recognises that global interconnectivity plays a key role in respect of information infrastructures, and therefore promotes the adoption of international information security standards. These standards will play a vital role in building the confidence of South Africans in the secure use of ICT. Susanto (2011) concurs that information is the life blood of organisations and a vital business asset in today's information-driven world. Therefore, securing information systems is vital. While globalisation and the interconnection of networks has improved access to essential services, it has also increased the exposure of organisation to cyber threats. International In order to mitigate these risks, standards have been developed to provide common international guidelines, objectives and controls.

When organisations adopt these information security standards and protocols, they build trust among their clients and other stakeholders that they are serious about securing their information systems. Hassouna, Bari and Mohammed (2015) agree that the adoption of cyber security standards help organisations to prepare for, respond to and recover from cyber-attacks. Governments can adopt these standards as a basis for managing information security risks to CIIs, and evaluating service providers. As the biggest consumer of the essential services provided by the private sector, government can also use information security standards as the minimum requirements for doing business with government. It will also allow the government to formulate clear compliance evaluation criteria. Besides implementing the information security domains provided for in ISO 27001, CII operators are also required to comply with all applicable policies, laws and regulations, particularly the NCPF.

Compliance with international standards such as ISO 27001 enables companies to be certified as compliant, thus enhancing its ability to attract international business. The government is also expected to is adopt a flexible approach to the implementation of standards, thus giving companies some leeway in applying them in practice. These information security standards present the best opportunity for public-private cooperation in that it allows the government to focus on monitoring compliance with the adopted standards while also using compliance as an incentive for preferential government contracts. This would give the private sector a reason to invest in the implementation of a comprehensive compliance framework.

5.5.2 Compliance audit and risk management

This standard seeks to provide guidelines for identifying, evaluating and mitigating information security risks before they affect service delivery (ISO/IEC 27005). It also requires compliance with statutory, regulatory or contractual obligations as well as security requirements. Risk assessments should be done continuously to determine areas of vulnerability and ensure appropriate remedial action. In order to be effective, information security must be risk-oriented. CIIs need to implement baseline security controls and other measures identified through threat and risk assessments or needs analysis ex-

ercises. The application of this standard takes into account policies, laws, and regulations dealing with government-wide risk assessment processes.

The repealed Electronic Communications Security (Pty) Ltd Act (No 68 of 2002) provided for periodic risk assessments of NCIIs, taking into account technological developments and the criticality of the NCII in terms of the severity levels referred to previously. The State Security Agency, as the government department responsible for securing CIIs, issued regulations prescribing periodic reviews of the risk status of NCIIs, as well as the risk assessment methodology. The South African approach to risk management mainly focused on the security of CIIs within organs of state, and not those in the private sector. This reflected the absence of structured public-private cooperation. The repealed Act defined critical electronic communications' as electronic communications held by organs of state which are necessary for the protection of the national security of the Republic', and critical electronic communications infrastructure as 'electronic communications, products or systems used to transmit and store or transmit or store critical electronic communications'.

As noted previously, not much was achieved in implementing these laws. As a result, South Africa remained exposed to a range of security threats. More recently, the government has introduced the Cybersecurity and Cybercrime Bill, which empowers the Minister, following recommendations by the Cyber Security Centre and after consulting proposed NCIIs, to declare information infrastructures as NCIIs of they are so strategic that any interference, or their loss, damage, disruption or immobilization, may prejudice the security, defence, law enforcement, health, economy, essential services or international relations of the Republic.

The Bill allows proposed NCIIs to object to such classification, after being informed of this by the Minister. Section 60 of the Bill requires the owner or manager of a NCII to organise a yearly audit, and inform the Director General of the State Security Agency of the intended audit.

The Bill does not state whether the Minister should follow a sector or service approach to declaring NCIIs. The critical service approach as proposed by Mattioli and Bencheton (2014) looks at the criticality of the service to the social, economic and na-

tional security of a country, which also informs the eventual declaration and security measures. The Bill does not express itself on the role of owners of CIIs in this process except that they would have an opportunity to oppose the intended declaration. The Bill does not indicate whether identification will follow a sector approach in terms of which the impact of each sector on the social, economic and national security of the Republic would be assessed and given the necessary categorisation. The Bill also does not refer to the certification of NCIIs as compliant with international information security standards.

5.5.3 Information security governance

Information security policy (ISO/IEC 27001: A.5) sets standards for governing information security in a given organisation. It is used as a basis for conducting risk assessments and audits of compliance with relevant laws, regulations and directives (Fenz, Heurix, Neubar & Pechstein, 2014).

Some of the South African laws dealing with information security overlap, or do not provide clear guidelines for implementation. There is no coordination between the entities involved in administering these laws.

These overlaps and contradictory mandates lead to the duplication of resources and tensions between departments, resulting in information security rhetoric that is not backed up by coherent implementation.

Information security policy is meant to take the NCPF into account, and to create various structures with specific roles. The NCPF establishes the JCPS Cybersecurity Response Committee, tasked with coordinating cybersecurity activities and at as a central point of contact on all cybersecurity matters pertinent to national security. This provision is also contained in the Cybersecurity and Cybercrimes Bill. The Bill provides for the establishment of a Cybersecurity Centre within the Department of State Security. The NCPF also mandates the Cybersecurity Centre to assume responsibility for protecting NCIIs, including introducing public-private partnerships and action plans.

Besides these structures, a Cybersecurity hub is meant to be established within the Department of Telecommunications and Postal Services, serving as a forum of cooperation and engagement between the public and the private sector on matters relating to cybersecurity culture and awareness as well as local and international cooperation issues. Government and private sector CSIRTs are meant to be established to coordinate responses to identified cybersecurity incidents. The policy framework also calls for measures for identifying and categorising CIIs in critical sectors of the economy such as the maintenance of national law and order, the provision of public health or social services, economic growth, or environmental matters. The determination of the sector impact and the severity levels of impact will be informed by the categorisation and severity ratings of the CIIs. The severity ratings and impact analyses are based on maximum, moderate and minimum severity.

The ISO standard on information security policy also requires executive management to develop an information security strategy setting out the vision and mission of the organisation in respect of information security. The strategy document should also outline management's commitment to information security. The strategy is also meant to address internal and external factors that might have a negative impact on information security.

As regards human resources security, the standard requires employees to be subjected to security screening before employment, depending on the level of access they will have to valuable and classified information. Not all employees or contractors should be granted access to CIIs. Employees with lower levels of security clearance are meant to have access to information equal to their security competency.

Theoharidou (2010) notes that in terms of ISO 27005, risk assessments should be conducted to determine the value of information, identify threats and vulnerabilities, and identify existing controls and their effects. In addition, risk assessments should prioritise the assessed, risks and rank them as a basis for mitigation. Government and CII owners need to develop a risk assessment process that outlines the scope of the risk assessment as well as the risk rating, or overall impact, taking into account the interdependences of the critical systems and the service. The risk assessment process needs to identify, ana-

lyse and evaluate risks in relation to the criticality of the service provided by the relevant CII.

Contractors that may have access to CIIs should be subject to security clearance, and should not be given unlimited access to information. For information security to be effective, organisations need a smooth intersection between people, processes and technologies, and government and CII operators need to ensure that individuals who have access to classified information and assets are reliable and trustworthy, and loyal to the Republic.

This standard also encompasses disciplinary procedures for violations, exit strategies to ensure an understanding of the need to preserve confidential information beyond employment, and restraint of trade. As regards asset management, this standard seeks to regulate the management of information security assets from an information security perspective, highlighting the importance of maintaining a comprehensive information assets inventory, assigning ownership, and outlining the acceptable use of these assets. CII operators are required to develop rules for information security inventories with an emphasis on information generated, transmitted, stored and destroyed/disposed. The inventories should cover both physical security assets and ICT assets. The asset management process should also deal with the destruction of information security assets such as shredded material and old ICT equipment.

As regards access control, the standard seeks to integrate physical and logical access using new technologies such as smart cards and biometric technologies to ensure the easy monitoring of access to buildings and computer networks. The idea is that if an employee has not logged in at a perimeter access point, she/he should be denied access to the organisation's computer network. Access control in all NCIIs should preserve the confidentiality, integrity and availability of information. Control measures should be implemented and monitored in accordance with applicable ICT standards and procedures to ensure the confidentiality, integrity and availability of information.

5.5.4 *Physical and environmental security*

This standard seeks to prescribe baseline measures to address these disasters and the response approach and seeks to regulate the broad physical and environmental controls that need to be observed by al CIIs from perimeter fences in stand-alone buildings, entry controls into buildings and high security offices in order to prevent unauthorized access (ISO 27002). Environmental factors like fire, bombs, and floods need to be regulated. Standard operating procedures need to be prescribed and observed for cabling, and uninterrupted supply of air-conditioning and power in certain areas. Security alertness needs to be a point of emphasis for every employee, especially in relation to strangers lingering in buildings.

The standard also addresses regular threat assessments need to be conducted in order to monitor changes in the threat environment. On information security systems acquisition, development and maintenance, the information security policy needs to provide for provide guidance on continuous R&D process as an integral part of the security of the CIIs. Government has its own research capacities which can be used by both Government and NCII owners for further technology or systems development and also to consult on matters related to verification of industry-based soft wares.

5.5.5 Security breaches and incident management

The continuous monitoring of ICT security incidents and the planning of responses to such incidents is a vital protection mechanism of NCIIs. In this regard, the NCPF requires the Cybersecurity Centre to develop processes and procedures for incident monitoring as well as a response plan in accordance with ISO 27035. It also requires the Minister to provide guidelines and procedures for detecting potential security breaches and the expected response to each incident type, aimed at ensuring that critical systems remain operational, as well as actions to be taken to recover and minimise exposure to a system compromise, and the role of Private Sector Security Incident Response Teams in supporting the CSC.

5.5.6 Business continuity and recovery plans

This standard deals with backups, redundancy sites, and minimum security requirements (ISO 27031). The NCPF requires all CIIs to have business continuity and disaster recovery plans. They are also required to build data centres for the safe storage of sensitive data. Not minimum requirements have been laid down. Some state entities have outsourced the security and storage of their data to the private sector.

Cloud computing and data storage is growing trend which seems attractive to some institutions. However, there are no risk assessment procedures or regulations for managing offsite storage. The question to ask every institution is the following: If an aircraft crashes into your building, will you be able to function tomorrow? When your back-up information is managed by industry, what control do you have over that information? Some organisations have outsourced the hosting and management of critical databases. Do those private sector entities conform to the prescripts for securing, maintaining, and controlling access to these databases?

6 CHAPTER 3- RESEARCH METHODOLOGY

Secondary and primary data have been gathered for this study. Secondary data, as reflected in the literature review, was gathered to illuminate international practice, especially in respect of public-private collaboration on cybersecurity, to provide a context for examining CII policy and legislation in South Africa. As regards the primary data, the researcher interviewed senior government policy and security advisers to gather their views on key aspects of South African policy, notably the issue of whether it promotes collaboration between the state and the private sector in securing South Africa's CIIs. Lastly, the researcher recorded the views of critical sector companies by studying their comments on government legislation, and conducting interviews with key executives.

6.1 Conceptual framework

CIIs play a central role in providing essential services in well-functioning and democratic states. Therefore, ensuring that the CIIs are protected and secured is a key element of social and economic stability and national security. Most CIIS are owned or operated by private sector entities. Therefore, securing CIIs requires effective public-private collaboration.

Most countries in the developed world have successfully implemented models and standards for introducing public-private partnerships. While this is the stated intention of the South African government as well, this has not been translated into effective policy implementation. This study is aimed at examining the South African policy and legislative process to establish how it intends to implement this model, assess progress made, identify the factors that are hampering this process, and suggest how they could be removed, thus opening the way to an effective cybersecurity regime involving all South African stakeholders.

As noted previously, Brynard (2005) argues that the 5C protocol -- content, context, commitment, capacity and clients/coalitions -- are the pillars of successful policy implementation. Inter alia, the South African policy process is assessed against these criteria.

6.2 Research approach

This is a qualitative study, and an instance of critical research. According to Neuman (2011), critical research is not only aimed at studying society, but also aims to change it. More specifically, critical social science researchers seek to transform social relations by exposing sources of social control, power relations and inequality. This perspective helped to inspire the researcher to conduct this research.

While, until recently, issues of governance and national security were the exclusive preserve of those in power, this situation has changed fundamentally. Today, the only route to sustainable development and national security is to share power with citizens, inter alia via structured cooperation between government, the private sector and civil society.

Countries need to transform themselves by adopting democratic forms of governance marked by transparency, accountability, and respect for the rule of law. This study seeks to show that good governance and sustainable development can only achieved by means of cooperation between all national role players, and that this route should be adopted in South Africa as well.

6.3 Research design

The research focuses on document and process analysis and is divided into three sections. The first deals with governance matters such as existing policies, laws and regulations. The second part focuses on the process for identifying and securing NCIIs, taking into account the importance of enterprise information security architecture. This analysis is aligned with existing policies, regulations and laws. More specifically, it focuses on the extent to which the government is cooperating with the private sector in securing these CIIs. The secondary data shows that many developed economies have implemented policies and strategies that promote structured public-private cooperation within and among nation states, while taking global interconnected technologies into account. Various models are assessed in order to find an appropriate model for South Africa, taking into account its unique challenges in this regard.

The research focuses on models of public-private cooperation in other jurisdictions. This data is then used as a basis for engaging with South African policy, legal and security experts. Secondary data is analysed in order to develop a comparative analysis of South African policies and implementation strategies compared with those in selected jurisdictions. Senior government policy, legal and security experts were interviewed to gain their perspectives on the research questions and also to solicit their views on the best approach for South Africa.

These officials were given an option not to disclose their identities or positions. They all indicated that they would prefer their identities to be disclosed as they were dealing with the issues covered in the report, and were engaging the private sector. In order to focus the interviews, questions were supplied to them in advance. The selected officials play key roles in the government policy process. They are:

1. **Advocate S. Robbertse**, State Law Advisor on Cybersecurity legislation and relevant constitutional matters in the Department of Justice and Constitutional Development,

2. **Mr Jabu Radebe**, Chief Director, Cybersecurity and Critical Information Infrastructure Policy in the Department of Telecommunications and Postal Services,

3. **Mr V. Jaquire**, Cybersecurity expert, and Manager of National Information Security Risk Management within the State Security Agency.

As regards the private sector, the researcher selected key private sector entities that are likely to be identified as CIIs, namely Vodacom, Microsoft, the Internet Service Providers Association of South Africa, the Banking Association Of South Africa, R2k, and the Association of Fraud Examiners (SA). They were selected to provide a spectrum of services falling within the broad category CIIs.

6.4 Validity and reliability

All the secondary data as accurately referenced, in accordance with the recommended referencing approach. Most of the secondary data was accessed by electronic means and referenced accordingly.

6.5 Research constraints

The impact of technology and the interconnection of cyber networks on national security is relatively new, particularly in respect of developing nations. As a result, the literature on this matter, dealing with challenges in the developing world in particular, is limited. Most scholars deal mainly with the strategies and approaches adopted by developed countries in Europe and the Americas, as well as some Asian countries. This limited focus does not provide a balanced picture.

The research report focuses on the implementation of a public policy, and does not deal with sensitive or classified information. All the information referred to is publicly available, and the government officials interviewed were discouraged from referring to information that is not in the public domain.

7 CHAPTER 4-DATA PRESENTATION

7.1 Introduction

The primary research focused on gathering information from senior policy, constitutional and cybersecurity experts in the South African government. The interviews were conducted soon after the government had approved the NCPF.

The officials selected for the interviews had all served on the government advisory team that helped to develop the NCPF. They were also members of the government's Cyber Response Committee, which is responsible for developing and implementing cybersecurity policies, strategies, technical capacity and structures and developing a skills base aimed at enabling South Africa to respond to the challenge of cyber threats. They were well placed to comment on government policy in respect of collaboration with the private sector. The officials provided detailed replies to the questions submitted to them, thereby allowing the researcher to assess the government's position on the matter under investigation. AT the time of the interviews, the officials were involved in developing overarching national legislation on combatting cyber threats and promoting cybersecurity in South Africa.

7.2 Primary data: interviews of government officials

7.2.1 Advocate Sarel Robbertse

Advocate Sarel Robbertse is a Senior State Law Advisor in the Department of Justice and Correctional services. He is also a member of the JCPS Cyber Response Committee (CRC), an interdepartmental body established by the NCPF. He is responsible for coordinating the drafting of the Cybersecurity and Cybercrime Bill, which seeks to combat cybercrime and provide for the identification and protection of CIIs. He agreed to be interviewed, but also asked to respond in writing to certain questions. I have therefore summarised their responses to the questions posed so as to give the context of their responses to this matter.

Question 1: Do we have policies, laws, regulations that promote public and private sector cooperation on the security of NCIIs?

In relation to this question, Adv. Robbertse stated that, according to him, Government policy on NCII protection seeks to prevent cyber-attacks against CIIs; reduce national vulnerabilities to cyber attacks; and minimise damage and recovery time when they do occur. He also stated that cooperation should include, amongst others, identifying problems and threats to NCII; alerting software and hardware vendors about security and the protection of their products; general awareness; research, fast and efficient reaction to all incidents related to the functioning of critical systems; international cooperation; and the creation of systems for formal and informal sharing of information about cyber threats.

His view is that chapter IX of the Electronic Communications and Transactions Act, 2002 (Act No 25 of 2002) makes provision for the identification and protection of critical databases (but not systems). However, no real co-operation is built into that chapter. The state identifies critical databases, and prescribes procedures and standards for compliance and enforcement. He also stated that the National Key Points Act (No 102 of 1980) deals with physical infrastructure, including information infrastructures. Again, according to him, the state identifies Key Points, and prescribes procedures and standards for compliance and enforcement. So no real regulatory measures exist that facilitate co-operation between the public and private sector.

In relation to existing regulations, he stated that various regulatory measures are in place in respect of financial institutions but such regulations do not provide any space for public-private co-operation, and the same applies to our electronic communications regulatory measures, which prescribe to electronic communications providers what they must or must not do without allowing for public private sector co-operation.

Hs view is that private-to-private or government-to-government agency co-operation is limited. The banking industry has a body which looks after cybersecurity in the industry, as an example of private-to-private cooperation. He also stated that it is important to take into account that there are various laws on the statute book which limit information-sharing between private entities.

These include the State Information Technology Agency Act, 1998 (Act 88 of 1998). In conclusion on this question, he stated that there is no real regulatory framework which would facilitate public-private participation relating to the protection of NCIIs. He further submitted that, even, the concept of NCIIs is meagrely defined in section 53 of the ECTA as a 'database' which is 'of importance for the protection of the national security of the Republic or the economic and social wellbeing of its citizens'. And that the ECTA will not be applicable to the broader categories of structures which make up NCIIs.

Question 2. What is the preferred model for achieving an appropriate balance between secrecy, transparency and accountability in respect of the security of critical systems?

Adv Robbertse advised that models of cooperation differ from one country to the other depending on the unique socio-economic realities and national security approach of such a Country. He made the reference to the ENISA survey which shows the various models adopted by countries within the Council of Europe that South Africa could learn from.

Question 3. What is the preferred model for the identification of NCII -- a sector approach, a government-private sector approach, a cross-sector approach, or a critical institutions approach?

In relation to a preferred approach or criteria for the identification of CIIs, he stated that identifying CIIs depends on the results of national risk assessments, the impact any disruption would have on a country. These assessments may be affected by different factors at different times. He further indicated that he agrees with the approach of the European Union Agency for Network and Information Security to identifying CIIs. His view is also that a sector approach without the involvement of government would mean that the object and scope of protection is determined in most instances by a specific sector, which may not take the needs of another sector into account and that a Government-private sector approach is to be preferred, as this approach was also adopted by the US and the EU. In conclusion on this matter, he submitted that he does not think that South African government has the necessary capacity or resources to deal with this aspect and

this was demonstrated by the failure to implement the provisions of chapter IX of the Electronic Communications and Transactions Act.

Question 4. Do you believe that the relevant ISO standards can assist in the promotion of greater cooperation between the government and the private sector in securing NCIIs, and to what extent?

His view is that it would be preferable for Government to implement the ISO standards as the basis for improved cooperation between Government and the private sector but he states that the implementation of these standards usually has cost implications for service providers. CIIs which are serious about cybersecurity will prefer a standard of compliance, and the ISO may serve this purpose, since it may act as a shield against civil liability.

7.2.2 Mr V Jaquire

Mr Jaquire is a manager in the State Security Agency responsible for National Information security Risk Assessment and Management Services. His role includes leading a team that is responsible for conducting risk assessments within organs of state in order to determine their level of security and vulnerability against unauthorised access. He advises that, before the repeal of the Electronic Communications Security (Pty) Ltd Act, risk assessments were conducted every two years. He stated that while his confirmed area of responsibility includes identifying CIIs within the organs of state not much has been achieved in this regard due to a lack of policy clarity or a framework for cooperation between government and the private sector. In relation to the questions posed, he provided the following summarised responses.

Question 1: Do we have policies, laws, regulations that promote public--private cooperation on NCIIs?

His view is that due to the fact that both government and the private sector are affected should NCIIs be compromised, the securing of NCII needs to be addressed by both the public and private sectors, in line with an appropriate implementation strategy, timelines and public private partnership strategy. He further stated that he is not aware of laws or

regulations that specifically address public private cooperation on NCII (except for some provisions in the POPI Act), some frameworks (such as the NCPF) do touch on the issue. He went on to state that there is a need for guidelines with regard to public-private partnerships, specifically to ensure that the most effective resources within the country are engaged to ensure the effective securing of the country's NCIIs.

Question 2: What is the preferred model for achieving an appropriate balance between secrecy, transparency and accountability in respect of the security of critical systems?

With regard to the security of critical systems, he stated that he preferred more confidentiality. He argued that the less cyber criminals know about the systems and processes that are utilised to secure critical infrastructure, the more difficult it would be for them to select the most appropriate attack methods and vectors. That the preferred model would ideally be for strategic partnerships to be created between government and the private sector, both for the sharing of skills as well as the development and/or supply of technologies: specifically for securing NCII and critical systems and that this should happen within the framework of approved government procurement regulation and processes that can be audited by independent (security cleared) auditors. This will allow for appropriate transparency, while still ensuring the confidentiality of the security measures that are implemented.

Question 3: What is the preferred model for identifying NCIIs – a sector approach, a government-private sector approach, a cross-sector approach, or a critical institutions approach?

His view is that the security of NCIIs is the responsibility of both government and the private sector but it is widely understood and accepted that most of the NCIIs lie within the private sector. He suggested a sector approach, driven and coordinated by government, in consultation and with the assistance of the private sector.

Question 4: Do you believe that the relevant ISO standards can assist in the promotion of greater cooperation between government and the private sector in securing NCIIs, and to what extent?

He stated that ISO standards provide a worldwide set of standards that could form a best practice basis on which the government and the private sector could base its cooperation, without conflicting agendas influencing the desired outcome, namely securing NCIIs for the benefit of the country and its people.

7.2.3 Mr J. Radebe

Mr Radebe is a Chief Director in the Department of Telecommunications and Postal Services, and is responsible for cybersecurity and CII policy. He advised that he had been involved in the development of the Electronic Communications and Transactions Act of 2002. He also advised that the Department of Telecommunications and Postal Services was responsible for implementing the ECT Act, specifically the provisions relating to the identification and protection of critical databases. He is also a member of the JCPS cluster CRC which is responsible for implementing the NCPF in the Republic.

Question 1: Do we have policies, laws, regulations that promote public--private sector cooperation on NCIIs?

He stated that the NCPF requires the development of a National Critical Information Infrastructure Policy for South Africa which will enable through regulatory means the adoption of appropriate mechanisms to identify and protect CIIs, develop minimum security standards, and facilitate effective public-private partnerships for protecting NCIIs. He accepts that a significant portion of CIIs are privately owned or operated and as a result a result, is a need for cooperation with the private sector in this regard?

Hr admitted that, prior to the adoption by Cabinet of the NCPF, there was less interaction with the private sector on this issue. The Department of Telecommunications and Postal Services has continuously engaged with the private sector on a range of policy matters since the 1994 transition to democracy.

Question 2: What is the preferred model for achieving an appropriate balance between secrecy, transparency and accountability in respect of the security of critical systems?

He stated that NCIIs are exposed to various vulnerabilities which have an impact on the efficiency of the provision of services as they are responsible for providing a range of critical services to the general public. In this regard, he proposed that products and systems used to secure NCIIs should be assessed and certified by outside certification companies to ensure that they are secure. That there is a need for an appropriate balance between secrecy, transparency and accountability and such may be achieved by different categorisation and security classification of NCIIs, coupled with access control informed by the security classifications in question.

Question 3: What is the preferred model for identifying and securing NCIIs?

He submits that there is a need for clear regulatory measures that will guide the identification of NCIIs. Such regulatory measures should set out criteria for identifying NCIIs, including the process of declaring NCIIs by the Minister. He further submitted that other jurisdictions use a sector-based approach in which a dedicated sector NCII identification team is appointed and assists the Minister in identifying the sector's NCIIs and necessary risk classification for protection purposes including identifying sector and cross sector inter-dependencies as well as proposing measures for the protection of NCIIs within that sector. In addition, he proposed that the Minister of State Security may impose conditions of compliance on the owners of declared NCIIs.

Question 4: Do you believe that the relevant ISO standards can help to promote greater cooperation between government and the private sector in securing NCIIs, and to what extent?

He advised that regulatory measures should recommend the adoption of the ISO standards on information security, which sets out criteria which must be taken into account to secure NCIIs. He also proposed that the CRC should make recommendations to the Minister regarding the adoption of information security standards, including relevant

information structures which needed in the process of the auditing of compliance of the declared National Critical Information Infrastructures to the adopted standards.

7.3 Private sector perspectives

The views of various key relevant private sector entities and civil society organisations were researched and recorded. This was done by studying their comments on the draft Cybersecurity and Cybercrimes Bill in 2015, and by interviewing relevant executives. The interviews were guided by the research questions. The executive were asked to share their views on the issues raised by the research questions. Some of the interviewees also submitted responses in writing.

Most of the private sector experts indicated that their opinions about the government's approach to the identification and protection of the CIIS were guided by their companies' responses to the Cybersecurity and Cybercrime Bill. These submissions were important as they conveyed the views of those companies on the role of public-private cooperation in securing CIIs. The results of this research is presented below.

7.3.1 The Internet Service Providers Association (ISPA)

ISPA agreed with the proposal for the security of the NCIIs as contained in the proposed law in view of the fact that the size and scope of some of the larger private electronic communications networks and service providers in South Africa and the fact that it is quite conceivable that sabotage of those providers would:

a) prejudice the security, the defence, law enforcement or international relations of the Republic;

b) prejudice the health or safety of the public;

c) cause interference with or disruption of, an essential service;

d) cause any major economic loss;

e) cause destabilization of the economy of the Republic; or

f) create a public emergency situation.

In this regard, ISPA submitted that, given the extent of requirements and obligations relevant to NCII in the Draft Cybersecurity Bill, it would be of extreme concern to its membership if the criteria for declaration and the related process was not clarified and simplified to make it easy for compliance by their members. ISPA furthermore advised that Government should avoid adopting a 'one-size-fits-all' approach in dealing with this matter. My view of the submission from ISPA is that they do not envisage a partnership arrangement with Government on this matter but see themselves having to comply with Government policy requirements. This approach from ISPA is consistent with the policy implementation process that has been followed by Government in South Africa. As indicated above, it is clear that this approach has not worked in the implementation of this current policy.

Source: ISPA public submission on Cybercrime and Cybersecurity Bill, 2015. Department of Justice and Constitutional Development.

7.3.2 Vodacom

Vodacom submitted that the draft Bill should prescribe guidelines to be followed by the Cyber Security Centre and the Cyber Response Team before recommending infrastructure as National Critical Information Infrastructure in terms of Section 58 (1). That these guidelines should consist of a number of elements, which include inter alia the identification and classification of threats, the identification of the vulnerability of each infrastructure, and the identification of counter measures to be considered prior to declaration of infrastructure as critical.

Further, Vodacom proposes that the DoJ and CD should clarify whether certain ECSPs will be exempted from the definition of National Critical Information Infrastructure. If this is the case, the Bill should prescribe beforehand the criteria that will be followed in exempting the ECSPs as such exemptions are likely to place the exempted operators at an advantage compared to Critical Information ECSPs.

Source: Vodacom public submission on Cybercrime and Cybersecurity Bill, 2015. Department of Justice and Constitutional Development.

4.3.3 The Banking Association of South Africa

The view of the Banking association in this regard is that the inclusion of the private sector within the overly broad definition of state-managed/controlled 'National Critical Information Infrastructure' process is cause for concern, as this would result in significant regulatory, bureaucratic and security overlap, control and potential systemic risk to the private sector, let alone significant and potentially unwarranted compliance costs. The submission therefore recommended that the private sector be removed from this section.

They further submitted that Financial Sector Regulation Bill contained sufficient provisions which would enable the private sector to secure their critical systems against natural or man-made disasters and they further rejected any attempt by Government to impose conditions on security of their own systems. They proposed that the NCIIs referred to in the Bill should be ones owned by government and not private sector infrastructure. It was stared that the imposition of such externally imposed audit costs on, and the reporting by, the private sector is rejected as an unwarranted bureaucratic imposition, and should be amended to apply to government infrastructures only.

Source: Public submission by the Banking Council of South Africa on the Cybercrime and Cybersecurity Bill, 2015. Department of Justice and Constitutional Development.

7.3.3 The Right To Know Campaign (R2K)

The R2K submitted that it believes that a free and open internet is crucial to the full realisation of our constitutionally enshrined right to freedom of expression, which includes, but is not limited to, the freedom to impart or receive information or ideas, freedom of the press, freedom of artistic creativity, academic freedom, and freedom of scientific research. That the internet has the potential to democratise knowledge in unprecedented ways. It was noted by R2K with concern Government attempts, through the Cybersecurity Bill, to introduce widespread state and corporate surveillance, new censorship mechanisms to regulate online content, often under the guise of security or 'moral' reasons. In this regard, R2K in its submission advised the general public to re-

main vigilant in defending internet rights and push back against reactionary legislation and policies that enable greater state and corporate control of the internet and also to reject the draft Cybercrimes and Cybersecurity Bill ('the Cybercrimes Bill') in its entirety. The need to combat genuine cybercrime is not contested. However, the Bill contains deep and fundamental flaws that threaten the fundamental democratic spirit of the internet.

According to R2K, the Bill creates a regime that is so broad and overarching that almost all possible crimes that could exist on the internet are dealt with using the same set of tools – from the risk of terrorist cyberattacks to the imagined crimes of an ordinary Facebook or BBM user. That the Bill hands wide-ranging powers to state-security structures to secure vast parts of the internet as assets of state-security, rather than common spaces for the good of all and that the Bill establishes State Security structures to monitor internet and that such structures lack the necessary transparency, accountability, mandate and organisational culture. R2K further submitted that National Critical Information Infrastructures should be confined to government owned infrastructures and therefore the authoritarian and dictatorial approach reflected in the draft Bill, which is the inclusion of the privately owned, infrastructures is simply not constitutionally acceptable. As indicated above, this submission is also another clear example of a lack of trust and cooperation between Government and private sector. This trust deficit indicates the failure of government to implement the 5C protocols in policy development and implementation.

Source: Public submission of the Right to Know Campaign on the draft Cybercrimes and Cybersecurity Bill, 2015. Department of Justice and Constitutional Development.

7.3.4 The Association of Fraud Examiners (AFE SA Chapter)

The AFE submitted that the section on the identification and the protection of the CIIs is the most concerning of all, especially as it relates to government intervention in the operating of a private or public company. That if a piece of infrastructure within this company is considered to be a National Critical Information Infrastructure, then the Cyber Response Committee directly takes control of the rules and regulations governing the

Policies, classification of Data, Access, Archiving, Security measures, Disaster recovery and the time allowed for the owning entity to comply with these regulations. If the owner fails to comply, the Cabinet may make those changes, and recover the costs. Once an infrastructure has been declared a National Critical Information infrastructure, it may not even be audited by anyone without approval of the Director General.

The submission suggest that no Private Sector Infrastructures should be able to be declared National Critical Information Infrastructures as this is tantamount to Nationalization of these infrastructures.

Source: Public submission of the Association of Fraud Examiners (SA Chapter) on the draft Cybercrimes and Cybersecurity Bill, 2015. Department of Justice and Constitutional Development.

7.3.5 Microsoft South Africa

Microsoft South Africa submitted that the Draft Bill already goes some way towards implementing this risk-focused and that the notion that minimum physical and technical security measures be implemented is endorsed in order to protect NCIIs. That achieving a security baseline will significantly reduce the risk to NCIIs including the adoption of well-known security approaches to help manage risk, such as the ISO/IEC 27000 related standards. Microsoft further recommended the use of international standards–based frameworks where possible and that Government should consider to give providers flexibility to decide how best to fully comply with security requirements. Strict mandates will not stand the test of time and are likely to chill investment in innovative new security measures, turning cybersecurity into an administrative box-ticking exercise. The submission also proposed that Government bring together stakeholders to standardize what constitutes acceptable security requirements and the sequence of events required by the assessor, delineating the range of deviation allowable from the baseline requirement's recommendations. That this approach is important when the criteria are set for the first time, however, it is also critical that the criteria be revisited regularly to incorporate any new technological solutions. It is noted that this is the only submission that appears to support Government intention to identify and secure NCIIs. It is important to

also note that the submission is silent on the public private sector cooperation but it calls for the discussions by stakeholders of a criteria for compliance. As indicated above, this points to a failure of government to promote the public-private cooperation on this matter.

Source: Public submission of Microsoft on the draft Cybercrimes and Cybersecurity Bill, 2015. Department of Justice and Constitutional Development.

8 CHAPTER 5-DATA ANALYSIS

The data has been ordered and analysed in order to develop responses to the research questions. Focus areas include:

- Public policy or laws that are creating a conducive framework for public-private cooperation in respect to CIIP.
- Level of cooperation, if any, in the implementation of these policies or laws.
- An assessment of the extent to which the 5-C protocol has been taken into account in formulating government cybersecurity policy, or would have been helpful.

8.1 International practice

The research shows that private sector and civil society pressure for the democratisation of nation states and governments has played a central role in the transformation of governance in a number of world regions, and that this has led to more democratic, transparent and accountable systems of policy development and implementation involving all stakeholders, including private sector stakeholders.

The research also shows that many countries – particularly those in the developed world -- have adopted policies and strategies which promote structured public-private cooperation, particularly in areas affected by global technological changes such as identifying and securing CIIs (Assaf, 2008). Experts agree that many essential services involve computer networks, that many of those systems are owned and operated by the private

sector, and that many of them are not secured against cyber-attack (Kyoung-Sik Min, 2015).

According to Muhaya (2010), CIIs are regularly penetrated by hackers and hostile agents. He argues that this calls for a partnership between government and the private sector so as to detect the attacks and prevent unauthorised access and theft of data. This view is supported by various experts in this field, including Suter (2007).

As noted earlier, the current approaches of European countries to identifying and protecting CIIs have been recorded in a survey, reflected in the ENISA report on methodologies for identifying CIIS published in 2014. It shows that most European countries have opted for structured public-private partnerships as opposed to a compliance approach imposed by the state. The research shows that the partnership approach has been effective in promoting cooperation between government and the private sector, based on trust and a joint commitment to achieving mutual objectives. By contrast, in the compliance approach, government assumes as 'big brother' role that alienates potential social partners. In this framework, the recommendation the ENISA report to member states and operators of CIIs are as follows:

- Member states should clearly identify CIIs, using one method or a mix of methods that best fit their needs.
- In doing so, member states should cooperate with all stakeholders involved in operating critical information infrastructures.
- Member states who base their identification of CIIs on critical services should develop a list of these services, and assess their internal and external interdependencies. This should include interdependencies within a critical sector (intra-sector); interdependencies between critical sectors (cross-sector); and interdependencies among data network assets.
- Following this, member states should foster baseline security measures.

Against this background, the report shows that most European countries have adopted national cyber security strategies and legislation aimed at fostering structured collaboration between the public and private sectors. These include:

- joint governance structures of institutions and instruments dealing with CIIs, including national cybersecurity centres, national computer security incident response teams CSIRTs), data protection inspectorates, and cyber cops responsible for preventing cyber incidents;
- Strategic plans for all economic sectors as well as cyber incident management plans drawn up by and involving all stakeholders. These include periodic risk assessments, operational plans for critical services, and protocols for reporting security incidents.

8.2 The South African policy and legal framework

The research shows that South African cybersecurity strategies are largely confined to government policies and laws without the involvement of the private sector.

8.2.1 Current legislation

The National Key Points Act (1980) empowers the Minister of Police to declare any place or area which he/she believes is so important that its loss, damage, disruption or immobilization may prejudice the Republic, or whenever he considers it necessary or expedient for the safety of the Republic or in the public interest, as a National Key Point. The Act requires the Minister to advise owners of these places or areas of their declaration of National Key Points, upon which they are required to secure them.

This law was made in the apartheid era to secure physical infrastructure, particularly those owned by the state or state entities. As a result, it has not featured prominently in the current debates on identifying and securing CIIs, and is due to be repealed by the Critical Infrastructure Protection Bill.

T**he Electronic Communications and Transactions Act (2002)** provides for certain classes of information that are important to the protection of the national security of the Republic or the economic and social well-being of its citizens to be declared as critical data, and the identification of critical databases. It empowers the Minister of Communications to prescribe procedures, requirements and standards for registering and managing critical databases.

This Act was passed in 2002 soon after the South African government had signed the Budapest Convention, and represented South Africa's first attempt to implement the Convention. While it criminalised cybercrime, and provided for the identification and protection of critical databases, it did not provide any implementation mechanisms. As a result, the South African Police Service has not been able to implement the provisions on cybercrime contained in the Act. No regulations have been developed to determine the 'classes of information' referred to in the Act, or identifying and securing critical databases, despite the fact this is required by the Act. Some of its provisions are meant to be repealed by the Cybercrimes and Cybersecurity Bill.

8.2.2 *New policy framework and proposed legislation*

Following the rapid escalation of cybercrime from the late 1990s onwards, the government went back to the drawing board and developed a National Cybersecurity Policy Framework (NCPF). Approved by Cabinet in 2012, and gazetted in 2015, it seeks to foster the development and implementation of a 'government-led, coherent and integrated' approach to cybersecurity.

Key objectives include centralising the coordination of cybersecurity activities, but also fostering cooperation and coordination between government, the private sector and civil society.

The policy framework would be overseen by the Justice, Crime Prevention and Security Cluster (JCPS), working in consultation with other government clusters, with the aim of ensuring the centralised coordination of cybersecurity issues.

Government and private sector cooperation on security of Critical information Infrastructures

A dedicated committee, the JCPS Cybersecurity Response Committee, would be established within the CPS Cluster to coordinate cybersecurity activities and drive the implementation of the NCPF. The committee would be chaired by the State Security Agency (SSA) and supported operationally by a Cybersecurity Centre situated in the SSA. All relevant JCPS departments would be represented on the committee.

Inter alia, it would oversee and guide the functioning of the Cybersecurity Centre, the Cybersecurity Hub, the government's Computer Security Incidence Response team (ECT-CSIRT), and any other CSIRTs in the country.

Coordination and consultation between the JCPS cluster departments, the private sector and civil society would be promoted by a Cybersecurity Hub to be established within the Department of Telecommunications and Postal Services (DOC).

Among other things, the hub would develop public-private partnerships; collaborate with other sector SSIRTs; provide best practice guidance to government, business and civil society; initiate cybersecurity awareness campaigns; promote compliance with standards, procedures and policy development by the CRC; and encourage and facilitate the development of additional sector SSIRTs

Following approval of the NCPF, the government began to develop the Cybercrimes and Cybersecurity Bill (2015). While tabled in Parliament, it has not been passed or promulgated. It is generally consistent with the Budapest Convention and the NCPF.

It empowers the Minister of State Security, upon receipt of a recommendation by the Cyber Response Committee and after consulting the owner of the CII in question, to declare an information infrastructure as a CII. It also empowers the Minister to prescribe minimum standards for classification, storage and disaster recovery. Owners are required to audit declare CIIs every 24 months, at their own cost. The Bill also empowers the Director-General of the SSA to order an audit of a CII. The Bill does not promote structured cooperation between the government and the private sector. Instead, it requires owners of information infrastructures and networks to comply with mandatory provisions relating to the identification and security of CIIs.

International experiences as shown that this approach is unlikely to produce positive results. Given the government's lack of capacity, it will also struggle to ensure compliance. A more collaborative approach is likely to produce better results, as this would create a win-win situation for both the government and the private sector.

Advocate Robbertse confirmed that there was no current legislation or regulations that facilitated public-private cooperation in identifying and protecting NCIIs.

Mr Jacquire also stated that, while the NCPF supported the principle of public-private cooperation on NCIIs, he was not aware of any laws or regulations (except for some provisions in the POPI Act) that applied this in practice. This principle should be applied more widely to ensure that national resources for identifying and securing NCIIs were used as effectively as possible. The preferred model would be to introduce strategic partnerships between the government and the private sector for sharing skills as well as developing and / or supplying technologies for securing NCIIs.

Mr Radebe concurred that the current regulatory framework did not incorporate public-private cooperation, but that the NCPF sought to provide for via in a different way. Given that a significant portion of CIIs were privately owned or operated, there was a need for cooperation with the private sector in this regard. Prior to the adoption by Cabinet of the NCPF, there was less interaction with the private sector on this issue. The views of senior government policy managers and major private sector entities differed on what form this should take, and how this should be achieved.

The submissions by key private sector entities which are likely to meet the criteria for the declaration as CIIs also reflect different and even opposing views.

Vodacom proposes that the government should prescribe guidelines to be followed by the Cyber Security Centre and Cyber Response Team before recommending infrastructure as CIIs. This approach seems to preferring compliance with laid down rules rather some form of partnership. As argued above, this approach has not succeeded in South Africa, partly due to the government's endemic lack of capacity to enforce laws and regulations.

The **Banking Council of SA** argues that inclusion of the private sector within the overly broad definition of state-managed/controlled CIIs is cause for concern, 'as this would result in significant regulatory, bureaucratic and security overlap, control and potential systemic risk to the private sector, let alone significant and potentially unwarranted compliance costs. It is therefore recommended that the private sector, per se, be removed from this section'.

R2K submits that legal provisions on CIIs contained in the draft legislation must be confined to government-owned infrastructure, and that the 'authoritarian and dictatorial approach reflected in the legislation is simply not constitutionally acceptable'.

According to **Microsoft**, 'the most effective way to improve cybersecurity is to give providers flexibility to decide how best to fully comply with security requirements. Strict mandates will not stand the test of time and are likely to chill investment in innovative new security measures, turning cybersecurity into an administrative box-ticking exercise. To allow for this the government should also bring together stakeholders to standardize what constitutes acceptable security requirements and the sequence of events required by the assessor, delineating the range of deviation allowable from the baseline requirement's recommendations.'

The **Association of Fraud Examiners** believes that no private sector infrastructures should declared as NCIIs, as this would amount to their nationalisation.

Therefore, it is clear that while the NCPF supports the principle of public-private cooperation as a mechanisms for identifying and securing CIIs, current legislation and draft legislation does not put this principle into practice. Moreover, the South African private sector appears to view any proposed cooperation with government as an unnecessary interference in its private affairs which, in its view, contravenes the South African Constitution.

9 CHAPTER 6- FINDINGS AND RECOMMENDATIONS

Experts agree that the need to secure CIIs present nation states with major new policy challenges. They also agree that structured public-private cooperation is one of the most effective ways of addressing those challenges, both nationally and internationally. Some areas of cooperation are outlined below.

9.1 International cooperation

Given the borderless and transnational nature of cybercrime, national states cannot focus only on securing their own CIIs. Instead, they need to collaborate with other countries, notably their trading partners.

The Council of Europe and European Union have taken important steps to promote international collaboration on this issue. This includes the Budapest Convention, which is managed by the Council of Europe but is open to signature by countries worldwide.

The Convention seeks to assist its signatories to develop legal and technical systems for dealing with cybersecurity within their national boundaries on the one hand, and cooperate with other member states on cybersecurity and cybercrime on the other. Among other things, the Council of Europe, with funding from the European Union, has embarked on a global initiative aimed at ensuring that member states have the necessary technical capacity to implement the Budapest Convention.

While the UN has undertaken some initiatives on cybersecurity through the UNDOC, it has not achieved much except for a global study that was finalised in 2013, and the Budapest Convention remains the only international instrument for promoting cybersecurity that is currently being implemented on a global scale. It has been argued that the UN should adopt another global convention on cybercrime on the grounds that the Budapest Convention is essentially a European convention. The Council of Europe disputes this view on the grounds that the Convention is not confined to European member states, has signatories on all continents, and therefore qualifies to be regarded as the required global instrument. While the AU has adopted its own convention on cybersecurity, it does not incorporate a detailed implementation process like that in the Budapest Convention.

9.1.1 National policies, laws and structures for dealing with cybersecurity

ENISA reports and other sources provide a rich source of information on how other jurisdictions have deal with cybersecurity. While South Africa should not necessarily adopt the same approach – and ENISA itself emphasises that countries should adapt their responses to their specific needs – the best practice models in Europe and elsewhere are instructive. Most European counties have adopted initiatives to deal with the issue of cybersecurity and identifying and securing CIIs.

Most of these countries have adopted national cybersecurity policies and strategies as well as legislation emanating from those policies, including laws dealing with emergencies as well as data recovery. These policies and legislation contain explicit provisions for identifying CIIs. All the countries sampled have developed methods for identifying critical sectors and subsectors as well as services that are vital to their socio-economic and national security. Most of these critical services and sectors are listed in their national cybersecurity strategies.

The policies and strategies of most European countries incorporate structured cooperation between their governments and private sectors, and the roles and responsibilities of public and private sector entities are clearly set out in relevant laws and regulations. There are relations of mutual trust between governments and the owners / operators of critical infrastructure. Most countries have national plans for protecting critical infrastructure that cover both the public and private sectors, and encompass all sectors of the economy. There are clear frameworks for cooperation between government and its agencies, such as ministries responsible for security; national cybersecurity centres; the owners or operators of CIIs; government and private sector CSIRTs; academia; and research and development institutions.

By contrast, there is a lack of clarity about South Africa's international cooperation on cybercrime and cybersecurity. South Africa signed the Budapest Convention in 2001, but has not yet ratified it despite the fact that it has participated in and benefited from the Council of Europe's GLACY project. South Africa has also signed the [SADC

Model Law on Cybersecurity. There is also no clarity about how South Africa intends to deal with the African Convention in the context of its participation in the Budapest Convention.

South Africa is also part of the BRICS grouping, which is known to be pushing for a UN Convention on Cybercrime and Cybersecurity. None of the other BRICS members are signatories to the Budapest Convention. This lack of clarity is likely to affect South Africa's international standing. Its unclear policy position and its simultaneous involvement in and support for different multilateral groupings and instruments may detract from levels of trust between South Africa and its African, European and CRICS partners.

At the national level, the Electronic Communications and Transactions Act (ECTA) of 2002 provided for the declaration of certain classes of information which are of importance to the protection of the national security of the Republic or the economic and social well-being of its citizens as critical data, and for identifying critical databases It also empowered the Minister to prescribe procedures, requirements and minimum standards for the registration and management of critical databases. None of these provisions have been implemented, and no regulations have been adopted to clarify the procedures for identifying and securing CIIs, or clarifying the roles of the owners of CIIs which are, in the main, private sector entities.

Instead of implementing ECTA, the South African government has adopted the NCPF which recognises that a significant proportion of South Africa critical infrastructures are owned or operated by the private sector, and expresses support for the principle of public-private cooperation in identifying and securing CIIs. However, no significant progress has been made in implementing the NCPF. The private sector players who are likely to be declared CIIs are opposed to the government being involved in declaring their systems as CIIs, which they regard as a contravention of the constitutional right to privacy. While the Cybercrime and Cybersecurity Bill was first tabled in parliament in 2015, it has been redrafted several times, and it is still unclear when it will pass into law.

Global information security is governed by a set of international standards adopted and amended by international bodies such as ISO (ISO/IEC 27000). Institutions that have adopted these standards generally require their trading partners to comply with these standards. The extent to which South African institutions involved in cybersecurity have adopted these standards, or intend to comply with them, is uncertain.

This report has argued that policy implementation should be well structured, and that the 5C protocol provides a useful model for structuring public policies such as policy on cybersecurity. It has also argued the South African should consistently adopt a model of public-private cooperation for managing cybersecurity, including the identification and securing of CIIs.

It has done so on the grounds that public-private cooperation is a form of participatory democracy in which those who are governed play a significant role in holding government accountable and improving access to information, but also bring their own skills and capacity to bear on public policy and its implementation. Noting that public-private cooperation in South Africa is complicated by the different and often divergent political interests of the various parties and stakeholders, the report has found that the government has been unable to implement legislation on cybersecurity passed in 2002 and that implementation of the more recent national cybersecurity policy framework appears to be faltering, largely due to the government's capacity challenges as well as its majoritarian approach to policy implementation.

9.2 RECOMMENDATIONS

Given the findings of this study, the author recommends that the South African government should consider the following public policy choices in respect of cybersecurity:

- Policy-makers need to clarify South Africa's position in relation to the Budapest Convention – specifically whether South Africa is prepared to ratify the Convention.
- Similarly, policy-makers need to clarify South Africa's position in respect of the African Union Convention on Cybersecurity. The Council of Europe is increasingly

focusing on assisting African countries to sign and observe the Budapest Convention. A growing number of African states are participating in the Budapest Convention process, some as observers, while others are in the process of ratifying the convention (TCY 2016).

- Similarly, policy-makers should decide on South Africa's stance on UN efforts to develop another international convention on cybercrime. In the course of doing so, they should compare the advantages of developing a new international convention with those of broadening the scope of the existing instruments to take account of issues being raised by non-members.

- Studies show that a lack of skills and capacity for technological development are the biggest impediments to the implementation of cybersecurity strategies in the developing world, and this deficit is making itself felt in South Africa as well. IT is closely linked to deficiencies in the South African education system and its relative inability to develop scarce skills. Notable initiatives in this area are being undertaken by the institutions such as the University of the Witwatersrand and the University of Johannesburg. The government should take advantage of the interest shown by these institutions in order to entrench a capacity-building culture in South Africa in this area. Structured cooperation between Government, private sector and academia will go a long way towards resolving some of the challenges identified in this report.

- Government should take note of the reservations of the private sector about aspects of its policy and legislative framework, and seek to reassure the private sector of its commitment to sound principles of governance. This process should include discussions about capacity-building partnerships as well as research and development. In this regard, the NCPF proposes various structures that should promote cooperation between government, private sector and the academia in this regard.

- All stakeholders should reaffirm their commitment to negotiating and agreeing on a sound and effective policy and legislative framework for meeting the urgent challenge of securing South Africa's CIIs, which are playing a vital role in providing essential services.

10 REFERENCES

Asaf, D. (2013). *Models of Critical Information Infrastructure protection*. University of Toronto, Faculty of Law, Toronto, Canada. Accessed online.

Berliner, D. and Erlich, A. (2015). Competing for transparency: political competition and institutional reform in Mexican states. *American Political Science Review*, 109(1), pp. 110–128. Retrieved from www.google.com/googlescholar

Brynard P. (2005). *Policy implementation: lessons for service delivery*. African Association for Public Administration and Management, School of Public Management and Administration, University of Pretoria, South Africa. Accessed online.

Chia, T. (2012, August). *Confidentiality, integrity, availability: three components of the CIA triad*. Retrieved from www.google.com/googlescholar

Clarke R. (1999, October). Threats to US National Security: proposed partnership towards preventing cyber terrorist attacks. Keynote address to the Terrorism and Business Conference dinner. Retrieved from http://www.heinonline.org

Corruption Watch. (2012, March 27). Submission to the NCOP Ad Hoc Committee on the Protection of State Information Bill [B6 – 2010]. Pretoria, South Africa. Accessed online.

Cosatu. (2012). Why we oppose the secrecy Bill. *Mail & Guardian*. http://www.m&g.co.za

Council of Europe. (2001, November). Convention on Cybercrime. Retrieved from www.coe.int/cybercrime

Council of Europe. (2014, October). Glacy Project CyberCrime@EAP: Draft reports on law enforcement training strategies. Retrieved from www.coe.int/cybercrime

Council of Europe. (2014, September). Glacy Project CyberCrime@EAP: Draft reports on judicial training strategies. Retrieved from www.coe.int/cybercrime

Council of Europe. (2014). Glacy Project: Guidelines for implementation of judicial training. Retrieved from www.coe.int/cybercrime;

Disterer, G. (2013). ISO/IEC 27000, 27001 and 27002 for Information Security Management. *Journal of Information Security*, 4, pp. 92-100. doi:10.4236/jis.2013.42011

Dunn-Cavelty, M. and Suter, M. (2009). *Public-private partnerships are no silver bullets: an expanded model for Critical Infrastructure Protection*. Centre for Security Studies, Zurich, Switzerland. Retrieved from www.scholar.google.com

European Union Agency for Network and Information Security (ENISA). (2014, December). *Methodologies for the identification of Critical Information Infrastructure assets and services: guidelines for charting electronic data communication networks*. Retrieved from www.enisa.europa.eu

Fenz S., Heurix J., Neubar T. & Pechstein F. (2014). Current challenges in information security risk management. *Information Management and Computer,* 22, p 410. Retrieved from www.google.com/googlescholar

Hassouna, M, Barri

, B. & Mohammed, N. (2013, November). An integrated public key infrastructure model based on certificateless cryptography. Retrieved from www.google.com/googlescholar

Helen Suzman Foundation. (2012, February). Submission to the National Council of Provinces on the Protection of State Information Bill (B6D, 2010). Retrieved from www.hsf.org.za

Kirtley, Jane E. (2006, June 8). Transparency and accountability in a time of terror: the Bush Administration's assault on freedom of information. University of Minnesota. http://dx.doi.org/10.1207/s15326926clp1104_2

Kyoung-Sik, M, Seung-Woan, C. and Mijeong, H. (2015). An international comparative study on cyber security strategy. Korea Internet & Security Agency. *International Journal of Security and Its Applications,* 9. http://dx.doi.org/10.14257/ijsia.2015.9.2.02

Mabelebele J (2012, February 17): The Protection of State Information Bill, universities and academic freedom. Higher Education of South Africa, Pretoria South Africa. Retriede from admin@hesa.org.za

Mattioli R, and Levy-Bencheton, C. (2014, December). Methodologies for identification of Critical Information Infrastructure assets & services: guidelines for charting electronic data communication networks. Retrieved from www.enisa.europa.eu

Mohammed, M. (2015). Cyber security standards compliance: a vital measure to Critical Infrastructure protection. Retrieved from kpmg.com/my

Mtshali, N. (2014, June 12). South Africa's policy on civilian participation in post conflict peace building: Burundi 2000-2008. University of the Witwatersrand library, Johannesburg, South Africa.

Muhaya, B. (2010). Dominant factors in national information security policies. King Saud University, Riyadh, Saudi Arabia. Trerieved from www.scholar.google.com

Ndlangisa, M. and Hebst, D. (2009). CII Protection: lessons for developing countries -- South Africa as a case study. Pretoria. Retrieved from Google scholar.

Nueman, W. L. (2006). *Social research methods: qualitative and quantitative approaches (seventh edition*). Boston, Massachusetts: Pearson Education.

Pasquale, A. (2011). Restoring transparency to automated authority. *Journal on Telecommunications and High Technology Law*, 9. Yale University. Retrieved form Google Scholar

Radu, R. (2013). Negotiating meanings for security in the cyberspace. info, 15 (6), pp. 32 – 41. http://dx.doi.org/10.1108/info-04-2013-0018

Right to Know Campaign, (2015, May 12). Right to Know condemns the return of the secrecy Bill. Pretoria, South Africa. Retrieved from http://www.r2k.org.za/

RSA. (1996). Constitution of the Republic of South Africa (Act no 108 of 1996). Pretoria, Government Press.

RSA. (1994). The National Strategic Intelligence Act (Act no 39 of 1994). Pretoria: Government Press.

RSA. (2002). The Electronic Communication and Transactions Act (Act no 25 of 2002). Pretoria: Government Press.

RSA. (2011). Protection of State Information Bill (B6D-2011). Pretoria; Government Press.

Shaw, T. (2004). Two Africas? Two Ugandas? An African 'democratic development state' or another 'failed state'? Working Paper no 125, Development Research Series, Research Centre on Development and International Relations, Aalborg University: Denmark.

State Security Agency. (2015, December 4). National Cybersecurity Policy Framework for South Africa. Pretoria, Government Press.

Susanto, H. (2011). Information Security Management System Standards: A comparative study of the Big Five. Retrieved from www.google.com/googlescholar

Suter, M. (2007, May 14). A Generic National Framework for Critical Information Infrastructure Protection. Centre for Security Studies, Zurich, Switzerland. Retrieved from www.scholar.google.com

Theoharidou, M., Panayotis, K., and Gritzalis, D. (2010, September). *A multi-layer criticality assessment based on interdependencies.* Retrieved from www.google.com/googlescholar

United Nations (UN). (2013, February). *Comprehensive study on cybercrime*. Retrieved from www.unodc.org/documents/organisedcrime

Von Solms, R., Van Niekerk, J. (2013, October). From information security to cybersecurity. www.google.com/googlescholar