



**A CYBERSECURITY GOVERNANCE FRAMEWORK FOR BROADBAND  
EXPANSION PROJECTS IN THE WESTERN CAPE**

by

**REBECCA DZIDZAI BURE**

**Thesis submitted in fulfilment of the requirements for the degree**

**Master of Technology: Information Technology**

**in the Faculty of Informatics and Design**

**at the Cape Peninsula University of Technology**

**Supervisor: Prof. Bennett Alexander**

**Co-Supervisor: Prof. Justine Olawande Daramola**

**District Six Campus**

**May 2022**

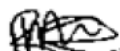
**CPUT Copyright information**

The dissertation may not be published either in part (in scholarly, scientific or technical journals), or as a whole (as a monograph), unless permission has been obtained from the University

## DECLARATION

I, Rebecca Dzidzai Bure, declare that the contents of this thesis represent my own unaided work, and that the thesis has not previously been submitted for academic examination towards any qualification. Furthermore, it represents my own opinions and not necessarily those of the Cape Peninsula University of Technology.

**Signature:**



**Date:** 3 November 2022

## **ABSTRACT**

In recent years, cybersecurity has emerged as a major concern for governments across the globe. Protection of computer systems, networks, information and software from cyberattacks and cybercrimes is the motivation behind the focus on cybersecurity. Cyberattacks and cybercrimes vary in complexity and nature, but usually are aimed at gaining access to sensitive information, modifying and potentially stealing it, leading to denial of access to and the destruction of network and system services in businesses, identity theft or personification and, in some cases, holding users to ransom.

There is a worldwide drive to bridge the digital divide and to grant universal Internet access to citizens. The global push for universal access to the Internet has seen a growing dependence on various digital services and the mushrooming of a wide range of social networks. Consequently, this has seen the growth of a new range of threats called cyberthreats and witnessed the birth of cybercrimes and cyberattacks, which threaten governments, public and private institutions as well as individuals in communities.

Having an effective and definite cybersecurity system is crucial and a necessity for every organisation. The aim of this study was to investigate cybersecurity governance in broadband expansion projects and to propose the development of a framework to administer cybersecurity in broadband expansion projects. This study includes a review of South Africa's current cybersecurity policies and legislation relating to this topic. A sociotechnical research approach that explores the relevant standards of cybersecurity administration and user awareness at broadband expansion projects is assumed.

The study employed the multiple case study strategy. Broadband expansion projects are a collective drive in South Africa, both in the private and public sector, with the goal of expanding broadband access to all citizens. For this reason, the multiple case study approach was employed as the researcher investigated both public and private broadband expansion projects. A qualitative model of enquiry was used. Data collection methods used in this research included semi-structured interviews, multiple case studies and a literature review.

The unit of analysis for the research was cybersecurity legislation in the selected broadband expansion projects. Selected personnel involved with cybersecurity on these broadband expansion projects of the selected cases were interviewed with their consent. The literature was surveyed and the data collected from various cases alluded to the fact that user engagement, awareness training and education are vital for cybersecurity. On the upside is the fact that legislation is already in place in South Africa, for example the Protection of Personal Information Act, the National Cybersecurity Policy Framework (NCPF) and the Cybercrimes Act 19 of 2020. However, all these are top level documents that do not provide reference for the broadband expansion projects.

This being the case, an operational framework that informs appropriate cybersecurity practices in broadband expansion projects is recommended in the conclusion to this study. The framework seeks to address cybersecurity practices by considering network data and information security; user awareness and engagement; policies; and legislation. The result of the framework, if implemented, would be a broad preventative, investigative and corrective approach when organisations deal with cybersecurity.

**Keywords:** Cybersecurity, engagement, awareness, training, legislation, cybercrimes, cyberattacks, cyber awareness, broadband expansion, governance, security, user empowerment.

## ACKNOWLEDGEMENTS

- I am immensely grateful to the Almighty for taking me this far. I would like to thank my husband and our children for their support throughout my studies. You have been patient and may the good Lord bless you.
- I would like to thank my father, Clifford, and mother, Molly, who have always been supportive and inspirational, pushing me to achieve greater things.
- I appreciate my siblings, Fadzai, Caroline, Rejoice and, posthumously, my dear brother, Simbarashe. You guys were a continuous source of inspiration to me in pursuing my studies.
- I appreciate Dr Dora Dubihlela for the continuous checking in and motivation.
- I would like to express my deepest thanks to my friends, Shingirirayi, Chengetai, Theresa and Phyllis to mention a few, for the moral support and motivation.
- I have had many people read this work, encouraging me to keep working and, at times, simply checking on my progress, the list is so long but I am entirely grateful for that support and encouragement.
- The four cases that I consulted and gathered data from, I am grateful. Without your information that you gladly shared this thesis could never had gone this far.
- I am immensely appreciative of Prof. Louise Leenen, the huge role that you played at the inception of this study was profound, your advice and motivation was always outstanding. I truly appreciate it.
- Finally, I would like to thank my supervisors: Prof. Bennett Alexander and Prof. Justine Olawande Daramola for the guidance, support, advice, encouragement and direction. Words will not be sufficient to express my gratitude. I am extremely grateful.

## **DEDICATION**

To my children, education will forever be an emancipation tool. It can take you anywhere. Strive for the best all the time. This is a dedication to you. Anything you set your mind to, you can achieve. The sky is always the limit!

## TABLE OF CONTENTS

<b>DECLARATION</b> .....	<b>ii</b>
<b>ABSTRACT</b> .....	<b>iii</b>
<b>ACKNOWLEDGEMENTS</b> .....	<b>v</b>
<b>DEDICATION</b> .....	<b>vi</b>
<b>LIST OF FIGURES</b> .....	<b>x</b>
<b>LIST OF TABLES</b> .....	<b>xi</b>
<b>CLARIFICATION OF BASIC TERMS AND CONCEPTS</b> .....	<b>xii</b>
<b>ABBREVIATIONS AND ACRONYMS</b> .....	<b>xiv</b>
<b>CHAPTER 1: INTRODUCTION</b> .....	<b>1</b>
1.1 Background to the study .....	1
1.2 Background to the research problem .....	4
1.3 Research problem .....	8
1.4 Research aim .....	8
1.5 Research question, sub-questions, and objectives .....	8
1.5.1 Research questions .....	8
1.5.2 Research objectives .....	9
1.6 Overview of research methodology.....	10
1.7 Ethical considerations.....	11
1.8 Delineation of the research.....	12
1.9 Significance of the research.....	13
1.10 Thesis structure .....	14
<b>2. CHAPTER 2: LITERATURE REVIEW</b> .....	<b>15</b>
2.1 Overview .....	15
2.2 Cybersecurity.....	15
2.3 Background to cybersecurity.....	16
2.4 Global context of cybersecurity.....	18
2.4.1 Cybersecurity in the African context.....	20
2.4.2 Cybersecurity in the South African context.....	22
2.5 Cyberthreats .....	27
2.5.1 Cyberthreats examples.....	27
2.5.2 Sources of cyberthreats.....	27
2.5.3 Forms of cyberthreats.....	28
2.5.4 The need for cybersecurity .....	30
2.5.5 Approaches to identify and address cyberthreats .....	30
2.6 Broadband expansion in South Africa.....	31
2.7 Cybersecurity awareness and user engagement .....	33
2.8 Cybersecurity policies and governance.....	37

2.8.1	The National Cybersecurity Policy Framework (NCPF) of South Africa.....	41
2.8.2	The South African Cybercrimes Act 19 of 2020 .....	43
2.8.3	Protection of Personal Information (PoPI) in South Africa .....	44
2.9	Security methods and practices used for cybersecurity .....	45
2.10	Conceptual framework.....	47
2.11	Broadband expansion in South Africa .....	48
2.12	Related work.....	51
2.12.1	Governance of cybersecurity in South Africa .....	51
2.12.2	Cybersecurity culture .....	52
2.13	Cybersecurity policies and legislation in South Africa.....	54
2.14	Cybersecurity awareness and user engagement.....	54
2.15	National Institute for Standards (NIST).....	54
2.16	Chapter summary .....	54
<b>3.</b>	<b>CHAPTER 3: RESEARCH METHODOLOGY .....</b>	<b>57</b>
3.1	Overview .....	57
3.2	Research paradigm .....	57
3.2.1	Research philosophy .....	57
3.2.2	Ontology.....	58
3.2.3	Epistemology.....	58
3.2.4	Axiology.....	58
3.3	Research methodology.....	59
3.4	Research approach .....	61
3.5	Units of analysis and sampling.....	61
3.6	Chapter summary .....	62
	<b>CHAPTER 4: CASE STUDY AND DATA COLLECTION .....</b>	<b>63</b>
4.1	Overview .....	63
4.2	Introduction to cases.....	63
4.2.1	Case 1 .....	63
4.2.2	Case 2.....	64
4.2.3	Case 3.....	64
4.2.4	Case 4.....	64
4.3	Data collection instruments.....	65
4.4	Content and discourse analysis .....	65
4.5	Literature review and sampling method .....	66
4.6	Use of semi-structured Interviews.....	66
4.7	Recruitment of participants .....	67
4.8	Interview protocol and process .....	67
4.9	Chapter summary .....	68



<b>1. CHAPTER 5: RESEARCH FINDINGS AND ANALYSIS</b> .....	<b>69</b>
5.1 Overview .....	69
5.2 Details of interview samples .....	69
5.3 Presentation and discussion of results.....	70
5.3.1 Adoption of policies and legislation in broadband projects .....	70
5.3.2 Cybersecurity governance in broadband expansion projects .....	72
5.3.3 Effect of broadband expansion on cybersecurity.....	75
5.3.4 Effective cybersecurity governance for broadband expansion projects .....	78
5.3.5 Lack of cybersecurity governance strategies .....	80
5.4 Summary of findings .....	82
5.5 Chapter summary .....	84
<b>6. CHAPTER 6: CONCLUSIONS, LIMITATIONS AND RECOMMENDATIONS</b> .....	<b>85</b>
6.1 Overview .....	85
6.2 Summary of chapters.....	85
6.3 Inferences of the study .....	86
6.4 Recommendation.....	87
6.4.1 Description of the operational framework.....	89
6.4.2 Network, data and information security .....	89
6.4.3 User awareness and engagement .....	90
6.4.4 Policies and legislation.....	91
6.5 Research limitations.....	92
6.6 Future research .....	92
6.7 Contributions of the research.....	93
6.8 Chapter summary .....	94
<b>REFERENCES</b> .....	<b>95</b>
<b>APPENDIX A: ETHICS APPROVAL</b> .....	<b>106</b>
<b>APPENDIX B: CONSENT LETTER</b> .....	<b>107</b>
<b>APPENDIX C: QUESTIONNAIRE</b> .....	<b>109</b>

## LIST OF FIGURES

<b>Figure 2.1: Increase in individuals using the Internet - Sub-Saharan Africa</b> .....	21
<b>Figure 2.2: Increase in sub-Saharan undersea cables</b> .....	23
<b>Figure 2.3: February–March 2020 phishing spike</b> .....	24
<b>Figure 2.4: Digital population South Africa 2020</b> .....	26
<b>Figure 2.5: Cybersecurity facets</b> .....	38
<b>Figure 2.6: Conceptual framework of the study</b> .....	48
<b>Figure 6.1: The Proposed Operational framework</b> .....	88

## LIST OF TABLES

Table 3.1: Research questions, objectives and methodology mapping.....	60
Table 5.1: Details of interview samples .....	69

## CLARIFICATION OF BASIC TERMS AND CONCEPTS

<b>Term</b>	<b>Definition</b>
Broadband	An ecosystem made up of high capacity, high speed and high-quality electronic networks, services, applications and content (Cardona, Schwarz, Yurtoglu & Zulehner, 2009).
Case study	An empirical investigation that analyses the factual context of a contemporary phenomenon in circumstances where there are no distinct precincts between phenomenon and context (Medlock, Wixon, Terrano, Romero & Fulton 2002).
Community	Group of people who reside in same geographic location and have about the same characteristics (MacQueen, McLellan, Metzger, Kegeles, Strauss, Scotti, Blanchard & Trotter, 2001).
Community broadband centres	Community broadband centres set up for citizens to gain access to the Internet.
Cyber thieves	Individuals who steal from others using a computer (Betts, 2018).
Cyberbullying	An act of harassing/harming another person, through the cyberspace using communication technologies (Betts, 2018).
Cybercrime	A delinquency that is related to the computer and or the cyberspace cyber aspect to it (Betts, 2018).
Cybersecurity	Tools, governance strategies, risk management plans, security guidelines, processes, technologies and practices that are designed to ensure protection of the cyberspace (Murthy, 2019).
Cyberthreats	Any possible danger that might exploit a vulnerability to breach security and, therefore, cause possible harm (Bidram, Poudel, Damodaran, Fierro & Guerrero, 2019) define cyberthreats in the context of computer security. Lamba (2020).
Governance	Method or system of government or management (Henriques, Pereira, Almeida & Da Silva, 2020).
Cyberspace	Environment that comprises of computing devices, applications, computer systems and networks, users, data and data traffic (Murthy, 2019).
Identity theft	A fraudulent act whereby an imposter acquires personal information about someone and impersonates them for various things (Ahmed, 2020).
Malware	Malicious software that includes Trojan horse, spyware, computer viruses and worms (Kalash, Rochan, Mohammed, Bruce, Wang & Iqbal, 2020).
Organisation and user assets	Computing devices connected on the network; infrastructure; data and information stored and transmitted within the cyberspace; and programs owned by either an organisation or users.

Phishing	Phishing is a practice whereby malicious content is sent via email as important delivery information, making recipients open the attachment containing malicious links that infect the victim's computer and, in the process, personal information is stolen (Chuprova, Gudkova & Marinets, 2019).
Ransomware	Ransomware is a type of malware that denies access to a computer system or data until a ransom is paid (Sharikov, 2020).
Spyware	Spyware is a form of malware that hides on a device, providing real-time information sharing with its host, enabling the host to steal data. such as bank details and passwords (Lamba, 2020).

## **ABBREVIATIONS AND ACRONYMS**

BYOD	Bring your own device
ICAN	Interactive Community Access Network
ICT	Information and Communications Technology
NCPF	National Cybersecurity Policy Framework
PoPI ACT	Protection of Personal Information Act 4 of 2013
RICA	Regulation of Interception of Communication and Provision of Communication-Related Information Amendment Act
TVET	Technical and Vocational Education Training
Wi-Fi	Wireless fidelity

## CHAPTER 1: INTRODUCTION

### 1.1 Background to the study

An increase in the importance of information and technology and the reliance on it by business and in people's everyday activities has become significant over the years. To that end, the complexity of the developed digital products does not align with end user readiness (Jones, Collins, Levordashka, Muir & Joinson, 2019; Sterlini, Massacci, Kadenko, Fiebig & Van Eeten, 2019). Nevertheless, it is prudent to note that digital data and operations are increasingly the nucleus of most modern organisations, and this trend is only increasing. Consequently, this reliance on computerisation has seen a spike in cyberthreats (Malm & Toyama, 2021).

Patel (2021) suggests that no matter where or why a cyberthreat originates, it has the potential to be catastrophic to individuals and even established companies. That being the case, it becomes of paramount importance to understand cybersecurity practices and tactics for effectively defending against hazards in the digital world.

With advancements in information technology (IT), there has been increasing dependence on the Internet and technology. The advancements in, and increased use of technology have broadened the surface area for cyberattacks, resulting in increased cybercrime (Thulin, 2015). Conversely, information and communications technologies bring forth tremendous socioeconomic advantages through Internet accessibility, even though they also pose serious cybercrime threats to society (Dickson & Bokhari, 2016).

Cybercriminals prey on businesses with masses of data, hoping that they can access this precious data (Seldon, 2016). The data usually targeted would include businesses' financial details; customers' financial details (for example credit card data); customer or staff email addresses and login credentials; customer databases; clients lists; IT infrastructure; IT services (for example the ability to accept online payments); and intellectual property (for example trade secrets or product designs). This data can then be used for financial gain either by demanding a ransom from the victim or by directly swindling funds from the company. Betts (2018) further suggests that cyberattacks could be motivated by the need to make a political point; for espionage, for example, spying on competitors to gain an unfair advantage and, in some cases, an intellectual advantage, for example, 'white hat' hacking. Undoubtedly, cybersecurity needs and its relevance is a global concern, and combating cyberattacks is receiving close attention

(Thulin, 2015). As the reliance on technology increases, countries are trying to come up with measures to counter cybersecurity threats. For example, in the United States of America (US), a country deemed to be steps ahead in terms of technological advancements, President Obama acknowledged that the US White House is targeted by hackers; the authorities, therefore, continuously work on improving their cybersecurity practices (Reuters, 2016).

Moreover, in England and Wales, close to six million fraud and cybercrimes are committed annually, with one in every ten people in these countries falling prey to either cyber-related fraud or cybercrime (Press Association, 2016). As a result, the government of England and Wales made commitments to spend as much as GBP1.9 bn on cybersecurity over a period of five years to curb cybercrime (Press Association, 2016). In the United Kingdom (UK) there have been over 2.5 million cases of cybercrime reported, most incidents of which were related to the computers of the victims, while the other cases were related to the Internet. There are many kinds of security solutions that could be employed for cybersecurity purposes and organisations could invest substantially in resources for cybersecurity, however, security breaches remain on the increase because of users' noncompliance with cybersecurity policies.

African countries are more prone to cybercrimes and South Africa is no exception. In relation to the whole of Africa, South Africa has so far been recorded to have suffered from the most cyberattacks (Fichardt, 2015). This results from vast broadband expansion; computer illiteracy that is high; and cybersecurity legislation that does not counter cybersecurity threats or address cybersecurity attacks (Jansen van Vuuren, Phahlamohlaka & Brazzoli, 2010). Cybersecurity governance strategies are needed to ensure protection of the cyber infrastructure and the cyberspace (South Africa. Department of Communications, 2020).

It is important to note that technological changes have been happening very fast and, although the intention has been good, gaping holes have been created in the IT infrastructure, resulting in the vulnerability of both the private and public sectors to cybercrime and cyberattacks (Fichardt, 2015). Furthermore, according to Fichardt (2015), personal information is easily gathered by hackers online or through websites where fake adverts appear, and that, when clicked on, the request for personal information or location of a user and other information can be easily used as a gateway



to personal data, eventually being used for ransom or as previously mentioned, to directly swindle funds from victims.

This being the case, the government of South Africa has put in place certain cybersecurity measures and legislation over the years to curb cybercrime. These include the regulation of Interception of Communication and Provision of Communication-Related Information Amendment Act of 2002, the Electronic Communications and Transactions Act of 2002, the Protection of Personal Information Act of 2013, the National Broadband Policy of 2013, the National Cybersecurity Policy Framework (NCPF) and Cybercrimes Act 19 of 2020. These policies and legislation seek to complement and enhance the objective of cybersecurity to ensure availability, integrity, authenticity, non-repudiation and confidentiality (Von Solms & Van Niekerk, 2013). Cybersecurity governance strategies include, amongst others, ways of seeking to reduce cyberthreats and risks; recovery policies and activities; as well as law enforcement in the cyberspace (Jansen van Vuuren, Grobler & Zaaiman, 2012).

Likewise, broadband expansion is a vision of the government to bridge the technology gap between communities that has seen some projects being undertaken in the Western Cape in pursuit of this cause (South African Government Gazette, 2010a). The aim of expanding broadband services in South Africa is to increase affordability, availability, accessibility and usage of broadband services countrywide.

The Interactive Community Access Network (ICAN) is an example of a broadband project in the Western Cape that aspire to expand broadband connection to disadvantaged communities by opening digital access centres in the Western Cape. The project's pilot centre was opened in Elsies River, namely the Elsies River Multi-Purpose Centre. This project is in line with the broadband initiative of the government of the Western Cape to provide Internet access, connecting communities within the Metro over a period of 3 years. This project has numerous socioeconomic benefits, including, but are not limited to, economic growth, employment creation, access to information and communication technologies (ICT) and broadband services that are secure, reliable and affordable (South African Government Gazette, 2013). Even though there are several projects that have been run by the Western Cape government, the researcher chose to do a case study of the ICAN project, bearing in mind the perception that broadband expansion in South Africa has made average citizens prone to cyberattacks (Grobler, Jansen van Vuuren & Zaaiman, 2011). Further

to that, with an increase in broadband access, so is there an increase in cyberattacks and threats, which is the reason why effective cybersecurity governance strategies must be implemented as a matter of urgency. As the government strives for community broadband expansion, it is crucial to pay attention to the risks that come with the growth in connectivity (Grobler, Jansen van Vuuren & Zaaïman, 2011).

## **1.2 Background to the research problem**

Chadwick, Costantino, de Lemos, Di Cerbo, Fan, Herwono, Manea, Mori, Sajjad and Wang (2020) define cyberthreats as the possibility of a malicious attempt to damage or disrupt a computer network or system. Keshk, Turnbull, Sitnikova, Vatsalan and Moustafa (2021) cite criminal gangs, nation-states, corporate spies, disgruntled insiders and individual hackers as some of the sources of cyberthreats. That being the case, it would be prudent for organisations to have mechanisms in place that will allow them to protect themselves from cyberthreats.

Cybersecurity is continuous and ongoing effort to ensure security in this Internet age that we are living in today. Cybersecurity is a broadly used term and its definition varies from source to source. The researcher consulted various sources to understand exactly what cybersecurity is and what it entails. It is clear that the definition of cybersecurity may appear to vary and be subjective, but sources consulted by the researcher seemingly agree that cybersecurity comprises of a collection of tools, governance strategies, risk management plans, security guidelines, processes, technologies and practices designed to support and protect the cyberspace, comprising networked systems, data and users at various levels, in personal, societal and national spheres, from malicious attacks, namely cybercrime, cyberattacks and, in some instances, cyberterrorism or, in short, any unauthorised use or prejudice (Murthy, 2019; Von Solms & Van Niekerk, 2013).

The working definition the researcher adopted for this study is that cybersecurity is a holistic collection of tools, governance strategies, risk management plans, security guidelines, processes, technologies and practices that are designed to ensure the protection of cyberspace. Cybersecurity is vital at all levels of society; from personal and corporate to state level, everyone should be cyber aware and take responsibility for their behaviour in cyberspace.

Betts (2018) classifies cybercrime as crimes that are committed by single actors or groups, targeting organisations' systems with the intended effect of financial gain or to cause disruption. Betts further describes cyberattacks as any type of offensive manoeuvre aimed at computer information systems, infrastructure, computer networks or personal computer devices. Mukherjee (2019) notes the increased reliance on computer systems, the Internet and wireless network standards, such as Bluetooth and Wi-Fi, as well as 'smart' devices, including cell phones, televisions and other such devices. The rapid increase in cyber technology has brought about major challenges in the contemporary world.

Cybercrime is on the increase globally (Sarre, Lau & Chang, 2018; Thulin, 2015). The increase in cybercrime demands the implementation of deliberate cybersecurity governance strategies to ensure the effective protection and control of the cyberspace and infrastructure (De Bruin & Von Solms, 2016). According to a research study conducted by Seldon (2016), people perceive that once someone has antivirus software, this software acts as sole protection, thus, they ignore cybercrime threats. Seldon (2016), however, opines that the use of antivirus software alone must never be deemed as giving full protection and immunity. Criminal activity has drastically increased in the cyberspace (SAPA, 2013). To effectively combat this threat, cybersecurity legislation and policies that are comprehensive, operative and effective have become a necessity. These pieces of legislation must, ultimately, be able to prevent, detect and, perhaps, correct cybersecurity concerns.

The South African NCPF was approved by Cabinet in 2012. However, critics like Jansen Van Vuuren, Leenen, Phahlamohlaka and Zaaiman (2013) argue that cybersecurity issues need a support system that would build a culture and awareness of the legislation, which they deemed not to be present. Further to this, Canetti and Shandler (2019) argue that monitoring tools and techniques are simply not present to support the implementation of the legislation. Seeing that cybersecurity was a new phenomenon at the time, the South African government proved that it was aware of the dangers of cybercrimes by taking the bold step of having discussions about cybersecurity (BDO, 2016). According to a SAPA (2013) report, it was alleged that 70% of the South African population had fallen victim to cybercrime, hence, it is of utmost importance for South Africa to implement and establish sound cybersecurity legislation and measures (SAPA, 2013).

South Africa Connect is a government project that aims to improve broadband in South Africa (South African Government, 2013). The vision of this project is to provide all South African citizens with access to broadband connection at a cost of 2.5% or less of the country's average monthly income (South Africa. Department of Communications, 2014). The South Africa Connect project has a deadline for the goal of 2030. However, Labuschagne, Ferentinou and Grobler (2020) note that due to cost, the first areas to receive fibre coverage were in the more affluent locations, where people could afford it. Nevertheless it is envisaged that, as it is rolled out further and more homes and businesses install it, fibre will become cheaper so that, eventually, even rural communities will be able to access fast internet via fibre optic cables. The absence of well implemented and effective cybersecurity governance strategies to support broadband expansion to increase internet usage could cause more harm than good to the community (Jansen van Vuuren, Grobler, Leenen & Phahlamohlaka, 2014).

In the case of the Western Cape, the broadband expansion is being propagated through the implementation of broadband expansion projects. The expansion is noticeably spreading. Academic institutions, mainly university and college campuses, are also at the forefront as they try to ensure that students have Internet access everywhere and all the times to improve effectiveness and efficiency when it comes to learning (South African Government Gazette, 2013).

With the South Africa Connect project, communities are being integrated into the global village. This goal is driven by government projects that intend to bridge the digital gap through the implementation of broadband expansion projects (Jansen van Vuuren, Grobler & Zaaiman, 2012). Broadband expansion is a drive to extend broadband to the less developed communities in South Africa (Jansen van Vuuren, Phahlamohlaka & Leenen, 2012). To achieve this, there are various projects that are underway, including the creation of community broadband centres, such as the Interactive Community Access Network (ICAN) Centre in Western Cape. This centre is a pilot broadband expansion project in Elsies River, created to ensure citizens within that community have access to broadband and Internet services. It is not just a community broadband centre but has evolved into an academic centre as well, where citizens in the Elsies River community can go and participate in various IT courses, including a Cisco cybersecurity course that empowers users with cyber education and makes them cyber aware. Academic institutions are also on a drive to expand broadband across their

campuses to improve users' effectiveness because, because of these projects, users will have internet access from anywhere on the institution's premises.

Many citizens who become Internet users through the implementation of such initiatives lack cybersecurity awareness because they are not appropriately trained to protect themselves against cybercrime threats (Jansen van Vuuren, Grobler & Zaaiman 2012). This exposes them and makes them vulnerable to cyberattacks and cybercrime (Jansen van Vuuren, Grobler & Zaaiman 2012). Generally, South Africa has become more exposed to cyberthreats since the increase in broadband availability in the country (Grobler, Jansen van Vuuren & Zaaiman, 2011). For example, the South African Police Service (SAPS, 2019) reported a more than 10% increase in organised crime in the form of people cloning cards and hacking payment systems. Another example came in October 2019, when the city of Johannesburg was hacked and the hacker demanded payment in Bitcoin. Information of clients in a metro with a population of more than 12 million was compromised (Moyo, 2019). All of this points to the need for strong cybersecurity governance.

The cybersecurity awareness levels of South Africans, together with cyberthreats, may potentially compromise national security. An increase in the cybersecurity awareness of citizens will reduce cyberattacks and prevent South African citizens from being used as digital soldiers in attacks against other countries (Jansen van Vuuren, Grobler & Zaaiman, 2012). Broadband expansion integrates technology into communities, bringing forth numerous benefits but, at the same time, this increase in connectivity and broadband access has increased the vulnerability to cyberattacks and cybercrime of governments, businesses and individuals (Van Heerden, Von Solms & Vorster, 2018).

Studies carried out by Jang-Jaccard and Nepal (2014), Williams (2019), and Wallace and Philip (2019) found that there is a direct relationship between the exponential growth in Internet interconnections and an increase in cyberattack incidents that could have disastrous and grievous consequences. Important to note is the fact that, with the broadband expansion initiatives booming everywhere, implementing effective cybersecurity strategies has become highly challenging as there are many devices that users have. In some cases, a single user will have multiple devices with which they access the Internet. With these advancements in technology, attackers have become more creative and innovative, devising many ways to attack users (Ahmed, 2020).

### **1.3 Research problem**

The legislation for cybersecurity in place in South Africa does not make direct and specific provision, nor does it provide a reference, for the cybersecurity governance in broadband expansion projects (Sutherland, 2017). While there is legislation in place in South Africa, such as the Protection of Personal Information Act of 2013 (PoPI Act); the National Cyber Security Policy Framework (NCPF) approved by the Cabinet in 2012 and gazetted in 2015; Cybercrimes Act 19 of 2020, critics suggest that this legislation has loopholes and, in some cases, neglects certain aspects that relate to cybersecurity.

Given this, it appears that a clear benchmark standard and a framework that applies directly to broadband expansion projects for cybersecurity governance are lacking. In view of the above, there is need for robust research that explores the important and relevant standards of cybersecurity governance and the promotion of user awareness in broadband expansion projects.

The lack of legislation or national policies on cybersecurity governance specifically tailored for the community centres, given the dangers and risk associated with cybercrimes, poses a security threat to the citizens who are getting connected to the Internet through the implementation of broadband expansion projects.

### **1.4 Research aim**

The aimed to investigate cybersecurity governance in broadband expansion projects in terms of practices, challenges, user awareness, and effectiveness.

### **1.5 Research question, sub-questions, and objectives**

To understand the problem of cybersecurity governance at broadband expansion projects, the following questions and objectives were posed.

#### **1.5.1 Research questions**

The main research question of this study is: What would constitute effective cybersecurity governance for broadband expansion projects in the Western Cape Province of South Africa?

The research sub-questions (RSQs) are:

- RSQ1:** What cybersecurity policies and legislation are being adopted and complied with in broadband expansion projects?
- RSQ2:** What cybersecurity governance is currently in practice in broadband expansion projects?
- RSQ3:** What are the cybersecurity challenges being faced by broadband expansion projects?
- RSQ4:** What constitutes effective cybersecurity governance for broadband expansion projects?
- RSQ5:** What are the results of a lack of cybersecurity governance strategies for broadband expansion projects?
- RSQ6:** How can cybersecurity awareness and training help alleviate occurrences of cyberattacks and cybercrimes?

### **1.5.2 Research objectives**

The study's research objectives (ROs) are:

- RO1:** To review and evaluate how cybersecurity legislation in South Africa is adopted and applied in broadband expansion projects.
- RO2:** To review and evaluate cybersecurity governance strategies currently in existence that support broadband expansion in broadband expansion projects.
- RO3:** To explore the salient dimensions (of a framework) for cybersecurity administration (governance) and user engagement (awareness) in broadband expansion projects.
- RO4:** To investigate the cybersecurity challenges being faced by broadband expansion projects.
- RO5:** To understand what more can be done on top of what is already being done to improve governance of cybersecurity in broadband expansion projects.
- RO6:** To understand the implications if no proper or effective governance of cybersecurity is implemented in broadband expansion projects.

**RO7:** To understand how cybersecurity awareness and training can help alleviate occurrences of cyberattacks and cybercrimes.

## **1.6 Overview of research methodology**

After considering that the research study involves aspects that deal with interactions between people and technology and also interactions between society's complex infrastructure and human behaviour, this study assumed a sociotechnical research approach that explored the relevant standards of cybersecurity administration and user awareness in broadband expansion projects.

For the purposes of this study the interpretivism philosophy was applied. The researcher intended to explore the salient dimensions (frameworks) of cybersecurity administration (governance) and user engagement (awareness) in broadband expansion projects.

Research design refers to a rational plan for acquiring answers to questions and to draw conclusions (Yin, 2003). According to Maree (2010), mention is often made of six types of qualitative research methodologies, namely conceptual studies, historical research, action research, case study research, ethnography and grounded theory.

The researcher employed the multiple case study strategy in this study. This method supports the exploration and reflection of multidimensional factors (Shoaib & Mujtaba, 2016:83-93). Broadband expansion is a collective drive in South Africa, both in the private and public environment, but with the same goal of expanding broadband access to all citizens. For this reason, the multiple case study approach was employed because the researcher investigated both the public and private broadband expansion projects.

In this research study, the research methodology used was qualitative model of enquiry. According to Hollstein (2011) qualitative research proposes to collect data, which is richly descriptive, concerning a precise phenomenon to gain an understanding of the case under observation. Qualitative research is non-numeric research, where the focus is not placed on the generation and analysis of numeric data, but rather on non-numeric data (Quinlan, Babin, Carr & Griffin, 2015).

For this research, the researcher used the inductive research approach. The inductive approach begins with the researcher making observations and, towards the end of the



research process, the researcher proposed theories resulting from the observations (Goddard & Melville, 2004).

## **1.7 Ethical considerations**

Ryen (2016) emphasises the need for research to follow clear and ethical principles and considerations. This research was undertaken after approval was granted by the relevant authorities, which included the Research Committee of the Cape Peninsula University of Technology. Various scholars such as Fontana and Frey (1994:372) warn investigators to take into consideration issues of 'informed consent', 'right to privacy' and 'protection' from harm. In that respect, before conducting this study the researcher first obtained ethical clearance from the Research Committee of the Cape Peninsula University of Technology.

### **i. Informed Consent**

According to Akintoye, Fothergill, Guerrero, Knight, Ulnicane, and Stahl, (2019) the purpose of science is to explore to acquire the truth. Miracle, (2016) alludes to the same fact arguing that, even though scientists have the right to go out in quest for truth, it should not be done at the cost of the rights of people. This study investigated the case of broadband expansion projects and empirical data was gathered from the four different cases indicated in the coming section. This data was collected mainly from personnel who were working on the broadband expansion projects. The researcher provided the research participants with a clear explanation of what was expected of them. Informed consent was obtained from the respondents by explaining to them the particulars of the research on an information sheet and on a consent form, asking them to sign the consent form if they agreed to participate in the study.

Participants were informed about the purpose of the study and their right to withdraw their participation at any stage of the research. Respondents were guaranteed that the researcher would ensure that anonymity, that confidentiality would be maintained throughout the research process and that information gathered would be used for the intended purpose only. This study was designed to cause no harm to the participants. All the participants participated voluntarily, with the full knowledge of their right to withdraw from participating in the study should they have decided that they no longer wanted to participate, or were no longer comfortable participating in the study. Voluntary participation was enhanced by informed consent. Informed consent ensured that participants had full knowledge of the circumstances they were agreeing to.

## **ii. Data Privacy**

Participants were informed that no information that would expose their identities was going to be shared and that pseudonyms would be used in the final report and in all published reports. The researcher ensured that the dignity of participants was not violated during the entire study. The local values and practices in the case study areas were always respected. The researcher only interviewed persons with permission from the relevant authority. Formal letters of consent received from the selected cases were signed off before the study commenced. Persons to be interviewed were not forced or coerced to do so, but they were sincerely asked and were interviewed willingly.

## **iii. Data protection**

The researcher made a commitment to anonymity of the participants of the study. The researcher also committed to report the findings of the research truthfully, without falsification or modification. A backup of all data collected was made so data was well protected and safeguarded from potential loss. The data collected during the study have been encrypted and protected for possible future reference if ever there was need for verifying research findings.

## **iv. Data storage**

Secure data storage is very important. The researcher committed to handle and store all research data safely and confidentially. The data that the researcher accumulated throughout the research included computer files securely saved in a reserved flash drive, paper documents; consent forms, printouts and case tracking sheets containing interviewees contact details. All the data was kept locked away in secure file cabinets when not being used and when it was actively used only the researcher and the supervisors had access to the data.

## **1.8 Delineation of the research**

This research study was limited to investigating cybersecurity governance in broadband expansion projects in the Western Cape Province of South Africa. The researcher analysed the issue of cybercrimes in broadband expansion and explored the salient dimensions of cybersecurity administration and user engagement in community broadband centres. For the purposes of this research, the researcher limited her focus on four different cases, namely Case 1, which is a community

broadband centre; Case 2, which is a Technical and Vocational Education Training (TVET) college; Case 3, which is a private tertiary institution; and Case 4, which is a public institution of higher learning. All the four cases had embarked on projects for expanding broadband access into their respective communities. These were the only facilities available for the researcher to conduct her study.

### **1.9 Significance of the research**

Worldwide, cybersecurity is currently a very important aspect of ICT. South Africa has yet to develop an effective cybersecurity governance framework that can be adopted by and utilised in community broadband centres. Currently the focus is to create a framework at national level only (Jansen van Vuuren et al., 2014). It is important to interrogate the relevant dimensions of cybersecurity administration and user engagement in broadband expansion projects, whilst divulging the shortfalls of current cybersecurity governance strategies, as purported in the literature studied, resulting from a lack of an effective and adequate cybersecurity governance.

The significance of this study is that after investigating cybersecurity governance in broadband expansion projects in terms of practices, challenges, user awareness, and their effectiveness the findings will shed light on the gap that exists in cybersecurity governance, indicating the need for cybersecurity governance strategies that apply directly to broadband expansion projects and, specifically, gives attention to user engagement, training, education and awareness. Broadband expansion projects could cause potential harm and be a security pitfall to the beneficiaries if there is no cybersecurity governance strategy in place to monitor the usage of resources, and to protect users and the infrastructure (Jansen van Vuuren et al., 2014).

## 1.10 Thesis structure

**Chapter 1:** The chapter served as the introduction to the research, giving a preview of the research, and presenting the problem statement, research objectives, research questions and the significance of the study.

**Chapter 2:** The chapter involves documenting a review of the literature applicable to this study and uncovering the relevant facts pertaining to cybersecurity governance in broadband expansion projects.

**Chapter 3:** This chapter provides in-depth details about the apt research design and research methods assumed for this study. A functionalist paradigm was assumed for this study and the researcher followed the multiple-case study route to gather empirical data for the study, employing a qualitative research strategy. To gather qualitative data, semi-structured interviews were conducted with chosen personnel from the case studies, where most of the questions used were open-ended.

**Chapter 4:** This chapter is a description of the multiple cases used in this study. It also includes the data collection methods, case by case.

**Chapter 5:** This chapter is the presentation, analysis, discussion and interpretation of findings in an attempt to address the objectives of the study and to derive answers to the research questions.

**Chapter 6:** This chapter is the concluding and summarising chapter of this study. The purpose of this chapter is to cite the limitations of the study, the study's contributions to the body of knowledge on the subject and recommendations for future research.

## **CHAPTER 2: LITERATURE REVIEW**

### **2.1 Overview**

This chapter provides an in-depth literature review and a discussion of literature relating to the study. Before undertaking this study, a review of the literature pertaining to the study was conducted with the purpose of understanding the theoretical underpinning of the research and the research area, and for identifying a research gap. This chapter is a discussion of pertinent concepts relating to the area of study. There are key tenets that the researcher identified, and will be focusing on, to ensure that the necessary body of knowledge is covered. These tenets are:

1. Cybersecurity
2. Community broadband projects in South Africa and the Western Cape
3. User engagement and awareness
4. Broadband expansion
5. National Cybersecurity Policy Framework (NCPF)
6. The Cybercrimes Act 19 of 2020
7. Protection of Personal Information Act (PoPI Act)
8. Security methods and practices used for cybersecurity

### **2.2 Cybersecurity**

Cybersecurity is a collection of tools and strategies used to govern; manage risk; and to develop processes, technologies, practices and guidelines for security, to support users and to protect the cyberspace (Craigen, Diakun-Thibault & Purse, 2014).

With most business systems transitioning to and incorporating information technology into their business operations, cybersecurity becomes a worldwide concern (Murthy, 2019). Despite the hype of businesses adopting information technology, there is limited public awareness of matters concerning cybercrime and cyberattacks, in other words, cybersecurity. People of all ages have embraced the use of the Internet and studies have shown that in South Africa active Internet users were 38.13 million as of January 2021, the use of Internet ranges from banking, shopping and studying to social interaction, to mention but a few (Statista, 2021). With the arrival of the coronavirus and resulting social distancing, business operations worldwide went online, creating a dependence on Internet services. Businesses are now faced with trusting the cyberspace for them to continue operations.

Undoubtedly, users are not aware of the imminent danger they face when using Internet and computer services. These include cyberthreats and cyberattacks. Cecil, Gupta, Pirela-Cruz and Ramanathan (2019) suggest the need for deliberate cyber training, readiness and awareness. The major reason for the lack of readiness and awareness regarding cybersecurity emanates from the absence of suitable cybersecurity policies governing cybersecurity at different levels (De Bruijn & Janssen, 2017).

### **2.3 Background to cybersecurity**

According to various authors, cybersecurity is a holistic collection of tools, governance strategies, risk management plans, security guidelines, processes, technologies and practices that are designed to ensure protection of the cyberspace (Craig et al., 2014; Von Solms & Van Niekerk, 2013). Cybersecurity is vital at all levels of society; from personal and corporate to state level, everyone should be cyber aware and be responsible for their behaviour in cyberspace. For the purposes of this study, cybersecurity is defined as a collection of tools, governance strategies, risk management plans, security guidelines, processes, technologies and practices designed to support and protect the cyberspace and users at different levels, namely in a personal, societal and national capacity.

Likewise, cybersecurity entails safeguarding of the users from cybercrimes, cyberattacks, cyberthreats, cyberbullying, cyberwarfare, cyberterrorism and cyberespionage intrusions, while maintaining confidentiality, availability and data and information integrity by detecting intrusions and incidents that do occur, and responding to and recovering from them. With such benefits, cybersecurity emerges as a global phenomenon as it involves interactions between people and technology and also interactions between society's complex infrastructure and human behaviour, which symbolises an emergent sociotechnical challenge for governments.

Cybersecurity is a sociotechnical challenge because it emerges from the interconnectivity of different communities of people and technology. Nevertheless, it is important to note that individual involvement and awareness plays a pivotal role in curbing the changes brought about by the advancement of information and technology. To date, cybersecurity is seen as a worldwide concern, posing new challenges to governments, but which still receives limited public awareness and user engagement.

Cybersecurity has not been fully comprehended by information and technology users and that there is very little awareness relating to it (Ahmed, 2020).

Furthermore, the Internet has become a significant part of people's lives and there is a reliance and a dependence on it for many things, such as sharing information, shopping, banking and more. Many perceive the Internet as a safe environment. Consequently, cybercrimes, cyberwars and cyberattacks are on the rise, calling for cyber readiness and cyber awareness to be proselytised in communities (Thomas, Vijayaraghavan & Emmanuel, 2020). The major reason for the lack of readiness and awareness regarding cybersecurity emanates from the absence of suitable cybersecurity policies governing cybersecurity at different levels (De Bruijn & Janssen, 2017).

More and more countries are seeing the need for implementing sound cybersecurity as it is a crucial issue that needs immediate attention, from community level to national level. Cybersecurity contributes to national security (Thulin, 2015; Sutherland, 2017). Inevitably and inherently, cybercrimes are becoming more and more complicated as more people harness information and technology, along with cybercriminals who always battle to find loopholes to crack. With these trends emerging, the cost to global economies is in the billions of dollars (Roškot, Wanasika & Kroupova, 2020) Huge cybercrimes are being planned and conducted, perpetuated by criminal networks made up of individuals from different companies, connected through the Internet. This shows how serious cybersecurity issues are. According to Ginni Rometty, chairperson, president and CEO of International Business Machines Corporation (IBM), in 2015, cybercrime was a big threat to every company in the world that had embraced information and technology in their business operations (Morgan, 2018).

In the context of South Africa, as a developing country experiencing rapid development in various ways, cyberthreats are increasing, and rapidly too, in information and communications technologies (ICTs) and broadband expansion, with a drive to increase user connectivity to the Internet countrywide (Meyer & Hamilton, 2020) More and more citizens are connected to the Internet along with broadband expansion. With the increase in broadband access and the spread of technology, new vulnerabilities have emerged in cyberspace. Advanced software and strategies to hack and crack systems are being developed by hackers and crackers to infiltrate systems and to access confidential information. New threats are being created for identity theft and to

commit computer fraud, just to mention a few. Abiodun, Anderson and Christoffels (2020) indicate that South Africa ranks third on the list of countries with the highest number of cybercrime victims.

## **2.4 Global context of cybersecurity**

Durodolu and Mojapelo (2020) note that there is a pursuit by governments all over the world to expand broadband throughout their countries to ensure universal Internet access and, thus, to bridge the digital divide. Consequently, Rubeis and Ketteler (2020) applaud the Internet, pointing to the fact that it bestows a huge variety of benefits upon all the people who use it, arguing that eventually Internet access should become a universal human right. In the same vein, the massive increase in Internet access has seen a reliance on the Internet for many things, including government services, commercial services and collaboration using social media, to mention a few. Consequently, this has resulted in a growing number and variety of cybercrimes and cyberattacks. The increased access to the Internet has resulted in an increase in cybercrimes, cyberattacks, theft of personal information and cyberbullying. With the increase, governments are challenged to coordinate cybersecurity at a national level, for municipalities and for independent agencies (Sutherland, 2017).

Cybersecurity is a growing concern worldwide (Sutherland, 2017). Cybersecurity governance strategies ensure the effective protection and control of the cyberspace and infrastructure. The cyberspace has become the biggest crime zone worldwide. With the threat of cybercrimes on the increase, cybersecurity legislation and policies that are comprehensive, operative and effective have become a necessity (SAPA, 2013).

The US Cybersecurity and Infrastructure Security Agency Act of 2018 encompasses strategies, standards and policies with regard to security and operations in the cyberspace. In addition to the already enacted legislation, a review team is also in place, comprised of government cybersecurity experts who are responsible for making and enhancing cybersecurity policy to make it more effective. Their policy review team argues that capacity building, supporting architecture, norms of behaviour and relevant government structures should be taken into consideration, bearing in mind that cybersecurity governance strategies ensure protection and control of the cyber environment and infrastructure (Dennehy, Meaney, Walsh, Sinnott, Cronin & Arensman, 2020; De Bruin & Von Solms, 2016).



To achieve cybersecurity, the entire nation's society needs to be involved in a comprehensive effort, with responsibilities clearly and efficiently distributed to prevent cyberattacks, as well as spreading awareness regarding cyberthreats (Masood & Shafqat, 2016). For instance, in the UK, a cybercrimes unit was established, leading to the creation of the Metropolitan Police's eCrime Unit, with police officers trained to handle cybercrimes. Some countries have put in place organisational structures that have been created to govern cybersecurity (De Bruijn & Janssen, 2017). Likewise, as in developed countries, Africa needs to be aware and have in place cybersecurity strategies that respond to cybersecurity threats (Dlamini, Taute & Radebe, 2011).

Cybersecurity governance is a division of information security governance that deals with the securing of electronic devices used in the cyber environment against various security risks and threats. The main objective of cybersecurity governance is to ensure the availability integrity, authenticity, non-repudiation and confidentiality of information (Von Solms & Van Niekerk, 2013). Cybersecurity governance strategies include, amongst others, seeking ways to reduce cyberthreats and risks, develop recovery policies and activities, as well as provide law enforcement in the cyberspace. To achieve cybersecurity, the government and the private sector must work hand in hand. Current cybersecurity governance seeks to ensure that the public understands cyberthreats and promote ways to increase public safety and security within the cyberspace (Jansen van Vuuren, Grobler & Zaaiman, 2012).

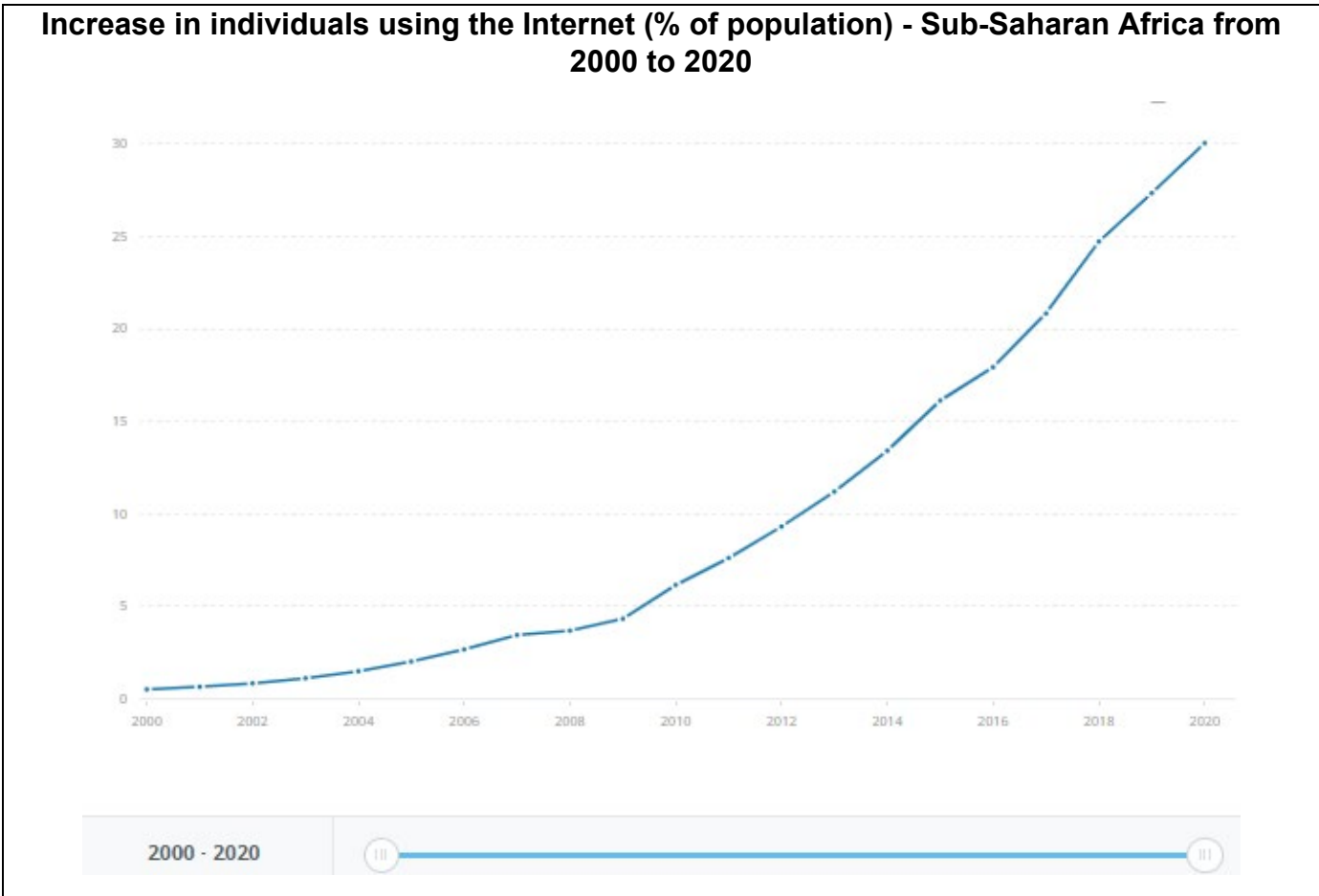
While countries battle with comprehending information and technology advancements, the Internet has become a vital tool used by criminal organisations to facilitate criminal activities worldwide and, because of the lack of awareness, unsophisticated users find themselves caught up in these crimes or being used as pawns after having their personal information stolen and wrongly used by these crime webs (Irshad & Soomro, 2018). In 2005, over seventy Chinese nationals were arrested in Kenya in relation to cybercrime, running a cybercrime ring operating with advanced technology to intercept short message service (SMS) messages, point of sale systems and mobile banking systems and to duplicate ATM cards (Jansen van Vuuren, Grobler & Zaaiman, 2012). This is a clear indication of the seriousness of the cybercrimes that are being committed.

### **2.4.1 Cybersecurity in the African context**

Broadband access is fast penetrating into many communities throughout most African countries through the introduction of wireless (Wi-Fi) and mobile networks that, in most cases, provide users with primary Internet access. According to a study conducted by the Kaspersky Lab, 40% of citizens in Africa access the Internet using their unprotected smart phones, providing opportunities for malware attacks. In most developing nations, much attention and effort are invested in increasing connectivity and community broadband expansion, but the risks and threats associated with such are not fully comprehended (Jansen van Vuuren, Grobler & Zaaiman, 2012). This has resulted in the skyrocketing of vulnerability to cybersecurity threats, malware infection and many other threats (Irshad & Soomro, 2018).

African countries are all regarded as developing countries, meaning they are not as advanced, technologically, and most of the population live below poverty datum lines of their respective countries. Cybersecurity awareness programmes need to be custom made to suit countries, noting how different developing countries are from developed countries. Nevertheless, the absence of a central organisation for cybersecurity in Africa makes most countries vulnerable to cyberattacks (Tikk & Kerttunen, 2020). Developing and underdeveloped African countries have limited awareness, knowledge, expertise and understanding of cybersecurity. Cybersecurity is a global issue and, like in the rest of the world, there is a need for African countries to be aware of cybersecurity and be ready for it. There is the need for initiatives to ensure best practice and cybersecurity awareness within the cyberspace (Dlamini et al., 2011).

Figure 2.1 illustrates the increase in individuals using the Internet (% of population) - Sub-Saharan Africa from 2000 to 2020. With the increase in Internet penetration into Africa more and more user have started using the Internet. However, with the increase in broadband access, so too are the cyberattacks and threats, hence the need for the implementation of effective cybersecurity governance strategies as a matter of urgency.



**Figure 2.1: Increase in individuals using the Internet - Sub-Saharan Africa  
Period from 2000 to 2020**  
 (Source: International Telecommunication Union (ITU) World  
 Telecommunication/ICT, no date,  
[https://data.worldbank.org/indicator/IT.NET.USER.ZS?end=2020&locations=ZG  
&start=2000&view=chart](https://data.worldbank.org/indicator/IT.NET.USER.ZS?end=2020&locations=ZG&start=2000&view=chart))

Based on Figure 2.1, there has been major increase in Internet usage in many developing countries of late who are mostly the Sub-Saharan African countries. Thomas et al. (2020) recorded a direct relationship between Internet usage and the number of cyber-related crimes and attacks in countries. Arguably, it can be taken as fact that these countries are becoming more vulnerable to cybersecurity threats. Broadband expansion has seen an outstanding growth in Internet interconnections and the formation of a great global village. However, in the process, this exponential growth of Internet interconnections has resulted in a massive increase of cyberattack incidents in communities that have both horrendous and serious consequences. It is highly urgent in the cybersecurity community that more innovative and effective cybersecurity governance strategies and mechanisms be adopted (Jang-Jaccard & Nepal, 2014).

#### **2.4.2 Cybersecurity in the South African context**

Cybersecurity is vital in everyday life in South Africa, just as it is anywhere else in the world. This is due to the prevalence of Internet-based attacks that will potentially keep increasing because of the increase in technology ubiquity. Cybersecurity includes the protection of information and systems from cyberthreats. When referring to cyberthreats, these include cyberattacks, cyberterrorism, cyberwarfare and cyberespionage. Cyberthreats vary in intention and damage that they can potentially cause, but the intentional causality is to bring harm to infrastructural assets, people or their nation. Cybersecurity is a critical part of any governments' security strategy (Sutherland, 2017). Cybersecurity is a critical contributor to national security in South Africa. Currently, South Africa has seen an increase in cyberattacks with a simultaneously increasing risk of such attacks in the business fraternity (Sutherland, 2017).

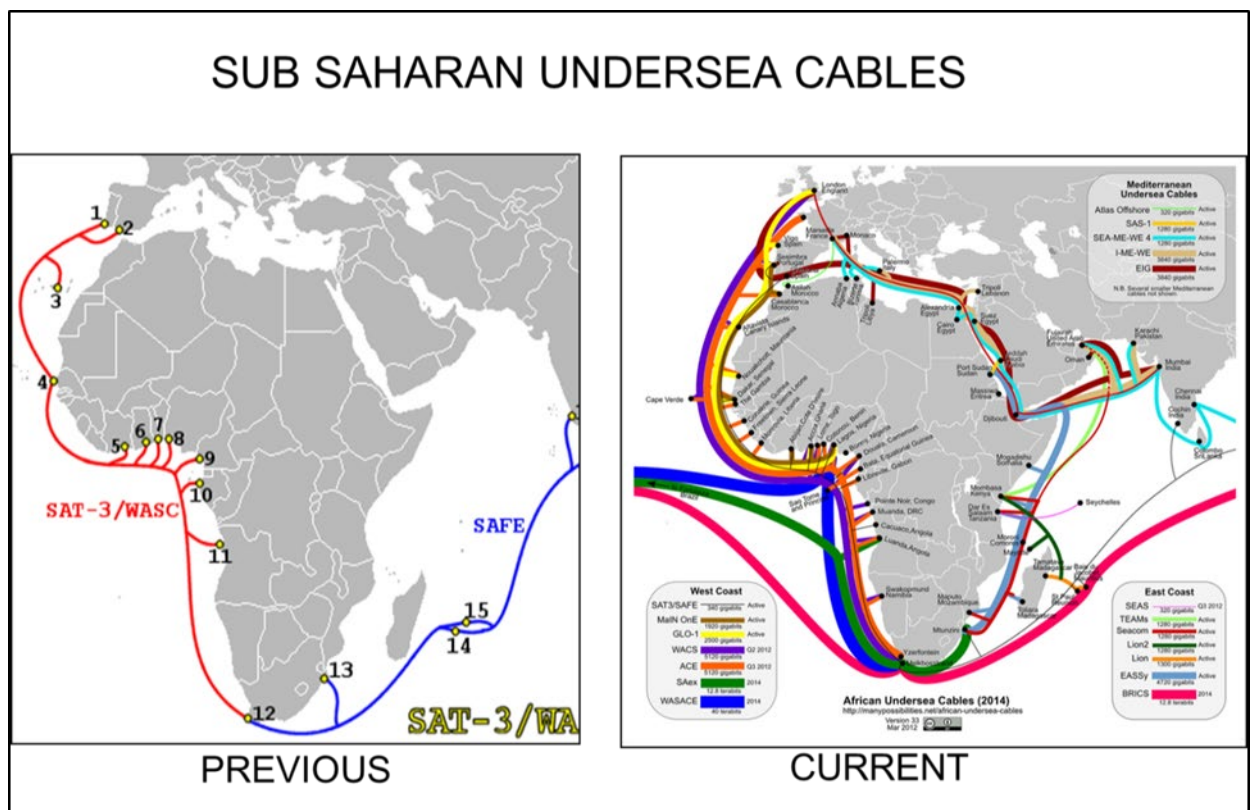
The rapid increase of and dependence on information technology for business operations and the direct relationship between the number of Internet users and cybercrime in South Africa, means that cybersecurity is a critical issue. Cyberattacks are continuously growing and neither the business fraternity nor the government are doing enough to combat it (Murthy 2019). The South Africa Department of Communications (2015) admits that more can be done to safeguard the cyberspace and protect the users, the infrastructure, organisations and the country, citing that, not only does cybercrime affect individuals and businesses, but it also affects the country's productivity and national security. South Africa had the third highest number of cybercrime victims worldwide in 2013, according to the Norton Report, after Russia and China. The level of cybercrime in South Africa is not quantifiable because of the absence of clear legal requirements as far as reporting cybercrimes is concerned. South Africa is one of the most targeted countries for cybercrimes in Africa (Sutherland, 2017).

Thomas et al. (2020) cites identity theft as one of the most prevalent ways that cyberthieves are operating in South Africa. This is done through credit card theft and fraud. If a person steals another person's personal information, by using that information they can create credit accounts and not pay those accounts, resulting in the individual whose information was stolen being blacklisted, with poor credit scores and financial charges that could cost them dearly Thomas et al. (2020) According to the 2014 Kaspersky Report, South African Internet users think that cybercriminals see

no value in their account credentials (MyBroadband, 2015). This misconception creates a relaxed attitude towards cybersecurity in users of information and technology. They do not really care about safeguarding their login credentials and other such ways of accessing and using the information technology, which they perceive as valueless, mistakenly thinking that no one would steal and use it, which is, regrettably, not true.

With the increase in broadband access, many socioeconomic advantages are created and will be created in the future. Moreover, with that increase in broadband access, cybercrime also increases as opportunities to exploit computers also increase (Doyle, 2015).

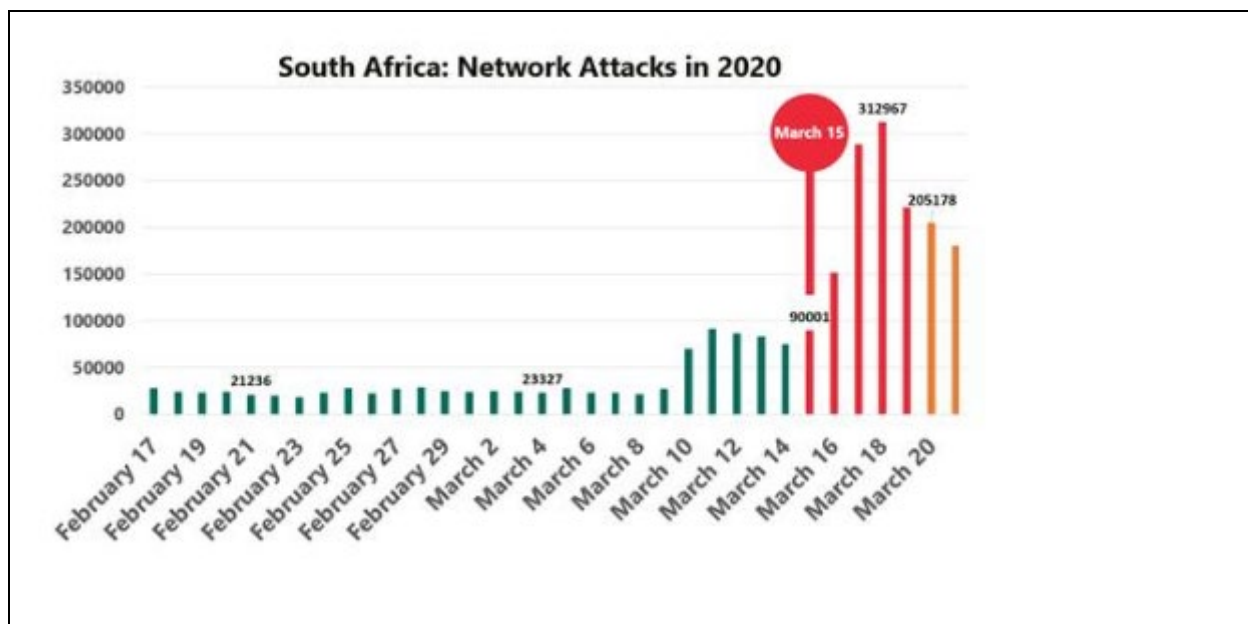
Figure 2.2 illustrates the rapid increase in undersea cables around Africa between 2008 and 2018. This enables greater use of information and technology and adds to the Internet usage.



**Figure 2.2: Increase in sub-Saharan undersea cables**  
**Comparison between 2008 and 2018**  
 (Source: Song, 2018)

Symantec (2019) posits that the inadequacy of security in IT systems and structures results in cybercrimes of a different nature. According to the Symantec's annual

Internet Security Threat Report, cybercriminals have engineered many ways to scam innocent, unsuspecting end users in the cyberspace by, for example, phishing, which is popularly used in Angola and Mozambique, resulting in consumers losing a great deal of money to criminals. Similarly, South Africa saw a spike in remote phishing scams inspired by the COVID-19 pandemic (Warburton & F5 Labs, 2020). The distribution of information relating to the pandemic has seen an increase in spam/scam emails being sent out to unsuspecting citizens, most of these emails were disguised as notices from the World Health Organization (WHO) and the Centre for Disease Control (CDC). With the second wave of the COVID-19 pandemic, new and novel phishing surfaced with cybercriminals trying new approaches to trick users into clicking through to malicious content. Also, security firm Kaspersky noted a similar rise in malware attacks during the early days of COVID-19. Kaspersky statistics show a sharp spike in network attacks in South Africa March 2020—with affected devices increasing in number from the 20 000—30 000 average to peak at approximately 310 000 over these few days. Figure 2.3 illustrates this.



**Figure 2.3: February–March 2020 phishing spike  
(Source: Techsmart, 2020)**

Phishing is a practice whereby malicious content is sent via email as important delivery information, making recipients open the attachment containing malicious links that infect the victim’s computer and, in the process, personal information is stolen (Chuprova, Gudkova & Marinets, 2019). The malicious emails targeted people from different countries and came in a variety of languages. Cybersecurity is undoubtedly an emergent concern for the South African government (Sutherland, 2017).

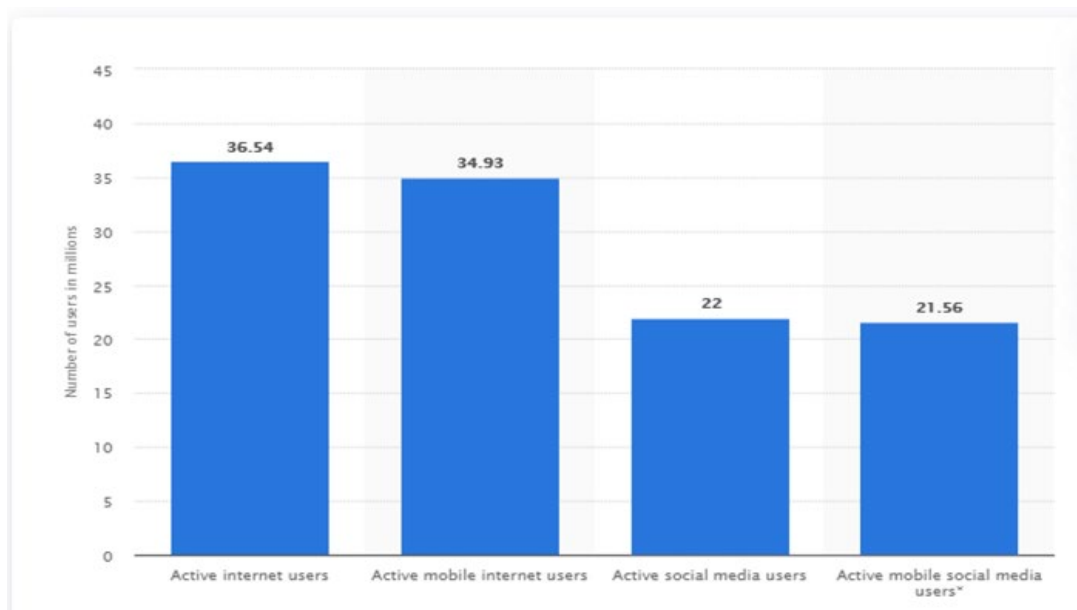
All of the above adds to the urgent need for the establishment of a legal platform in the fight against cybercrime, which is considered to be important and long overdue (Helyes, 2021). However, a legal platform alone will not be of much value. Public cybersecurity awareness campaigns are also necessary to educate the end users who are mostly preyed upon. Cybersecurity is a high priority for all nations. The absence of cybersecurity has detrimental effects on the nation. It affects the economy of the country and the safety of the country. The cyberspace is an interesting environment with so many advantages, but it poses a danger to vulnerable, innocent citizens who, unknowingly, fall prey to cybercriminals. The bulk of the South African population are exposed to cyberthreats because of a lack of exposure to and awareness of cybersecurity (Murthy, 2019). A correct and effective cybersecurity culture is an imperative need in South Africa.

A study done in Sri Lanka by Methmali (2016) found that 47% of people who participated in the study were not familiar with cybercrime news and 53% were not familiar with ICT news. Furthermore, Methmali (2016) found that those who use Internet cafés, in some cases, trust the café owner with their passwords or to do something on their behalf. This increases their exposure to cybercrimes. The results of Methmali's research correspond with the findings of Rubeis and Ketteler (2020), who suggest that there is a relationship between the causes of cybercrime and the and lack of awareness.

Although the government of South Africa is investing in training a few police officers to be competent in fighting cybercrime, a disturbing trend was noted by Kempen (2019), who found that 60% of police officials who become experts or specialists in cybercrime leave the service to join the private sector because this sector provides more security of tenure. In addition, the private sector allows cybercrime specialists to hone their skills and knowledge, as resources are readily available, unlike in the police service, where resources are scarce. Kempen (2019) recommended that responsibility of fighting cybercrime must, ultimately, be that of everyone who has access to the Internet, although nothing further to the recommendation was mentioned.

Figure 2.4 shows the digital population in South Africa, active Internet users, active mobile Internet users, active social media users and active social media on cell phone users. In Figure 2.4 34 million people (53 % of South Africa's population) access the Internet using their smart phones (Diwan, 2021). With the proliferation of mobile

Internet devices and numerous government programs aimed at expanding broadband access to communities, there are many new Internet users that have acquired broadband and Internet access without having been trained to protect themselves significantly and sufficiently in the cyberspace against cyberthreats and attacks. As a result, users are exposed and vulnerable to exploitation on the Internet (Kempen, 2019). Further to this Arensman, Cronin, Dennehy and Meaney (2020) allude to the fact that, if users are exposed to online exploitation, the national system is also compromised.



**Figure 2.4: Digital population South Africa 2020**  
(Source: Diwan, 2021)

The government of South Africa acknowledges that, as technology has simplified, life has become easier. ICT users have become reliant on ICTs for many activities, for example, communication, banking and more. This has left people exposed to cyberthreats and cyberattacks and they have been left vulnerable (South African Government Gazette, 2015).

Because the vulnerabilities growing in South African societies as a result of emerging threats of cybersecurity, there is a need for some concrete, integrated and practical approach to cybersecurity, thus ensuring the security of users in the cyberspace (Dlamini & Modise, 2013). There is a great need to secure the cyberspace as it benefits, enhances and innovates the economy and national security (Jansen van Vuuren, Phahlamohlaka, Leenen & Zaaiman, 2014).



## 2.5 Cyberthreats

Bidram, Poudel, Damodaran, Fierro and Guerrero (2019) define cyberthreats in the context of computer security as any possible danger that might exploit a vulnerability in order to breach security and, therefore, cause possible harm. Lamba (2020) further describes cyberthreats as malicious computerised acts that are intended to defile one's data, steal sensitive data or disrupt the digital life flow. These authors are in unison that cyberthreats are perpetuated, causing harm to an individual, systems or companies. The researcher agrees with these definitions. It is from this understanding that, for the purposes of this study, the researcher defines cyberthreats as malicious acts that can possibly cause harm that is characterised by, but not limited to, damage or theft of sensitive data, which can be harmful to a person or an organisation. Cyberthreat is a threat due to the use of cyber infrastructure.

### 2.5.1 Cyberthreats examples

Dwivedi, Vardhan & Tripathi (2020) provide examples illustrating that cyberthreats include computer viruses, data breaches, Denial of Service (DoS) attacks and other attack vectors. Betts (2018) adds that cyberthreats refer to the possibility of a successful cyberattack that aims to gain unauthorised access, damage, disrupt or steal an information technology asset, computer network, intellectual property or any other form of sensitive data. Cyberthreats may emanate from within an organisation by trusted users or from remote locations by unknown parties (Murthy, 2019).

### 2.5.2 Sources of cyberthreats

- i. **Hostile nation states:** Cyberthreats range from propaganda, website defacement, espionage, and disruption of key infrastructure to loss of life. Recent years have seen an increase in government-sponsored programmes that are evolving to become sophisticated, posing advanced threats, in comparison to other threat actors. There is an increased risk of long-term damage to the national security of many countries. Hostile nation states pose the greatest risk because of their ability to effectively employ technology and tools against the most difficult targets, such as classified networks and critical infrastructure, including electricity grids and gas control valves (Mozid & Yesmen, 2020).
- ii. **Terrorist groups:** Cyberattacks are becoming common, targeted at national interests. Lamba (2020) warns that terrorist groups will present substantial

cyberthreats as more technically competent generations join their ranks (Mozid & Yesmen, 2020).

- iii. **Corporate spies and organised crime organisations:** The objective would be to conduct industrial espionage to steal trade secrets or large-scale monetary theft. Perpetrators are driven by profit-based activities, either making a profit or disrupting a business competitors' ability to make a profit by attacking key infrastructure, stealing trade secrets, gaining access and blackmail (Mozid & Yesmen, 2020).
- iv. **Hactivists:** These are people who want their political ideals and issues to be heard. Most hacktivist groups are concerned with spreading propaganda rather than damaging infrastructure or disrupting services. Their goal is to support their political agenda rather than cause maximum damage to an organisation (Sharikov, 2020).
- v. **Disgruntled insiders:** Disgruntled insiders are a common source of cybercrime. Insiders often do not need a high level of computer knowledge to expose sensitive data because they may be authorised to access the data (Sharikov, 2020).
- vi. **Hackers:** Malicious intruders could take advantage of a zero-day exploit to gain unauthorised access to data. Hackers may break into information systems as a challenge or for bragging rights. In the past, this required a high level of skill (Bidram et al., 2019).
- vii. **Accidental actions of authorised users:** An authorised user may forget to correctly configure S3 security, causing a potential data leak. Some of the biggest data breaches have been caused by poor configuration rather than hackers or disgruntled insiders (Balakrishna & Soman, 2020).

### 2.5.3 Forms of cyberthreats

There are various forms of cyberthreats, and they are discussed in the section below:

- i. **Malware:** Software that commits malicious acts on a device or network, such as corrupting data or taking control of a system (Sharikov, 2020).
- ii. **Spyware:** Spyware is a form of malware that hides on a device, providing real-time information sharing with its host, enabling the host to steal data. such as bank details and passwords (Lamba, 2020).

- iii. **Phishing attacks:** Phishing occurs when a cybercriminal attempts to lure individuals into providing sensitive data, such as personally identifiable information (PII), banking and credit card details and passwords (Gudkova, Vergelis, Shcherbakova & Demidova, 2017).
- iv. **Distributed denial of service (DDoS) attacks:** DDoS attacks aim to disrupt a computer network by flooding the network with superfluous requests to overload the system and to prevent legitimate requests being fulfilled ((Lamba, 2020).
- v. **Ransomware:** Ransomware is a type of malware that denies access to a computer system or data until a ransom is paid (Sharikov, 2020).
- vi. **Zero-day exploits:** A zero-day exploit is a flaw in software, hardware or firmware that is unknown to the party or parties responsible for patching the flaw (Betts, 2018).
- vii. **Advanced persistent threats:** An advanced persistent threat occurs when an unauthorised user gains access to a system or network and remains there without being detected for an extended period (Betts, 2018).
- viii. **Trojans:** A Trojan creates a backdoor into a system, allowing the attacker to gain control of a computer or access to confidential information (Lamba, 2020).
- ix. **Wiper attacks:** A wiper attack is a form of malware whose intention is to wipe the hard drive of the computer it infects (Lamba, 2020).
- x. **Intellectual property theft:** Intellectual property theft is stealing or using someone else's intellectual property without permission (Lamba, 2020).
- xi. **Data manipulation:** Data manipulation is a form of cyberattack that does not steal data but aims to change the data to make it harder for an organisation to operate (Lamba, 2020).
- xii. **Data destruction:** Data destruction occurs when a cyberattacker attempts to delete data without authorization (Lamba, 2020).
- xiii. **Man-in-the-middle (MITM) attack:** An MITM attack occurs when an attack relays and, possibly, alters the communication between two parties who believe they are communicating with each other (Lamba, 2020).
- xiv. **Drive-by downloads:** A drive-by download attack is a download that happens without a person's knowledge, often installing a computer virus, spyware or malware (Lamba, 2020).

- xv. **Malvertising:** Malvertising is the use of online advertising to spread malware (Lamba, 2020).
- xvi. **Rogue software:** Rogue software is malware that is disguised as real software (Lamba, 2020).
- xvii. **Unpatched software:** Unpatched software is software that has a known security weakness that has been fixed in a later release but has not yet been updated (Murthy, 2019)

#### **2.5.4 The need for cybersecurity**

There is increased risk that organisations' do not have direct control of information technology (IT) security teams. The trend has increased because of global connectivity and the usage and reliance of cloud services, and is exacerbated by outsourcing by companies, resulting in a much larger attack vector than in the past, when systems were not IT dependent. Shin and Lowry (2020) noted that third and fourth parties are increasing as information and technology dependence and use increases. This leads to third-party risk management, vendor risk management and cybersecurity risk management being of greater importance in reducing the risk of third-party data breaches. Reducing third-party risk can potentially help managers who make decisions by making sure that their clients do not fall victim to cyberthieves.

#### **2.5.5 Approaches to identify and address cyberthreats**

Dwivedi et al. (2020) suggest the following approaches:

- i. **Strategic assessments:** This level of assessment aims to inform decision-makers about broad and long-term issues and, in so doing, provide timely warning of threats. Strategic cyberthreat intelligence imagines and predicts the intent and the capabilities of malicious cyberattackers and what cyberthreats they could pose.
- ii. **Operational assessments:** This level of assessment targets incidents related to events, investigations or activities. It provides guidance on how to respond to them, for example, by identifying which steps should be taken by an employee when a computer is infected with malware.
- iii. **Tactical assessments:** This level of assessment involves real-time assessment of events, investigations and activities that provide day-to-day support.

## **2.6 Broadband expansion in South Africa**

Williams (2019) posits that Internet access has become a universal basic human right, not a mere luxury enjoyed by a few people. It has become the goal of most governments to provide broadband access to ensure universal access to the Internet. Through the South African Connect project, the government aims to expand broadband access to all communities in South Africa, including rural areas (Wallace & Philip, 2019).

According to Williams (2019), broadband expansion is an initiative undertaken to expand broadband to bridge the digital divide in South Africa. This is a national drive in the country that aims to integrate all communities, urban and rural, into the global village in South Africa through the implementation of broadband expansion projects. Wallace and Philip (2019) attest to the fact that various projects have been rolled out because of the South Africa Connect project's vision. The researcher will refer to such projects as broadband expansion projects.

The government has implemented programmes to provide citizens in specific communities with broadband access and affordable Internet access that can meet the needs of the society and both private and public users (Strover, Whitacre, Rhinesmith & Schrubbe, 2020). Iqbal and Anwar (2020) allude to the fact that there has been an increase in corporate donations of hardware and software, as well as an increase in the number of mobile Internet devices, which has resulted in more and more citizens acquiring broadband access. Moreover, the digital world brings forth many advantages. However, the same digital facilities that have revolutionised lives also leaves a window of opportunity open for an increase in cybercrime and cyberattacks.

The National Broadband Policy (South Africa. Department of Telecommunications and Postal Services, 2013) outlines objectives to ensure broadband services and access that are secure, reliable, and affordable to all South African citizens, especially in underdeveloped and rural communities. Furthermore, the National Broadband Policy aimed to enable the development of highly skilled persons and to put policies and regulations in place to enable public and private sector investment to attain South Africa's broadband ambition of enabling more people to connect to the Internet and to increase the Internet speed when connected (South Africa. Department of Communications, 2020). The target was to ensure 99% broadband connectivity by the year 2020 (South African Government Gazette, 2013). To ensure that this goal could

be realised, the government of South Africa rolled out free Wi-Fi access in cities around the country and launched community broadband expansion projects (Massey, 2020).

The South Africa Connect project aims to improve broadband in South Africa. Its vision is to provide all South African citizens with access to broadband connection at a cost of 2.5% or less of the average monthly income (South Africa. Department of Communications, 2014). All these efforts are aimed at the provision of a better living standard and better service delivery for the citizens. There is, however, no simultaneous effort at the same rate to combat the cyberthreats that Shin and Lowry (2020) and Balakrishna and Soman (2020) all found and that there is a direct correlation between increased usage, dependence on information and technology and the number of cybercrimes.

Among the numerous benefits that are realised from this project include an increase in employment opportunities, the reduction of the cost of communication, stimulation of growth of local businesses and an improved quality of education, to mention but a few (South African Government Gazette, 2013). Broadband expansion implemented by the South African Connect project will build resources, ability, vigour and competencies of the entire community towards achieving a connected society (South African Government, 2013). This is thus, the future and it is rolling out and cannot be stopped as more and more business will operate with greater dependence on information technology (Jones et al., 2019).

Even so, Williams (2019) notes that, as the government strives for community broadband expansion in the Western Cape Province, it is crucial to pay attention to the risks that come with the growth in connectivity. The absence, however, of appropriate, well implemented and effective cybersecurity governance strategies to support broadband expansion could cause more harm to the community than good (Jansen van Vuuren, Phahlamohlaka, Leenen & Zaaiman, 2014).

The intention of the community broadband expansion is to bridge the technology gap. Several projects have been rolled out in the Western Cape towards realising this cause (South African Government Gazette, 2019). The digital divide in South Africa is largely because of the issue of poverty and underdevelopment in the impoverished and rural communities. It is in these underdeveloped communities where the poor people are found. By poor, the researcher means people who live below the poverty datum line,

comprising 55,5% of the total population of South Africa (Stats SA, 2018). To these communities, increased broadband means better connections, hence people and businesses will see no need migrate to bigger cities to live and work in search of economic opportunities. By reducing migration, local economies are stimulated by newcomers who, instead, move into these areas, reversing this migration trend.

Secondly, cell phone coverage in rural areas can be patchy due to the cost of installing towers and masts across the sparsely populated countryside. Thirdly, students can access college or high school courses over the Internet, alleviating disruption caused by flooding and pandemics like COVID-19, which has seen schools appreciating online learning more than ever. Fourthly, traditional rural businesses, such as farmers, also benefit. They can access the latest commodity prices and decide when and where to send their crops or livestock to realise the best price. Finally, tourism also benefits as visitors increasingly expect to be able to instantly post photos and videos of unspoilt national parks on social media from their tablets, smartphones and computers (Wallace & Philip, 2019).

Poy and Schüller (2020) commend the rolling out of broadband as they find that a large proportion of South African citizens have already managed to gain Internet access using traditional desktop computers, laptops, tablets and the mobile Internet devices that have flooded the market at very affordable prices.

## **2.7 Cybersecurity awareness and user engagement**

Awareness is the interrelationship between the following elements: consciousness; knowledge; behaviour and attitude realisation; cognisance; attitude realisation; self-perception; understanding and skills (Chandarman 2016). Cybersecurity awareness training is security training used to establish and build cybersecurity knowledge and skills among systems users that informs users of cyberthreats and susceptibilities in the environment they are in, as well as how to deal with the threats and vulnerabilities (Mashiane, Dlamini & Mahlangu, 2019).

In this study, cybersecurity awareness is defined as having consciousness, knowledge, being informed about cyberthreats and vulnerabilities in one's environment and knowing how to deal with them. Cybersecurity awareness training can be used to spread this awareness and is vital for empowering users, as well as equipping them

with the knowledge and skills necessary for them to be able to protect themselves from cyberattacks and defend themselves in the event of a cyberattack.

Cybersecurity awareness is important for users to empower themselves to prevent them from becoming victims of cybercrimes, cyberattacks and cyberthreats. Additionally, cybersecurity awareness and user engagement ensure that users or citizens are aware of the vulnerabilities they are prone to and the imminent danger they could potentially find themselves in when using digital resources and the Internet, which are the elements that make up the cyberspace.

Consequently, it is important to have correct user training, awareness and attitudes as an essential contribution to knowledge about cybersecurity in a cybersecurity drive. The ordinary end user is the easiest target for cybercriminals because they are mostly naïve as far as cybersecurity is concerned. It is crucial for the user be educated and to be made aware of the ruthless cybercrimes and how to effectively protect their personal information and data in the cyberspace. User awareness and involvement or engagement is very important for any security programme to be successful, which also applies to cybersecurity (Cecil et al., 2019).

Since 2009, with the increase in the number of undersea cables around the African continent, there has been an increase in broadband access throughout South Africa and many citizens have since gained Internet access. Therefore, a large proportion of the population of South Africans who previously did not have regular and continuous Internet access and exposure to ICTs became vulnerable to cyberattacks, cybercrimes and cyberthreats (Grobler, Jansen van Vuuren & Zaaiman, 2011). Because of this, it is crucial that cybersecurity awareness is increased among citizens to empower them and to prevent them from becoming victims of cybercrimes.

Jones et al. (2019) note that due to ICT advancements, daily activities of ordinary citizens have been changed and simplified. That said, there has been a reliance on ICTs for many day-to-day activities. The Internet has provided a platform on which ordinary citizens may conduct various daily activities, including online banking, job searches and even general communication with others.

As a result of this, various entities have invested in cybersecurity awareness and training initiatives meant to ensure the cybersecurity awareness of the citizens of South Africa. According to Stats SA (2018), South Africa has many impoverished citizens



who, in most cases, have limited digital literacy and exposure to digital technologies. This lack of cyber education and awareness makes Internet users vulnerable to cybercrimes and citizens are, unfortunately, not well equipped and empowered to address and deal with cyberattacks. Recent cases of cyberattacks indicate that attackers can successfully launch attacks by taking advantage of and exploit the ignorance of users (Mashiane et al., 2019).

In South Africa, access to broadband and the benefits thereof is considered a universal right (Wallace & Philip, 2019). Moreover, the National Broadband Policy considers broadband access by poor people as important for social development (Sutherland, 2020). However, the ICTs that provide citizens with access to broadband, services and information are also used by potential criminals to commit numerous crimes, including cyberattacks, data theft and identity theft and to gain access to the homes of average citizens, through their computers (Mozid & Yesmen, 2020). Through the implementation of the National Broadband Policy, the government made a commitment to ensure broadband access to citizens and has acknowledged its role in providing cybersecurity as a subdivision of national security (South African Government Gazette, 2019).

The ordinary end user is the easiest target for cybercriminals because they are mostly naïve as far as cybersecurity is concerned. This being the case, enterprises like banks have always been investing in cybersecurity as they were previously the most affected by cybercrimes and have begun providing training to their employees (Adams, Fourie, Marivate & Plantinga, 2020). To that effect, attention has shifted from banks to innocent, naïve end users, who, through various practices, such as socially engineered cyberattacks, suffer various cybercrimes such as identity theft because of their personal login information and personal information being collected or harvested without their knowledge (Sutherland, 2020). It is, indeed, of vital importance that the end user be educated and made aware of the ruthless cybercrimes and how to effectively protect their personal information and data in the cyberspace.

The Academy of Science of South Africa (2020) acknowledges the fact that times are changing and technology is fast advancing. The technological advances that are rapidly occurring have affected the way in which daily activities are happening; how commercial enterprises conduct their business; and how customers are accessing business operations. In accordance with the National Broadband Policy, the

government realised that it needed to ensure that it provides cybersecurity. However, cybersecurity needs to be appropriate in relation to different groups of users and should be directly responding to their vulnerabilities and levels of understanding.

Additionally, Ahmed (2020) is of the opinion that user awareness is very important for any security programme to be successful, which also applies to cybersecurity. With the broadband expansion initiatives to bridge the technology gap in societies on a global scale, citizens are gladly utilising the resources being provided, enabling them to have access to the Internet and to enjoy usage of computers. One of the major challenges regarding cybersecurity is the lack of awareness on the part of the users of the facilities provided to ensure free and/or affordable Internet access. Users lack awareness regarding basic things like malware and cyberattacks, or even random threats like ransomware, suggesting the need for greater user cybersecurity knowledge and awareness (Dahabiyeh, 2021).

Pretorius and van Niekerk (2015) found that the existence of weaknesses in industrial control systems emanated from insecure management of users' passwords; having outdated or even a lack of antivirus and malware protection; software that is not updated; and uninstalled software patches. Pretorius and van Niekerk (2015) believe that user awareness and training are important for users. Williams (2019), nonetheless, suggests that cybersecurity education, user engagement, user awareness and user training play a crucial role as part of a cybersecurity prevention approach programme. As the sole strategy being implemented for protection against cybersecurity threats, however, it is inadequate. There is need for a joint approach to cybersecurity governance and protection that should include hardware and software protection as well as providing adequate training for people involved in cybersecurity (Rubeis & Ketteler, 2020).

Bidram et al. (2019) recommend a total shift in how cyber training is done; encouraging proper planning aimed at changing employee behaviour. By so doing, the organisation's risk is kept to a minimum. Lamba (2020) concurs, adding that a greater proportion of cyber risk stems from simple mistakes on the part of employees when they perform their duties. Sharikov (2020) posits that it is important for users to be responsible when online and to be able to protect personal information, arguing that information is power. Users need to be encouraged to be responsible when using Internet resources. There is a need for complete, understandable and simple codes of

conduct that users should comply with when accessing the Internet through these broadband expansion projects, whether they are using their own devices or the centre's computers.

Consequently, it means that deploying employees as an active part of the defence is a priority, in addition, the National Institute of Standards and Technology (NIST, 2019) advocates for vigorous cyber training and education, arguing that it is key for effective and efficient cybersecurity. Security policies dealing with proper usage of IT resources and information protection are important, but there is a critical need for users to be trained and educated in issues of security (NIST, 2019). Durodolu and Mojapelo (2020) add that more emphasis should be placed on the user training and awareness, rather than only concentrating on securing the network IT infrastructure to protect the organisation's information and IT infrastructure.

A study conducted by Pramod and Raman (2014) on students in tertiary institutions found that, while students may have some knowledge pertaining to security concerns regarding smartphones, they are not entirely mindful of all the security threats and risks, as well as of the essential security practices. This points to misconceptions in the community; therefore awareness, training and continuous refresher training are necessary to make sure that the community is aware of cybercrime trends and how to combat any innovation or new trick that may be used to cyberattack them.

## **2.8 Cybersecurity policies and governance**

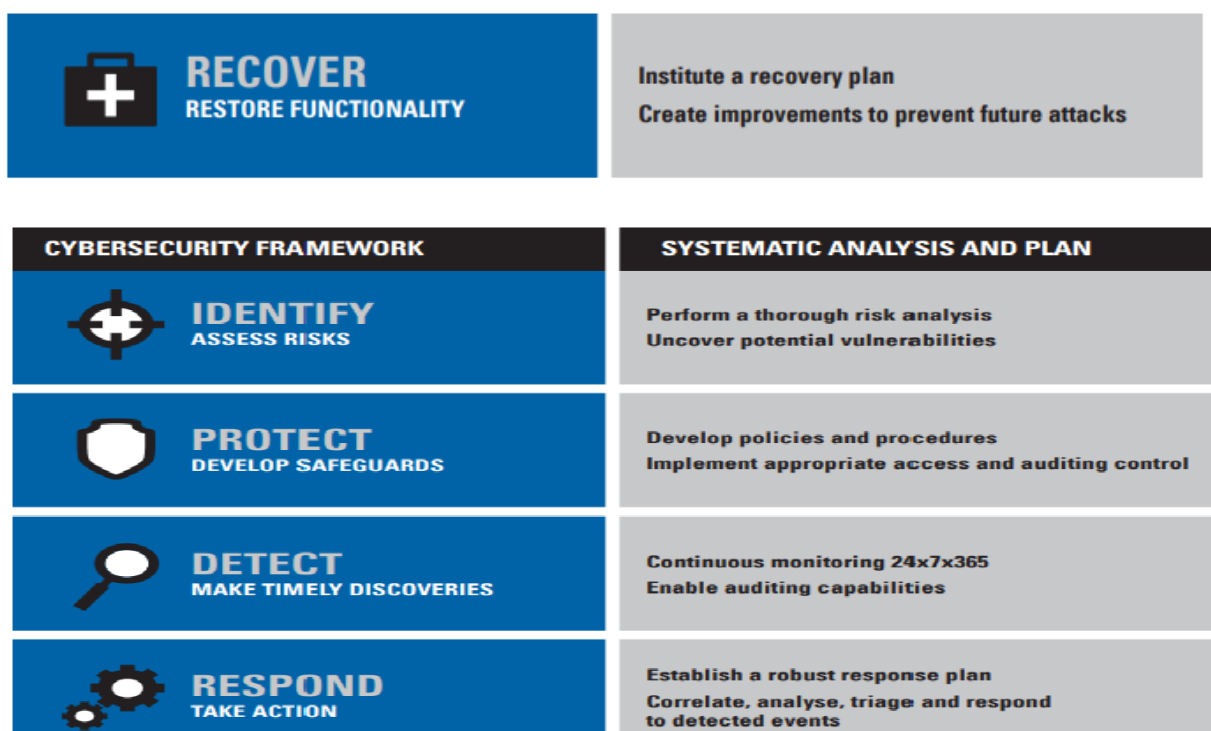
For cybersecurity to be possible there is a need for policies and governance strategies to be implemented that govern cyber usage as well as policing the cyberspace; implementing cybersecurity strategies to administer the range of cyberthreats (OECD, 2015).

Like any other developed and developing countries, the government of South Africa has legislation in place dealing with cybersecurity governance. The reason behind having such policies/legislation, or rather strategies, relating to cybersecurity in place is to deal with different types of cyberthreats that occur all the time and which are forever increasing in complexity and significance (Sterlini et al., 2019).

Cybersecurity is a multifaceted and difficult issue that cannot have a single solution to implement it. Cybersecurity implementation requires different angles to be used to ensure cybersecurity. The facets include policies and procedures aimed at

identification, protection, detection, response and recovery (Mukherjee, 2019), as illustrated in Figure 2.5.

Figure 2.5 clearly illustrates that cybersecurity governance requires a collective effort in the form of legislation, administration and user engagement. There is a need for policies and legislation to govern and police the cyberspace. Countries are busy working on policies and legislation to protect users and the infrastructure from cyberattacks, cyberthreats, cybercriminals and even cyberterrorists. Reuters (2016) reports that developed countries like the US diligently keep working on improving cybersecurity practices on an ongoing basis.



**Figure 2.5: Cybersecurity facets**  
(Source: Mukherjee, 2019)

Cybersecurity policies are implemented to improve the cybersecurity ICT risks, threats and misuses in the cyberspace. In South Africa, there are national cybersecurity strategies that have been considered, reviewed and revised but have not been properly structured to ensure efficient governance of cybersecurity (OECD, 2015; Dean, 2016).

The National Cybersecurity Policy Framework (NCPF) was adopted to ensure cybersecurity coordination in South Africa. The Protection of Personal Information Act of 2013 (PoPI Act) was enacted for citizens' privacy and data protection but, until early

2018 it was not fully implemented and executed Cybercrimes Act 19 of 2020 was also introduced to assist with cybercrimes regulation in South Africa (Betts, 2018).

Laws and regulations concerning cybersecurity need to be evaluated for their influence on how people use or misuse electronic information on an ongoing basis because both information and technological advancements are continuous. South Africa needs to be well equipped to tackle the numerous challenges being faced in cyberspace. Such challenges include phishing attacks, cyberbullying, cyberharassment, cyberattacks, distribution of malware, the theft of intellectual property rights (IPR) and cyberespionage attacks (NIST, 2019) on the Internet so that the information cannot be diverted, monitored or altered. The seriousness of the cyberattacks and their potential effects has led to the need of high-level security measures to be put in place to support information and communication technology. Governments globally are implementing cybersecurity strategies to administer the range of cyberthreats (OECD, 2017).

To achieve cybersecurity in South Africa, skills are needed that include network monitoring, cyber forensics, software development, cyber analysis and cyber investigations. It is the duty of the government of South Africa to produce sound governance strategies to mitigate cyberthreats and risks, and to conquer cybercrime (Karlidag & Bulut, 2020). The State Security Agency has been given the responsibility of coordinating, developing and implementing measures for cybersecurity. The effectiveness and success of cybersecurity governance strategies depends on three main factors, namely local and international cooperation; capacity building and research and development; and the promotion of a cybersecurity culture in South African society (Joshi & Akhilesh, 2020).

Cybersecurity strategies have been proposed and some implemented at a national level. South Africa, however, does not have adequate and effective cybersecurity governance policies that can secure its cyberspace (Jansen van Vuuren, Grobler, Leenen & Phahlamohlaka, 2014). Broadband expansion in South Africa has rendered average citizens prone to cyberattacks (Sutherland, 2020).

Without effective and adequate cybersecurity strategies being implemented, the lives of ordinary citizens could potentially be endangered as citizens become exposed to a range of risks emerging from critical infrastructure (electricity grid, water purification, traffic lights, shopping centres and hospitals) on which business operations are largely

reliant. Any disruption in these essential services may be catastrophic for communities (Jahankhani, Kendzierskyj, Chelvachandran & Ibarra, 2020). Cybersecurity strategies include measures to fight cybercrime as well as criminal justice responses to cyberattacks (South African Government Gazette, 2015). Massey (2020) argues that policy documents and pieces of legislation exist at top levels and not being implemented on the ground where broadband expansion projects are being run. Moreover, Massey notes that, at the grassroots level, within communities at large, there is a need for hands-on approaches that ensure that there is security within the cyberspace.

Important to note is the fact that, throughout the world, strategies for cybersecurity are being developed with the objective of putting in place policy goals, procedures and institutional responsibilities for cybersecurity governance (Balakrishna & Soman, 2020). The daily functioning of society currently is dependent on ICT solutions, resulting in a need for the development of adequate security measures (South African Government Gazette, 2015). Cybersecurity strategies are needed to ensure protection of the cyber infrastructure and the cyberspace (South Africa. Department of Communications, 2020).

In 2015, only 28 countries had a cybersecurity policy in place and South Africa was amongst these countries (Fichardt, 2015). Research and legislation review raise the following: firstly, government agencies need to implement training or specific types of security policies and practices to improve incidence response times and preparedness. Secondly, cybersecurity 'activists' call for increased penalties for computer crime and for legislation that must fully address specific crimes, for example, ransomware. Thirdly, there are calls to fully regulate cybersecurity within the insurance industry to address cybersecurity. Fourthly, there are calls to create task forces, councils or commissions to study or advise on cybersecurity issues on a continuous basis for improved efficiency and effectiveness. Lastly, there is a need to create an environment that supports programmes or incentives for cybersecurity training and education (Pretorius & van Niekerk, 2020; Rajabiun, 2020; Iqbal & Anwar, 2020).

Karlidag and Bulut (2020) note that the issue of cyberattacks and cyberthreats is not only a problem in South Africa, but this is common to most countries worldwide. It is essential for South Africa to have practical structures in place to ensure cybersecurity. The enormous growth in Internet connectivity in many developing countries such as

South Africa has resulted in these countries being more vulnerable to cybersecurity threats (Jansen van Vuuren, Phahlamohlaka, Leenen & Zaaiman, 2014).

Studies and reports point to the fact that South Africa is among the countries most targeted by cyberattacks and has, in the past, ranked third in numbers of cyberattack victims worldwide. On the African continent, South Africa has experienced the most cyberattacks in comparison to other countries (Van Heerden et al., 2018). There has been a large influx of migrants and tourists to South Africa compared to other countries on the continent, which accounts for the high numbers of cybercrimes, arguing that tourists and migrants also bring with them ideas and sophisticated means to perpetrate crime. Moreover, Adams, Fourie, Marivate & Plantinga (2020) also suggests that tourists and migrants are equally victims as they must interact with local information and technology that they might not be able to fully comprehend.

There are, therefore, justified calls to have proper cybersecurity measures in place that complement the use of IT that the government cannot afford to ignore. South Africa has begun to make strides as evidenced by the NCPF of 2015, PoPI Act and, recently, the Cybercrimes Act. However, Sutherland (2017) maintains that South Africa trails behind other countries when it comes to cybersecurity legislation in terms of alignment with government coordination and engagement in the private and public sectors in comparison to advanced economy countries

### **2.8.1 The National Cybersecurity Policy Framework (NCPF) of South Africa**

The grounds for the establishment of the NCPF was to create a secure, dependable, reliable and trustworthy cyber environment that facilitates the protection of critical information infrastructure, while strengthening shared human values and an understanding of cybersecurity in support of national security imperatives and the economy. As a result, the framework should enable the development of an information society that considers the fundamental rights of every South African, which are privacy, security, dignity, access to information, the right to communication and the freedom of expression (South Africa. Department of Communications, 2015).

A committee called the Cybersecurity Response Committee (CRC) was put in place with the responsibility of overseeing the implementation of the NCPF. Inasmuch as this prospective policy framework is a high-level policy, it is too vague. At this stage, there is not really anything to comply with. It is rather a case of making sure that citizens are

cybersecurity-aware and that community projects comply with general cybersecurity best practices and guidelines. The NCPF was established for all relevant stakeholders, which includes the State and public and private sectors, as far as cybersecurity is concerned (South African Government Gazette, 2015).

The NCPF aims to set policy goals and measures, as well as institutional responsibilities, to ensure national cybersecurity. The aims of this policy, among many other aims, include promotion of a cybersecurity culture and mandatory acquiescence to a set minimum standard. The South African NCPF is focused on a safety and security response as far as the cyberspace is concerned. South Africa depends on the Internet for governance and for conducting its affairs, as well as for social purposes. Many people use the Internet and access a great deal of information through the Internet. Cybercrimes and threats have also greatly increased, which, potentially, impacts on the national security and economy of the country (South African Government Gazette, 2015).

The Cybersecurity Hub was launched in October 2015. Following the establishment of the NCPF, a National Cyber Security Awareness Month (NCSAM) was launched in October 2016 and has since been observed annually during October. This hub provides a platform for anyone to report cybercrimes and, thereafter, all complaints made are investigated and feedback is provided to the complainant. Cyber awareness campaigns have been launched throughout South Africa by the Cybersecurity Hub to increase awareness amongst citizens (Helyes, 2021). The Cybersecurity Hub is South Africa's National Computer Security Incident Response Team (CSIRT) and its aim is to make the cyberspace a safe and conducive environment, where all South African citizens can safely communicate, socialise and transact in confidence (South African Government Gazette, 2015).

The hub does not work in isolation. It achieves its objectives by being involved in combined efforts with the government, private sector, civil society and members of the public, having one goal, which is to identify and to counter cybersecurity threats in the country (South African Government Gazette, 2015). This is a collaborative effort between government and the private sector to ensure citizens' awareness in the cyberspace, to raise awareness and to educate citizens and organisations. The hub aims to provide initiatives to raise awareness regarding the importance of cybersecurity and awareness as well as providing tools and resources that are needed to ensure



user safety whilst using the Internet or, generally, the cyberspace (South African Government Gazette, 2015).

The Cybersecurity Hub was set up to serve as a central point for all groups of society, namely industry, government and civil society, and provides information on awareness creation about cybersecurity and that encourages South African citizens and organisations to be secure while on the Internet. At the Cybersecurity Hub, citizens may obtain information regarding the do's and don'ts of the Internet, how to protect oneself against malicious attacks, information and identity theft and financial security while using the Internet. Further information may be found on [www.cybersecurityhub.gov.za](http://www.cybersecurityhub.gov.za) (South African Government Gazette, 2015). The NCPF does not make specific provision for cybersecurity governance in community broadband centres (Jansen van Vuuren, Grobler, Leenen & Phahlamohlaka, 2014).

In conclusion, Bote (2019) sums up the demerits of the policy, stating that several loopholes or contradictory issues have been noted, such as the NCPF being underspecified, lacking clarity on cooperation and partnership and flimsy implementation by the State. Furthermore, Ramluckan (2019) notes that the NCPF needs to focus more on reducing the likelihood and consequences of both intentional and accidental cyberattacks.

### **2.8.2 The South African Cybercrimes Act 19 of 2020**

Cybercrimes Act 19 of 2020 was introduced with the objective of providing a coordinated approach to combat cybercrime and securing the cyberspace. The Act provides a list of new cybercrime and cybersecurity crimes related to data, computers and networks. It will look at criminalising the theft and interference of data and will also herald the introduction of new laws surrounding any malicious electronic communication. According to the South Africa Cybercrimes Act 19, cybersecurity is defined as “technologies, measures, and practices designed to protect data, computer programs, computer data storage mediums or a computer system against cybercrime, damage or interference”.

The Act addresses several issues relating to cybersecurity, including cybertheft; theft of personal information; cyber fraud; cyber forgery and uttering; cyberextortion; unlawful interference and interception relating to computer systems; and data theft, to mention but a few areas of interest. All these, and more, are made punishable offenses

with the possibility of getting up to three years jail time as a penalty for cybercrimes (South African Government Gazette, 2020).

There are several good things that can potentially come from the Act such as jail time of up to three years for activities such as hate-speech online, inciting violence against anyone and cyberbullying, to mention but a few. The legislation is, unfortunately, still too broad and does not directly acknowledge that the legislation to curb cybercrime is desperately needed in an age where hacking, unlawful interception of data, ransomware, cyber forgery, uttering and cyberextortion (all offences under the Cybercrimes Act) are experienced by South Africans daily.

### **2.8.3 Protection of Personal Information (PoPI) in South Africa**

The PoPI Act 2013 was enacted to try and ensure data privacy as a means of information regulation. Its purpose is to ensure the protection of the personal information of citizens and to ensure that institutions in South Africa safeguard people's personal information and conduct themselves responsibly in all processes regarding any entity's personal information (Abdulrauf, 2020).

The PoPI Act holds institutions involved in collection, processing, storage and sharing of anyone's personal information, liable and accountable if there is any abuse of a person's personal information. This legislation considers personal information as valuable. The owner of the information has certain rights in respect of protection and may exercise certain control over that information (South African Government Gazette, 2013). However, the PoPI Act needs to be fully enforced and must make citizens, organisations and service providers accountable as its implementation is currently very slow (Sutherland, 2017).

Personal information refers to information such as phone numbers, age, email addresses, gender and an individual's identity number, to mention but a few in detail. The owner of this information has rights over when and how their information can be shared, how their data will be used, how much of their data may be accessed, who can access their data, data accuracy and the integrity of their data, amongst other rights. The right to protection of personal information applies to natural persons as well as legal entities, be they companies or communities (South African Government Gazette, 2013).

With the emergence of social media platforms, such as LinkedIn and Facebook, it becomes a challenge to exercise these rights in terms of PoPI Act because once personal information is shared in public services it becomes difficult to manage, control and protect. The use of modern technologies has created an easy way of harvesting people's personal information without their knowledge, through the Internet. Personal information is collected when entities buy online, and their information is potentially shared with third parties. This personal information may be sold or redistributed and, if the information falls into the wrong hands, irretrievable damage may be caused to people and/or companies. Personal information shared or distributed on public platforms is difficult to manage and control, thus, the best way to protect one's personal information is by limiting the amount of personal information that one shares on social sites (South African Government Gazette, 2013).

According to the PoPI Act, companies are at liberty to use personal information only for the agreed upon purpose and they may only share or process personal information further with the consent of the individual or entity. The PoPI Act cannot, however, protect a person if they themselves cannot protect themselves and manage their personal information (South African Government Gazette, 2013).

## **2.9 Security methods and practices used for cybersecurity**

To achieve cybersecurity, it may be best to integrate different kinds of security techniques rather than to rely on one. There are many kinds of security solutions that may be employed for cybersecurity. For example, companies may embark on deliberate cybersecurity training courses for their employees; they may have standard operating procedures that become company policy; and the informed adoption of mechanisms such as Secure Sockets Layer (SSL) cryptographic protocols designed to provide communications security over a computer network. Using the Cisco Identity Services Engine (ISE), one may monitor a network. The network administrator will know who is connected to the network and which applications are installed and running, to mention a few activities. Implementation of an Intrusion Prevention System (IPS) is another method being used to protect networks. IPS is a threat-prevention technology used on a network to monitor traffic that gets onto the network and detects vulnerable aspects of that traffic, most commonly in the form of malware (Uçtu, G., Alkan, M., Doğru, İ.A. & Dörterler, M., 2021).

The implementation of more internal controls, such as user authentication, is another solution that may be relied upon for network security by allowing only authorised users to access and to use the network resources. The users need to be authenticated using login username and password credentials to utilise network resources. User access rights also need to be established to limit the resources that users may have access to. For example, users who are students may only access the Internet and not the network resources of an institution of learning. Employees may also register their personal devices that they bring to work to connect to the network and use. The devices may then be set up to access the local area network, as well as network resources, so users can work from any location on the campus (Bure & Tengeh, 2019; Massey, 2020).

Furthermore, network monitoring tools can be used to monitor user logs and usage on a network and protect the network from intrusions. There are different solutions that can be used to monitor networks, including cloud monitoring tools, Identity Services Engines (ISEs), Intrusion Detection Systems (IDES) and more. Using these monitoring tools, network administrators can evaluate and review how the cloud infrastructure is functioning and know its operational status. With an ISE, users and devices are registered and profiled, and the application provides streamlined network visibility and policy enforcement, which makes it easy to manage and control the network access of users and devices. This software is used to monitor incoming and outgoing traffic and to block certain malicious websites, when necessary.

With the advancement of technological developments, some institutions now allow users to bring and use their own devices. These are usually devices that the users are comfortable with, to perform their work. This trend is popularly known as 'bring your own device (BYOD)'. BYOD is a trend where users bring their own computing devices and use them to connect to the institution's network to utilise the network resources. This approach provides users with the agility to connect and to use their own devices on the network, on their own, without needing IT assistance (Williams, 2019). However, Cecil et al. (2019) warns that, in this situation, greater precaution needs to be practised for security purposes. For example, users' devices need to have updated antivirus and system software on them to protect the network from intrusion.

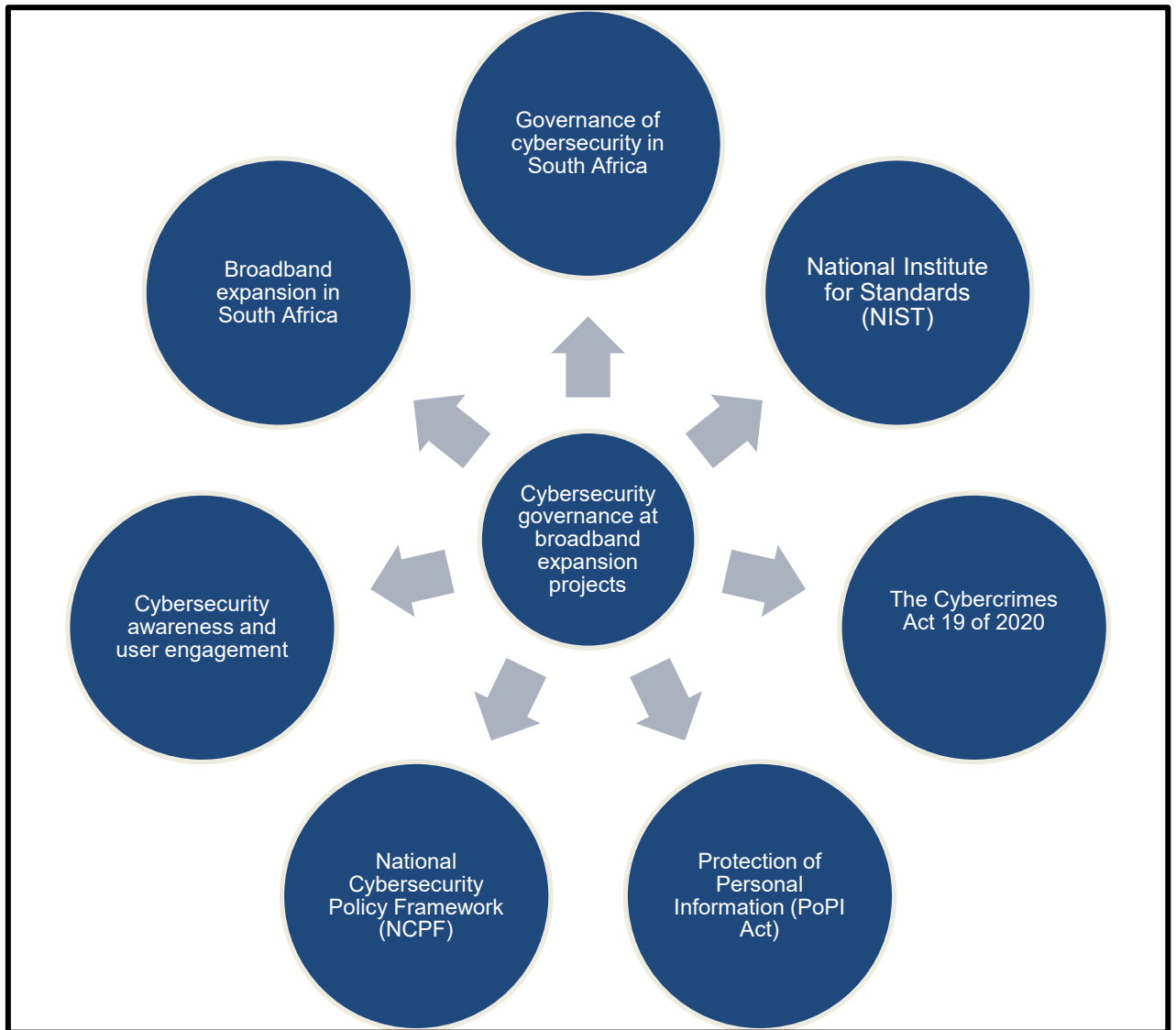
Cisco ISE supports and assists users, as well as enabling self-service device onboarding, which enables users to manage the devices that they bring to work in

terms of a BYOD approach in accordance with the business policies in place in the institution. Cisco ISE enables IT staff to implement automated provisioning, profiling and posturing of devices that need to comply with security policies. All this help to ensure network security and reduce users' risk of bringing malware onto the network or, even worse, of losing their sensitive data (Cisco, 2019b).

Malware is any software intentionally designed to cause damage to a computer, server, client or computer network (Bingham, 2019). The Intrusion Prevention System (IPS) is an inline security component that should work effectively, in real time, to combat these exploits and to avoid network performance degradation. An IPS is often positioned behind the network firewall where it directly examines all traffic flows onto the network and its actions can be automated (Pandur, Mohan & Kumar, 2019). These actions include notifying the administrator of malicious input by sending an alarm, discarding contaminated packets or malicious packets, blocking traffic from the source address that has sent malicious packets and resetting the connection (Cisco, 2019b).

## **2.10 Conceptual framework**

This research is underpinned by the conceptual framework shown in Figure 2.6. The framework contains the main nuggets of the research that were extracted from a review of literature. The conceptual framework guided the formulation of research questions of the study and the analysis of finding of this study. Research questions were created to gather facts regarding to cybersecurity governance in broadband expansion to enable the researcher to understand cybersecurity practices, challenges, user awareness, and effectiveness of currently implemented cybersecurity governance strategies in broadband expansion projects.



**Figure 2.6: Conceptual framework of the study  
(Source: Researcher)**

The following section briefly expands the main nuggets of this study contained in the above conceptual framework.

### **2.11 Broadband expansion in South Africa**

This section presents an overview of cybersecurity governance and broadband expansion projects in South Africa.

The National Broadband Policy was published in December 2013. Among other reasons, this policy was brought into being to provide a long-term plan for bridging the digital divide in South Africa, to actuate broadband connectivity in South Africa, and to ensure universal, affordable broadband access by South Africans. Broadband

expansion projects are being used to catalyse broadband connectivity worldwide, South Africa included.

Broadband expansion is not a new dispensation in South Africa. It started years back and was implemented through the establishment of telecentres. Telecentres were, and still are, ICT centres that are installed in disadvantaged communities. The purpose of such facilities is to enable people living in those communities to access the digital world, in other words, to access the Internet thereby being able to access information, and to access and use ICTs for individual and community development. Telecentres are public spaces where access is reserved for a community member requiring access to technology. In such centres, people can use computers and have access to the Internet. Telecentres are mainly found in disadvantaged communities that exist in rural areas or in marginalised urban areas. Although the concept is the same, broadband expansion projects though are projects implemented for expanding broadband access to the community, they are not primarily focused on previously disadvantaged communities. Rather, any community where there is a need for broadband connectivity is considered. Broadband expansion projects can be initiated across the board, involving a variety of communities, including private and public communities in urban and rural areas.

Indeed, as the digital revolution is proving to be successful, great milestones have been realised and celebrated in respect of broadband connectivity in South Africa. Many broadband expansion projects have sprouted as strategized by the National Broadband Policy, and more and more communities are being digitally included as universal access to broadband within communities is being achieved. Broadband expansion is currently in progress in South Africa, being driven primarily because of the need to bridge the digital divide and ensure that all citizens are incorporated into the digital era. We are living in a world where most services are slowly becoming digitised, including communication, shopping, government services and lately, even education. Many projects have been rolled out to expand broadband access to different communities.

Some of the notable broadband expansion projects in South Africa that have been reported in the literature are described as follows.

Williams (2019) suggests that broadband expansion is thriving in South Africa, citing projects like the Project Isizwe, Tshwane Free Wi-Fi powered by the City of Tshwane. Academic institutions have also embarked on private and public initiatives to provide broadband access to their staff and students across campuses, which is also a form of community broadband expansion. Community broadband expansion is proliferating in the Western Cape through projects such as the establishment of community broadband centres, the Smart Cape Access Project, the Universal Broadband Network Strategy and the Bandwidth Barn (South African Government Gazette, 2013).

The Smart Cape Access Project, is a project undertaken by the Cape Town City Council, designed to provide citizens of Cape Town with computers to access the Internet free of charge. This project saw free internet access provision to 102 public libraries within the metro. Cape Town citizens who cannot afford to pay for Internet access and who do not have devices with which to access the Internet can now access information and use computers, with free Internet access, because of this project. A public access point was opened in the foyer of the 44 Wale Street building, where five computers were installed and are open for the public for at least 45 minutes per person per day. Using these computers, users can surf the Internet and register email accounts (CLIR, 2004).

Since the launching of the Smart Cape Access Project in 2002, thousands of people have enjoyed the use of free computers in Cape Town's public libraries, along with free Internet access. This project has provided for computer and Internet access; moreover, it has witnessed an increase in computer literacy and experience among its users. The Smart Cape Access Project is expanding its reach in the city (CLIR, 2004).

Project Isizwe is a non-profit project launched in 2013 to provide free Internet to Africa. It is a Wi-Fi service powered by the City of Tshwane that provides free Internet access in public spaces, educational institutions, schools, libraries and clinics across Tshwane. Tshwane Free Wi-Fi is in collaboration between Project Isizwe and the City of Tshwane that is managing to achieve milestones in accordance with the national government's broadband plans. Project Isizwe works with local, provincial and national government to provide wireless Internet access to low-income communities, poorer communities, highly dignified urban areas and educational institutions in the city. Expansion of broadband into these communities enables change; it is a true facilitator of change (Project Isizwe, 2018).



Since November 2013, over 1 076 free internet zones (FIZs) have been deployed in Tshwane, connecting over 3 500 000 users and over 276 million sessions have been recorded by Project Isizwe. This initiative is not only limited to Tshwane. There are 408 free Wi-Fi hotspots in Johannesburg and 408 free Wi-Fi hotspots in Ekurhuleni (these figures could have increased since 2013). Users have 500 MB of free data daily that enables them to surf the Internet, make free data calls and live stream video while on Tshwane Free WIFI.

A content portal called Tobetsa was developed to allow access to content relating to education and skills development, amongst others, that empowers citizens in those communities to participate in the economy. Thus, the provision of free Internet access through FIZs in Tshwane propels economic development. This has been a huge step forward towards bridging the digital divide in South Africa (Project Isizwe, 2018). Project Isizwe seeks to ensure that more and more South Africans freely access the internet by means of their FIZs.

The broadband expansion into South African communities is mainly for the purposes of education, social inclusion and economic development. The City of Tshwane is looking at doubling the size of the Tshwane Free Wi-Fi network. The city wants to ensure that 50% of Tshwane citizens are within walking distance of a Tshwane Free Wi-Fi zone. The City of Tshwane also intends to roll out 1 500km of broadband fibre across Tshwane. This broadband network will facilitate the Tshwane Free Wi-Fi project, enabling the network to reach areas that currently do not have a telecommunications infrastructure.

## **2.12 Related work**

Many studies have been conducted about cybersecurity. The researcher took time to look at other studies done regarding cybersecurity and there are many. Below are descriptions of the studies that most related to this study.

### **2.12.1 Governance of cybersecurity in South Africa**

Sutherland (2017) assessed the performance of South Africa in terms of cybersecurity governance by examining and analysing the NCPF, privacy and data protection, the surveillance system of South Africa, and information available to the public regarding cybersecurity and cybersecurity skills in the country. This paper was written in a South African context. In his findings, Sutherland (2017) pointed out that the South African

government is failing to deliver cybersecurity, indicating that, while the NCPF has been adopted, it is quite a complex framework, its implementation is slow, there is indication that not much consideration given to how the NCPF would be implemented and there is limited reporting. According to Sutherland (2017), there is weakness in cybersecurity governance and the big challenge is cybersecurity education and user awareness that will ensure citizens, either as individuals or as families, adopt good practices in respect of cybersecurity. Internet adoption is on the increase, as are cyberthreats, which is a global concern but not much has been planned or done as far as cybersecurity education and user awareness is concerned.

The challenges of cybersecurity impact on national security worldwide. Internationally, there is a drive by different governments, such as the US, to develop and implement new cybersecurity policies and to revise any existing cybersecurity policies. Because of the over reliance on the cyberspace in developed countries, it becomes compelling to start cybersecurity initiatives. As for developing countries like South Africa, the focus is on expanding broadband and increasing connectivity to bridge the digital divide. However, in the process, risks that arise as citizens become more connected to the Internet are neglected. Developing countries must join the race to develop and implement cybersecurity policies (Jansen van Vuuren, Phahlamohlaka & Leenen, 2012). There is no coordinated approach to address cybersecurity in South Africa, according to the South African Government Gazette (2010b). There is need for a holistic approach to cybersecurity to adequately secure the cyberspace. A cybersecurity governance structure and an implementation model based on the Cyber Security Awareness Toolkit is proposed as part of cybersecurity strategy and implementation (Jansen van Vuuren, Phahlamohlaka & Leenen, 2012).

### **2.12.2 Cybersecurity culture**

South Africa has seen the roll out of free Wi-Fi in many cities as part of a national drive to connect South African citizens to the Internet. However, the effort of connecting South Africans to the Internet does not tally with national cybersecurity efforts, which are inadequate. There should be a culture of cybersecurity amongst citizens, but there is no apparent practical plan to nurture this culture of cybersecurity in South African citizens (Gcaza & Von Solms, 2017). There is an increasing dependence on and adoption of the cyberspace, but as good as the cyberspace may be, with many opportunities, there are also many security risks that are posed in this space.

According to Lewis (2015) South Africa ranked third in cybercrimes victims worldwide. There is need for implementation of cybersecurity governance strategies to ensure the safety of South African citizens as they enjoy the different opportunities brought about by the cyberspace. The culture of cybersecurity is important as seen by the drafting of the NCPF and its approval by Cabinet in 2012. This is an acknowledgement of the importance of a cybersecurity culture in South Africa as it contributes to the national security. Yes, a cybersecurity culture is fundamental but a practical strategy to implement a cybersecurity culture in South Africa is not there. In the study by Gcaza & von Solms, (2017) an environmental assessment was done to identify challenges (referred to as diagnostics in this study) facing the South Africa cyber environment.

Diagnostics indicated by the study include:

Diagnosis 1 (D1): Poor Government Accountability

Diagnosis 2 (D2): Lack of Resources

Diagnosis 3 (D3): Poor Stakeholder Management

Diagnosis 4 (D4): Lack of Regulation

Diagnosis 5 (D5): Lack of Skilled Human Resources

Diagnosis 6 (D6): Lack of Research and Development

Diagnosis 7 (D7): Lack of Monitoring and Evaluation (Gcaza & von Solms, 2017).

The idea of a security culture refers to an information security and cybersecurity culture. The security culture is developed in an organisation with attention being paid to factors within the organisation that have the potential to influence the security culture (Da Veiga, 2019). It is important to assess the current security culture in an organisation, audit what is happening within the organisation with the intention of understanding what is happening within the organisation to identify the corrective action needed to achieve a security culture and to then implement the corrective action.

Cybersecurity has been toping the agenda in South Africa for years. The increasing cybersecurity risks have been a big concern for the South African government and its position is that to address and deal with cybersecurity, threats should be one of three dimensions, namely personal, national and international (Mabunda, 2021). Regulation of cybersecurity in South Africa includes the coordination of cybersecurity activities and data protection at national, regional and municipal levels of government.

The researcher did not find any study done in South Africa that deals directly with cybersecurity in broadband expansion projects. There appears to be a gap in literature.

### **2.13 Cybersecurity policies and legislation in South Africa**

South Africa has already approved cybersecurity policies and legislation that were explained in previous sections. There is the National Cybersecurity Policy Framework (NCPF), the Cybercrimes Act 19 of 2020 and the Protection of Personal Information Act (PoPI Act) all these were approved to deal with protection of personal information and protecting users and the cyberspace to ensure data privacy. However, according to Sutherland (2017), South Africa trails behind other countries when it comes to cybersecurity legislation in terms of alignment with government coordination and engagement in the private and public sectors in comparison to advanced economy countries.

### **2.14 Cybersecurity awareness and user engagement**

Cybersecurity awareness is important for users to empower themselves to prevent them from becoming victims of cybercrimes, cyberattacks and cyberthreats. Additionally, cybersecurity awareness and user engagement ensure that users or citizens are aware of the vulnerabilities they are prone to and the imminent danger they could potentially find themselves in when using digital resources and the Internet, which are the elements that make up the cyberspace.

### **2.15 National Institute for Standards (NIST)**

The National Institute for Standards (NIST) Cybersecurity framework provides guidelines and best practices recommended for Cybersecurity governance. This guided the formation of the conceptual framework the researcher is using in this study.

### **2.16 Chapter summary**

This chapter provided a contextual analysis of the literature available on cybersecurity governance in community broadband projects on a very general level. Broadband expansion is a government vision propelled by SA Connect with the vision of bridging the digital divide in South Africa and ensuring broadband access in all corners of the Republic.

In this study, the researcher ties cybersecurity governance to user awareness as cybersecurity cannot be achieved by policies and legislation along, but also with user engagement and the behaviour of users as they access and use the cyberspace

resources, ensuring that users are aware of the risks that arise along with access to the cyberspace. The main themes illustrated by the conceptual framework in this chapter are what underpin this study, the researcher discussed all the themes in this chapter. These main themes are as listed below.

1. Cybersecurity; in South Africa, Africa and world-wide.
2. Cybersecurity legislation in South Africa, which includes:
  - a. The Cybercrimes Act.
  - b. Protection of Personal Information Act (PoPI Act)
  - c. National Cybersecurity Policy Framework (NCPF).
3. Cybersecurity awareness and user engagement.
4. Broadband expansion projects.

Cybersecurity is a trending issue that is a concern, not just in South Africa, but across the globe. Worldwide, developing and developed countries are racing to devise adequate governance strategies to ensure cybersecurity. The aim of this study is to contextualise cybersecurity in broadband expansion projects and explore what is being done regarding ensuring cybersecurity in the broadband projects that are mushrooming all over South Africa in a bid to bridge the digital divide because of the global push for universal access to the Internet.

Once one talks about access to the Internet, one can never do so without talking about cybersecurity. For years, cybersecurity has been an area of concern that is topping on the South African agenda. The rapid increase in broadband access through the implementation of broadband expansion projects has also seen the proliferation of cybercrime, together with challenges that come with cybersecurity governance challenges. Yes, there is rapid growth in broadband connectivity as well as growth of digital technology in South Africa, which is being attained through the implementation of a variety of broadband expansion projects; however, the concerns remain in respect of the issues of cybersecurity governance. Digital inclusion is being pushed across the globe, with more and more people are gaining access to the Internet and to digital technologies. Technology companies are even investing in subsidised smartphones to afford citizens the opportunity to access broadband. This has seen more and more people taking advantage of the broadband access that is being extended to different communities in South Africa and, as a result, access to digital platforms is on the increase.

Awareness is the interrelationship between the following elements: consciousness; knowledge; behaviour and attitude realisation; cognizance; attitude realisation; self-perception; understanding; and skills (Chandarman 2016). Cybersecurity awareness training is security training used to establish and build the cybersecurity knowledge and skills of systems users that informs users of cyberthreats and susceptibilities in the environment they are working in, as well as how to deal with the threats and vulnerabilities (Mashiane et al., 2019).

In this study, cybersecurity awareness is defined as having consciousness and knowledge, being informed about cyberthreats and vulnerabilities in one's environment and knowing how to deal with them. Cybersecurity awareness training can be used to spread this awareness and training is vital for empowering users as well as equipping them with the knowledge and skills to enable them to protect themselves from cyberattacks and defend themselves in the event of a cyberattack.

Mardis, Jones and McClure (2019) allude to the fact that cybersecurity awareness is important for users to empower themselves and to prevent them from becoming victims of cybercrimes, cyberattacks and cyberthreats. Additionally, cybersecurity awareness and user engagement ensure that users, or citizens, are aware of the vulnerabilities they are prone to and the imminent danger they could potentially find themselves in while using digital resources and the Internet, which is what makes up the cyberspace.

Globally, the idea is to ensure all citizens have access to the Internet, which is the case in South Africa too. Access to the Internet is now considered as a human right but the efforts to expand broadband and make sure that South African citizens are connected to the Internet are not equivalent to the cybersecurity awareness efforts in the country. However, as good as this may be, are citizens aware of the intrinsic risks associated with data sharing as they share data on different digital platforms? Are they aware of the issue of protection of personal information? How much do citizens know about data privacy and their rights to data privacy? Cybersecurity legislation is in place in South Africa, but none of this legislation deals directly with broadband expansion projects.

## **CHAPTER 3: RESEARCH METHODOLOGY**

### **3.1 Overview**

The purpose of this chapter is to describe comprehensively the details pertaining to how and where the research was conducted, the tools and the research methods that were used for the research study. In addition, the chapter provides an outline of the qualitative data collected for the study.

Research design refers to a rational plan for acquiring answers to questions and drawing conclusions (Yin, 2003). According to Maree (2010), there are six types of qualitative research methodologies, namely conceptual studies, historical research, action research, case study research, ethnography and grounded theory. The researcher followed a multiple case study design strategy.

### **3.2 Research paradigm**

A research paradigm is referred to as a set of held beliefs and assumptions that are shared within a research community regarding how problems should be understood and addressed. It encapsulates research philosophy, ontology, epistemology, methodology and axiology.

#### **3.2.1 Research philosophy**

According to Saunders, Lewis and Thornhill (2009), philosophy deals with knowledge – its source, nature and development. They contend that the adopted research philosophy contains important assumptions on how the researcher views the world.

A researcher must have values and beliefs regarding how data pertaining to the phenomenon under study should be gathered, analysed and used throughout the research study. The beliefs and values of the researcher greatly influence the formulation of the results of a study. The researcher assumes the interpretivism philosophy, which advocates for the subjectivity of the meanings of research results. The direction that the researcher went in was to investigate the striking dimensions of cybersecurity administration, user engagement and awareness in broadband expansion projects.

According to Saunders and Tosey (2015), the interpretivism philosophy of research advocates for the subjectivity of the meanings of research results. Iovino and Tsitsianis (2020) note that social scientists have come to understand and accept that subjectivity

plays an important role in making sense of human behaviour in the social world. However, this subjectivity must be conceptualised in the same way that the way research is influenced by the perspectives, values, social experiences and the viewpoint of the researcher (Munro & Hardie, 2019).

### **3.2.2 Ontology**

Ontology is the study of existence or the study of being (Weicheng, 2021). It is mainly concerned with what reality really entails. It is about 'what is' (Scotland, 2012). Ontology is concerned with looking at what constitutes reality and how it can be understood. In this study, the researcher adopted the ontology of relativism, which implies that there are different realities that can be different from one subject to another. The theories used by the researcher in this study are subjective to their realities. A researcher's ontological assumptions lead them to their choice of topic, construction of research questions and resultantly their research methods.

### **3.2.3 Epistemology**

Epistemology is the nature of knowledge and various forms of knowledge (Scotland, 2012). Epistemology is concerned with creation, acquisition and communication of knowledge. It focuses on what makes knowledge valid and how knowledge can be obtained (Raddon, 2010). An epistemological stance draws on being able to understand the knowledge one has and how one knows what one knows (Saunders et al., 2009). These authors contend that epistemology is concerned with what constitutes acceptable knowledge in a field of study. The epistemological stance used in this study was subjectivism, where meaning exists within a subject and meaning is dependent on a person perceiving any scenario; hence, there is no right or wrong because observations depend on the observer. Interpretation of concepts and findings in this study are imposed by the researcher.

### **3.2.4 Axiology**

Saunders et al. (2009) believe that axiology is a branch of research philosophy concerned with studying judgments about value. From an axiology perspective, the researcher was value biased, and her interpretations were based on the meaning structure as built up during her own experiences in life thus far.



### **3.3 Research methodology**

In this research study, a qualitative model of enquiry was used. In this method, human experiences, interpretations and the understanding of individuals or a group of people who are participants in the research pertaining to the cases under investigation are recorded and represented in the research. The human experiences, interpretations and the understanding of individuals or a group of people who are participants in the research pertaining to the cases under investigation were recorded and represented in the research (Quinlan et al., 2019). Qualitative research is non-numeric research, where the focus is not placed on the generation and analysis of numeric data but rather on non-numeric data (Quinlan et al., 2019). The aim of qualitative research is to provide meaning to the research case and to gain new insights.

Yin (2003) defines case study research as an empirical inquiry that investigates a contemporary phenomenon within its real-life context when boundaries between the phenomenon and the context are not clear. Case studies are used for purposes of explaining causal links; describing an intervention; exploring scenarios where interventions have no single output; meta-evaluation; and illustration of topics within an intervention (Yin, 2003). An interpretive approach to the multiple case study was employed for the empirical research (Antoniou, Brooks Ryan, Jiya, Macnish, & Stahl, 2021).

The researcher employed the multiple case study strategy in this study as it provides for more extensive descriptions and explanations of the phenomenon or issue. A multiple case study approach is the most suitable methodology to study ICTs as social systems, where the aim of the study was to review and understand the relevant framework of cybersecurity governance and user engagement at broadband expansion projects. The objective of this study was to investigate cybersecurity governance in broadband expansion projects and the cybersecurity awareness levels of users in broadband expansion projects, while the focus was on reviewing South Africa's current cybersecurity policies and legislation. An overview of the relationship between the research questions, objectives and research activities adopted for the study is shown in Table 3.1 below.

**Table 3.1: Research questions, objectives and methodology mapping**

<b>Research Problem</b>	For broadband expansion projects there is a lack of benchmark standards and a framework for cybersecurity governance that directly addresses issues of cybersecurity, resulting in ineffective governance of broadband expansion projects.	
<b>Main Research Question</b>	What would constitute effective governance for broadband expansion projects?	
<b>Research Sub-Questions</b>	<b>Research Objectives</b>	<b>Methods</b>
<b>RSQ1:</b> What cybersecurity policies and legislation are being adopted and complied with in broadband expansion projects?	Review and evaluate how cybersecurity legislation in South Africa is adopted and applied in broadband expansion projects.	Literature review Semi-structured Interviews
<b>RSQ2:</b> What cybersecurity governance is currently in practice in broadband expansion projects?	Review and evaluate cybersecurity governance strategies currently in existence that supports broadband expansion in broadband expansion projects.  Explore the salient dimensions (framework) of cybersecurity administration (governance) and user engagement (awareness) in broadband expansion projects.	Literature review Semi-structured Interviews
<b>RSQ3:</b> What are the cybersecurity challenges being faced by broadband expansion projects?	Investigate the cybersecurity challenges being faced by broadband expansion projects.	Literature review Semi-structured Interviews
<b>RSQ4:</b> What is effective cybersecurity governance for broadband expansion projects?	Understand what more can be done on top of what has already been done to improve governance of cybersecurity in broadband expansion projects.	Literature review Semi-structured Interviews
<b>RSQ5:</b> What are the results of the lack of cybersecurity governance strategies in broadband expansion projects?	Understand the implications if there is no proper or effective governance of cybersecurity in broadband expansion projects.	Literature review Semi-structured Interviews
<b>RSQ6:</b> How can cybersecurity awareness and training help alleviate occurrences of cyberattacks and cybercrimes?	Understand how cybersecurity awareness and training can help alleviate occurrences of cyberattacks and cybercrimes.	Literature review Semi-structured Interviews

### **3.4 Research approach**

Research approach is described as the researcher's way of thinking that they adopt in a study. It determines how the research will be conducted and how the design of the research is made. The research approach can either be inductive, deductive or a hybrid approach called the abductive approach, which is a combination of both induction and deduction. According to Goddard and Melville (2004), the inductive approach begins with the researcher making observations and towards the end of the research process they propose theories resulting from the observations made.

The researcher used the inductive research approach. Inductive research begins with making a thorough observation of a specific research area. The researcher collected data relevant to their topic of interest. After gathering a significant amount of data, the researcher takes time to analyse the data to identify data patterns in the collected data and develop a theory that explains those patterns. Following the inductive approach, the researcher generated theories directly out of the collected data.

### **3.5 Units of analysis and sampling**

The units of analysis for the research on cybersecurity legislation in various broadband expansion projects were Case 1, a community broadband centre; Case 2, a Technical and Vocational Education Training (TVET) college, Case 3, a private tertiary institution; and Case 4, a public institution of higher learning. The researcher chose these four distinct cases to avoid bias. The researcher included academic institutions in the scope of broadband expansion projects as the idea of broadband expansion is the same as providing broadband access to a community of students, in the case of academic institutions.

Purposive sampling is a technique that is used to selectively hand-pick a sample from a research population purely according to the aims of the researcher, as directed by the purpose of the study (Etikan, Musa & Alkassim, 2016). The purposive method of sampling was used to select participants from the 4 selected cases to participate in the interviews. The interviewed persons had to be directly involved in the broadband expansion projects in their organization, and they needed to have been with the organization for at least five years. This meant that the participants had sufficient understanding of the broadband expansion project in their organisation. In each case study, only persons that met this criterion were interviewed.

### **3.6 Chapter summary**

This chapter presented the methodological framework used in this study and outlined the methods followed in conducting this research. A concise description of cases used in this study was provided.

## **CHAPTER 4: CASE STUDY AND DATA COLLECTION**

### **4.1 Overview**

The purpose of this chapter is to introduce the case study design and data collection methods used in this study in more detail. The researcher provides an in-depth description of all the cases used. A case study is a detailed investigation of a real-life phenomenon (Yin, 2003). If a study involves more than a single case it is referred to as a multiple case study, which is like conducting multiple experiments. The multiple case study allows the researcher to analyse each different case to draw similarities and differences between the cases being investigated (Yin, 2003). In this study, the researcher used the multiple case study approach to investigate what is being done in various broadband expansion projects with regards to cybersecurity governance. This approach was used to avoid bias that can arise from using a single case. This chapter also outlines the data collection methods and instruments used in this study.

### **4.2 Introduction to cases**

Beneficiaries of the broadband expansion are citizens from different communities. Different broadband expansion projects were selected to get a broad overview of what is happening in different spaces, both private and public, and to avoid bias. The participants articulated their knowledge and experiences of the broadband expansion projects that they are involved in. As such, selected relevant people working on the community broadband expansion projects involved with cybersecurity governance were interviewed at the selected sites. The researcher chose the four distinct cases to avoid bias. The selected projects were at the budding stage, with potential to grow, which is why the researcher selected them as cases for the purposes of this study. A random sample representative of the population cannot be drawn as the concept of broadband expansion is a new one with very few people working in this field. The method used to select the sample was the non-probability sampling technique, and participants were selected.

#### **4.2.1 Case 1**

Case 1 is a community broadband centre that functions as a public access facility, providing users in a particular community with access to the Internet. Most users of this facility access the Internet for entertainment and education purposes. The objective of a community broadband centre is to provide broadband access to a disadvantaged community, to empower the citizens with digital skills and the creation

of entrepreneurship opportunities. One basic reason why one needs to be digitally literate and empowered is simply to communicate in this digital world. Most job opportunities require an applicant to be computer literate, thus, various digital skills courses are offered by the Case 1 centre, both free fee-paying courses.

Case 1 has become a digital centre where citizens use computers and access the Internet, with daily access to printing, scanning and faxing facilities. The skills programmes provided at this centre can potentially solve various community challenges, such as gangsterism, poverty and unemployment, to mention a few.

#### **4.2.2 Case 2**

Case 2 is a public TVET college in Cape Town in the Western Cape Province of South Africa. It predominantly serves students from the city's Southern Suburbs, Northern Suburbs and the Klipfontein District. Case 2 embarked on a broadband expansion project to ensure the provision of broadband access across all its campuses. Staff have access to Wi-Fi and the network. The institution is working on expanding this access to students as well.

#### **4.2.3 Case 3**

Case 3 is a private tertiary institution that has numerous campuses in South Africa. For the purposes of this study, the researcher conducted interviews at a campus located in Cape Town. Case 3 has a large catchment area, posing as a private educational hub for students from different walks of life seeking a conservative learning environment with a small lecturer to student ratio. Case 3 expanded their broadband access to accommodate students and staff who bring and use their own devices.

#### **4.2.4 Case 4**

Case 4 is a public institution of higher learning. It has numerous campuses in Cape Town. Although Case 4 has numerous campuses, all network and Internet issues are centrally administered from one of the campuses. It is a government-owned academic institution that has undergone broadband expansion across all its campuses and is continuously working on ensuring broadband coverage in all its premises. This coverage includes the academic facilities, sport grounds and student residences across the campus. Students and staff all have access to the Internet through these facilities. Case 4 has implemented BYOD; employees and students are allowed to

bring their own devices. They are currently working on a BYOD project to manage user devices that users use to access the network and Wi-Fi.

### **4.3 Data collection instruments**

Data collection instruments that were used are semi-structured questionnaires in the case studies, while the literature review was constantly used throughout the study. The data collection instrument comprised a series of questions intended to collect evidence of the problem being interrogated (Zaza, Wright-De Agüero, Briss, Truman, Hopkins, Hennessy, Zhao et al., 2000). Interviews provide an opportunity for in-depth engagement with respondents with unlimited responses (Lewis, 2015). The interview questions were mostly open-ended questions that the interviewees could answer and respond to, referring to their own knowledge and understanding of the community broadband project that they are involved in. Their responses were recorded during the interview with their consent.

Data was collected between January and July 2018. Attempts to access other broadband expansion projects were futile. The researcher attempted to access several broadband expansion projects in 2016 but all efforts were in vain as decision to allow the researcher access to these projects was hampered by bureaucracy. Only in January 2018 did the researcher finally breakthrough and was able to obtain consent to conduct interviews and to secure interview bookings because of the continuous efforts of the researcher's supervisor. The data was collected over a six-month period. The researcher booked interviews beforehand and, in all cases, found the respondents at the sites busy with work.

Semi-structured interviews were used where each of the participants elucidated their experiences at the respective sites in the different roles that they played. The researcher used a digital recorder to capture the interviews and took notes during the interviews. After the interviews, information recorded using the digital recorder was documented by the researcher. A thorough and well-structured procedure was followed during the interviews to ensure data accuracy and to ensure that the data of good quality was collected, as per the requirements for a master's degree.

### **4.4 Content and discourse analysis**

The researcher collected qualitative data. The responses from the participants were captured using a digital recorder during the interviews and then later discussed. The

qualitative data was analysed using content and discourse analysis. Discourse analysis is a technique used to analyse written texts or spoken words, while content analysis is used for the analysis of any texts. The researcher collected as much secondary data as possible from various literature sources and from the interviews undertaken at the selected case sites and analysed the qualitative data.

#### **4.5 Literature review and sampling method**

Throughout this study, document analysis and a review of the literature was continuously undertaken. Information that was acquired through a consistent analysis of literature and documents relating to the research area helped to shed light on this topic and the researcher gained further insights into the research matter. The researcher consulted several policy documents throughout the research, which were consistently referred to as they informed the study.

The researcher applied purposive sampling when selecting the literature and documents that informed the study. Purposive sampling is a sampling technique that is non-random and uses different ways to locate possible participants, based on bias, by the researcher to answer the research questions and to meet the objectives of the study (Saunders et al., 2009).

Purposive sampling is also called judgmental sampling. In purposive sampling, the researcher has the choice of selecting a few participants who will be most representative of the research population. This kind of sampling is important and appropriate when selecting unique cases in the population. This is done in a bid to gain an in-depth understanding of the concept that is being studied from a sample size that rarely represents the whole research population. The participants that were chosen were identified and carefully chosen in accordance with the criteria for participation in the study.

#### **4.6 Use of semi-structured Interviews**

The researcher struggled to secure interviews with people from Case 1, which was the sole case study from 2016. This was the only case that the proposed study was meant to be based on. Finally, in January 2018, the researcher had a breakthrough and managed to secure interviews with people involved in Case 1, with a follow-up interview in June 2018. Two employees from Case 1 were interviewed, including the centre manager.



However, upon completion of the interviews, the researcher realised that the data collected was insufficient to conclude the research. The researcher consulted different facilities embarking on broadband expansion to gain different views and to identify different cybersecurity governance strategies implemented. The researcher decided to move to a multiple case study strategy. The researcher went on to further gather data from cases 2, 3 and 4. These are different institutions that have worked on different projects to expand broadband to users in their respective communities; mainly students and staff.

#### **4.7 Recruitment of participants**

For the purposes of the interviews, the researcher used purposive sampling of people from the different cases who were directly involved in the broadband expansion project implemented by their institution in a bid to obtain accurate information about what was happening on the ground. In purposive sampling, according to Bernard (2006), the researcher knowingly selects participants in their research for a specific purpose, based on the research objectives. The four different sites that the researcher chose had all implemented community broadband expansion initiatives, albeit from different angles and in capacities. However, the goal in all cases was to expand broadband access to users.

#### **4.8 Interview protocol and process**

The guidelines below were followed to the quality and ethical correctness of the interview process:

1. Explain the purpose of the interview to the interviewee and provide them with the interview themes and questions beforehand.
2. Explain any jargon that the interviewee would not have understood when asking questions to ensure the interviewee understood what the researcher was asking.
3. Show the interviewee respect, even when the researcher disagrees with their opinion.
4. The researcher should also consider how the interviewees look on the day of the interview.
5. Address terms of confidentiality to ensure that the interviewees are aware that the researcher is interviewing them for research purposes. Ensure that a

consent form has been obtained and signed before conducting the interviews, to note that participation in the research is voluntary.

6. Explain the format of the interview to the interviewee before conducting the interview.
7. Ask the interviewee for permission to record the interview proceedings using an audio recording device.
8. Listen attentively and take notes during the interviews.
9. Indicate how long the interview usually takes and made sure to finish at about the indicated time so as not to keep the interviewee from their work for too long.
10. Ask the interviewee if they had any comments or additional information that they would like to provide to the researcher to assist in the research study.
11. Thank the interviewee for their time, effort and information at the end of the interview.

#### **4.9 Chapter summary**

This chapter presented the methods employed in conducting this study and the guidelines that the researcher used when conducting the interviews. In this study, primary data was collected using semi-structured interview questions. The chapter also clarified the research design, methodology and approach used during the study to investigate the research topic in a bid to answer the research questions and achieve the objectives of the study. The cases the researcher used for this study were described in this chapter.

## CHAPTER 5: RESEARCH FINDINGS AND ANALYSIS

### 5.1 Overview

This chapter discusses the research findings based on the data gathered from research respondents. The research results relate to the research question, which focused on understanding cybersecurity governance practices in broadband expansion projects that were being implemented on different premises and in different communities in a bid to benefit the public. The researcher conducted semi-structured interviews at four different centres, which were purposefully sampled for this investigation.

Qualitative data was gathered from eight semi-structured interviews that were conducted with key informants from the case study sites. The analysis of findings was guided by the study's main research question, research objectives and existing literature. The main aim of this findings and analysis chapter is to discuss and to analyse the results obtained from semi-structured interviews conducted at the selected sites, as explained in the previous chapter.

### 5.2 Details of interview samples

Table 5.1 below shows the interviewees the researcher interviewed to understand what constitutes effective governance in broadband expansion projects. A total of eight IT professionals participated in the interviews.

**Table 5.1: Details of interview samples**

<b>Company</b>	<b>Interviewee Job Title</b>
<i>Case 1 (referred to as C1 in this chapter)</i>	IT Manager (C1:1)
	LAN Administrator (C1:2)
	IT Technician (C1:3)
<i>Case 2 (referred to as C2 in this chapter)</i>	LAN Administrator (C2:1)
	Assistant IT Technician (C2:2)
<i>Case 3 (referred to as C3 in this chapter)</i>	Network Manager (C3:1)
	LAN Administrator (C3:2)
<i>Case 4 (referred to as C4 in this chapter)</i>	Network Engineer (C4:1)

Interview respondents will be referred by case number in this section. C1.1 is the first respondent from Case 1(C1); C2.1 is the first respondent from Case 2, and so on.

### **5.3 Presentation and discussion of results**

#### **5.3.1 Adoption of policies and legislation in broadband projects**

Research sub-question 1: What policies and legislation are being adopted and complied with in broadband expansion projects?

The researcher sought to understand the policies and legislation being adopted and complied with this in broadband expansion projects.

Respondents from C1 said:

*“We are not aware of the NCPF hence there was no way they could comply with it, however though we are aware of the Cybercrimes Act 19 of 2020 and the PoPI Act of 2013 we are not complying with any of them. We have come up with our own customised policies that we implement for protection against cyberthreats and secure the hardware, software, and network. Internal Internet Usage Policy and Data Integrity Policy are examples of such customised usage policies that have been implemented at one of the cases” (C1.1).*

On the other hand, respondents from C2 indicated that:

*“We are in the process of making our own policies that speak to our current situation in the broadband and BYOD projects currently underway. We are aware of quite a few national legislations being and already implemented to protect to help secure resources and users in the cyberspace.” (C2.1)*

*“As of right now, we are not complying with any of these legislations. We however get pointers here and there to help refine our own policies and documentation regarding cybersecurity governance.” (C2.2)*

Adding to the discussion respondents from C3 noted that:

*“Indeed, there is national legislation relating to cybersecurity governance. We know for instance about the PoPI Act, the NCPF and the Cybercrimes Act 19 of 2020. However, these are high level documents that though we are not complying*

*with any of them, we have our own customised policy that we try to use to ensure hardware, software and network security” (C3.1).*

Respondents from C4 claimed that:

*“We just create our own policies inhouse to govern user behaviour and do not really have any legislation that we have endorsed in our project” (C4.1).*

Considering the responses above, the researcher gathered that none of the interviewees were aware of the NCPF; hence there was no way they could comply with it. All of them were aware of Cybercrimes Act 19 of 2020 and the PoPI Act of 2013 but were not complying with either of them. The different sites that the researcher conducted interviews at have developed and were still working towards localised and customised cybersecurity governance strategies in the form of usage policies and not necessarily relying on the national legislation for guidance.

In 2015, the South African government, led by the Ministry of State Security approved the National Cybersecurity Policy Framework (NCPF), which is a legal framework with the mandate of protecting data as well as guiding and advising users, businesses and citizens, on cybersecurity.

Prior to the implementation of the NCPF another Bill had previously been passed in 2013, namely the Protection of Personal Information (PoPI) Act of 2013. This Act was created to ensure data privacy through the establishment of an Information Regulator. Implementation of this legislation was slow and the provisions of the Act were not followed or adhered to by the case implementers, based on the interviews that the researcher conducted. Legislation is there, but it does not make direct provision for small broadband expansion projects such as the ones which the researcher collected data from.

In agreement with Sutherland (2017), it is evident that more still needs to be done regarding cybersecurity legislation, government coordination and engagement with businesses and citizens as South Africa is behind other advanced countries, where legislation is being implemented. The study palpably indicates that the PoPI Act, the NCPF and now the recent Cybercrimes Act are there, but they remain high-level policies and legislation that exist at national level but are not adopted and complied with at community level.

The institutions have devised customised policies that they implement and utilise at an organisational level to ensure cybersecurity. Indeed, each of the sites under scrutiny had their own policies that they had been implemented, since the national legislation in place is very high level and does not address the requirements of their projects. These usage policies are meant to be communicated to users once they are registered on the institutional databases and can access the Internet through Wi-Fi resources provided by the centre. However, this rarely happens. Users do not access these usage policies that can potentially assist them to ensure that they are cybersafe and aware.

It is, therefore, necessary for follow-ups to be conducted to ensure that user training is happening and that the necessary information that can assist them to be cyber aware and safe is, indeed, passed on to them timeously.

### **5.3.2 Cybersecurity governance in broadband expansion projects**

Research sub-question 2: What cybersecurity governance is currently in practice at broadband expansion projects?

The researcher sought to understand from the research respondents the status of cybersecurity governance in practice in broadband expansion projects.

*“We have implemented compulsory registration on a database before users can get login credentials for authentication.” (C1.1)*

*“Keeping such a register helps to track and monitor user access and usage to know who is using the network resources. We can track all user activity.” (C1.2)*

*“PfSense is used to protect the network” (C1.3).*

On the other hand, respondents from C2 indicated that:

*“We use SSL [Secure Sockets Layer] certificate for encryption. It is a standard technology to secure an Internet connection and safeguard sensitive data being transmitted between two systems, hence the data is protected from anyone to access, read and modify the data.” (C2.1).*

*“Users can bring their own device BYOD [Bring Your Own Device]. To ensure network security at one case they are working on the introduction of the Cisco ISE [Identity Services Engine] for security on BYOD” (C2.2).*

Adding to the discussion respondents from C3 noted that:

*“Cloud monitoring is what we are using to ensure cybersecurity. Cloud monitoring is an aspect of cloud security and management processes. It is employed through monitoring software that is mostly automated and has provision of central access and control over cloud infrastructure. We give users (staff/students) forms to complete so they can access the Wi-Fi using their devices, (BYOD). This enables us to profile users as we map MAC addresses for users’ devices and their names, so we know who is doing what and can monitor traffic and usage. Using our WIFI access users can only access the Internet not our local network or network resources” (C3.2).*

In contrast to the above participants’ views, respondents from C4 said that:

*“We have no structure in place currently for cybersecurity. We have a generic password that allows users to connect to the Wi-Fi. Users can only access the Internet but not the Intranet or our local network or network resource which makes our intranet still secure. We do not have any profiling that we are doing on users hence we can only monitor traffic into and out of the network, but we cannot see who is using what device” (C4.1).*

From the responses the researcher discovered that there are many solutions being implemented for network, data and information security. With the network monitoring solutions, users and devices are registered and profiled and this practice provides streamlined network visibility and policy enforcement, which makes it easy to manage and control user and device network access. However, all these options leave the human element still vulnerable to cyberattacks as the solutions do not ensure that the users are cyber aware or up to date on good practices regarding cyber usage.

These are great and outstanding initiatives for cybersecurity but, just as the literature indicates, with threats of cybercrimes on the increase, cybersecurity legislation and policies that are comprehensive, operative and effective have become a necessity, working towards a collective effort on cybersecurity. Network and infrastructure

security on its own is no longer enough to ensure cybersecurity. There is an urgent need for appropriate and accurate user education, training and cyber awareness.

In accordance with the Cybercrimes Act discussed in Chapter 2, the researcher agrees that user training and education is a key element of cybersecurity; network security solutions alone are not adequate to ensure cybersecurity, based on the fact that campuses and organisations are rolling out Wi-Fi to allow more and more users to bring their own devices and to connect to the network, which organisations will have no outright control over in terms of who accesses these devices.

The human element, the user, is the target of the increase in the number of cybercriminals and of cybercrimes. Hence, there is a need to overcome this weakness by training adequately and educating users to equip them and to make them cyber ready and cyber aware. Cyber awareness campaigns can be conducted in other sectors or areas but there is a need to have correct and effective cybersecurity education, training and awareness that is relevant to this specific community broadband expansion initiative.

From the responses to the question above, there are different security strategies that can be used for network security, including ISE, cloud monitoring software, PfSense and the Cisco ISE are security policy management software tool that are used to monitor users and their usage, as well as applications and devices on a network and provide secure network access to them. Through cloud monitoring, network administrators can evaluate and review how the cloud infrastructure is functioning and know what its operational status is. It is also important to note that, from the responses above, there are currently organisations with no structures in place for cybersecurity, who still use generic passwords to allow users to connect to Wi-Fi. This poses a threat as the organisation becomes vulnerable to cyber threats and has no control over who is using their broadband as passwords can easily be shared with people who are not associated with the organisation. Wong, Ragothaman and Cisco Technology Inc. (2020) explain that Cisco ISE supports and assists users as well as enabling the onboarding of self-service devices, which enables them to manage their devices. Users bring their own devices in accordance with business policies in place in an institution. This protocol provides users with agility to connect and use their device in the network on their own without having IT assistance.



PfSense is open-source firewall/router software that is installed on a server and executes from either a physical computer or a virtual machine. It is used as a dedicated firewall/router on a network to monitor incoming and outgoing traffic and to block certain malicious websites, when necessary.

Linux open-source operating system is used on client computers; the ones users and staff use to access the Internet. An IPS (Intrusion Prevention System) is another method being used to protect the networks. IPS is a threat prevention technology used in a network to monitor traffic that gets into the network and to detect vulnerability campaigns most commonly in the form of malware and prevent these.

Williams (2019) stresses the importance of having a structure and strategies that deal with cybersecurity, stating that, in the absence of security strategies, cyberattacks are most likely to happen and that the organisation will take long to respond to and address the threat. Broadband expansion, the rise in Internet usage, fuelled by advancement of technology, nowadays has seen cybersecurity becoming complex and very challenging. Hackers, attackers and scammers to take advantage of the ignorance and vulnerabilities to launch successful cyberattacks (Mashiane et al., 2019).

### **5.3.3 Effect of broadband expansion on cybersecurity**

Research sub-question 3: What have been the results of broadband expansion and its effect as far as cybersecurity is concerned?

The researcher wanted to understand the effects of broadband expansion through broadband expansion projects. Of late there has been a global drive to expand broadband to all communities and South Africa is no exception, broadband expansion projects have become popular.

Respondents C1.1 and C1.2 stated that:

*“Broadband expansion is an agent of economic growth. Community members can access the Internet and conduct their research. Matric students can search for universities and the courses they can conduct online, and this has increased the number of students going into tertiary schools after matric. Internet access has taken many children off the streets as they can now have other forms of entertainment such as online games. They are to search and apply for jobs online thus reducing unemployment rates in the area.” (C1.1)*

*“Users are enjoying this Internet access but at times when they use the computers in the centre you realise that some forget to log off their accounts for instance emails, which make them cyber victims” (C1.2).*

On the other hand, respondents C2.1 and C2.2 indicated that:

*“Broadband expansion enables the students to get Internet access from any part of the campus and helps them improve their productivity. Users have an opportunity to be able to do their schoolwork from their areas of comfort like their residence. This has reduced pressure on our computer resources as students can just use their own device and Wi-Fi to do their work without being confined to a physical location and computer.” (C2.1)*

*“With this WI-FI expansion project we have had several cyber incidents taking place. Though very few get reported, we are aware that a lot of them take place.” (C2.2 )*

Adding to this, respondents C3.2 noted that:

*“Broadband expansion has enabled users to get Internet access to anywhere around the campus, this has improved user productivity, both staff and students. This has reduced pressure on our computer resources. It has improved communication as well as we mostly use email and WhatsApp, so staff can now use Wi-Fi to connect their devices and get all important information in time without having to log onto a computer to check their emails. We are aware of users that received spam through emails, had their emails and social media accounts hacked etc.” (C3.2)*

Respondent C4.1 said:

*“Broadband expansion has enabled users to get Internet access to anywhere around the campus, this has improved user productivity” (C4.1).*

The age of broadband expansion has seen an increase in social networks mushrooming everywhere and a growing reliance on digital government services. All these have resulted in a growing range of cyberthreats from different sources, including foreign powers, terrorists and criminals.

On the other side, according to the literature discussion in Chapter 2, increased access to the Internet has resulted in an increase in cybercrimes, cyberattacks, theft of personal information and cyberbullying, to mention a few, as echoed by Sutherland (2017). These are not only threats towards governments but even common citizens who are simply trying to connect to the Internet to apply for jobs; to use communication tools, such as emails; or to have access to the vast number of social platforms that are all over the Internet, including Facebook, Twitter and Instagram.

Through the broadband expansion projects, people access the Internet and if they are not properly trained on proper usage and how to protect themselves in the cyberspace, they become prone to different types of cyberattacks, ransomware and data theft, for example.

Following on the work of de Bruijn and Janssen (2017), the research findings concur that, as much as there are many benefits of broadband expansion, users are not necessarily cyber ready to safely enjoy broadband access without becoming victims of cyberattacks and cybercrime, as well as data and identity theft. The major reason for the lack of readiness and awareness regarding cybersecurity emanates from the absence of suitable cybersecurity policies governing cybersecurity at different levels. It is important to ensure that when users achieve Internet access, they are correctly trained and educated.

The respondents believed the expansion of broadband access to previously disadvantaged communities has resulted in improved access to broadband, improving user productivity and, in the process, creating dependence and reliance on the Internet for many things, digital government services included. On the other hand, however,

users do get broadband access to the Internet and begin to experience the many benefits of Internet access, but they will not necessarily be cyber ready.

#### **5.3.4 Effective cybersecurity governance for broadband expansion projects**

Research sub-question 4: What is effective cybersecurity governance for broadband expansion projects?

The researcher sought to understand what constitutes effective governance for broadband expansion projects.

*“User awareness and hardware and software protection are the two tools that should be used in conjunction to ensure cybersecurity. If users are aware and responsible, this also protects the network. We need good monitoring software to monitor users’ activities online” (C1.1).*

On the other hand, some respondents indicated that:

*“Even though we do not have a proper framework or strategy that speaks to cybersecurity, we believe that it is important to have immaculate and cutting-edge technology to protect the hardware and software against cyberthreats. That alone is however not adequate, the users in the system that get broadband access through our community broadband project need to be trained on good practice.” (C.2.1).*

*“There is need for a good cybersecurity awareness training programme for user engagement and equipping the users” (C2.2).*

Adding to the discussion, another respondent said that:

*“We need to have effective monitoring software that allows you to monitor network traffic and user logs and to align users and their logs whilst they are busy. We need to have intrusion detection and intrusion prevention systems that help to identify and immediately block malicious traffic from entering our network. We need software that enable us to see what users are busy with and immediately block certain sites that pose as harmful to our users. Users also need to be trained to be cyber-safe” (C3.1).*

A respondent from C4 said:

*“We need effective policies that users should adhere to when they access the Internet through our infrastructure. We need good anti-virus software to protect our hardware and software from malware. We need an efficient firewall to monitor traffic and block unwanted traffic from entering our network and policies that speak to good practices and usage” (C4.1).*

The interviewees agreed on the importance of cybersecurity governance. The responses indicate the need for top-notch security solutions and policies, ensuring that users are secure. There is a need for balance between cybersecurity administration and user awareness.

Cybersecurity, in most cases, is related to developing the best technology that can be used to decrease, or even eliminate, cybersecurity threats and risks; to protect the hardware and software. However, very little is done about the training of the stakeholders who are involved in cybersecurity, be it as users or as support staff.

From the literature review conducted by the researcher and all the data collected, it becomes quite evident that there is a need for a balance between network, information and system security, as well as user awareness. Consistent adequate training regarding cybersecurity for people involved in cybersecurity is important.

As far as combating cybersecurity risks and threats is concerned, according to the literature reviewed the focus is almost always on the cutting-edge technology. So much effort by companies is put into safeguarding hardware and software against cyberthreats that a blind eye is turned towards the engagement and training of users. Protecting hardware and software against cyberthreats alone is inadequate.

There should be adequate and functional security and usage policies regarding Internet access and usage. Policies to control user access should be strictly implemented. It is also important to install usage monitoring software to monitor how users are using the Internet in order to identify and address problems before they start.

The user devices that are brought onto and used on the network need monitoring to ensure that they have updated antivirus software, for example. It is crucial to have an ‘always-on’ firewall on the network that inspects and monitors network traffic into and out of the network to block malicious traffic from entering the network.

It is imperative to monitor user activities and devices that are used on the network; however, it is more vital to train users on good cybersecurity practices to keep the network safe and secure, and also for users to protect themselves and be cybersafe.

### **5.3.5 Lack of cybersecurity governance strategies**

Research sub-question 5: What are the results of lack of cybersecurity governance strategies at broadband expansion projects?

The researcher was interested to know what the implications of lack of cybersecurity governance strategies at community broadband projects were.

*“Ransomware, one of our staff actually experienced that and they lost all their data on the computer as they could not pay the requested money, data theft, identity theft, malware attacks” (C1.1).*

*“Catfishing, cyberattacks, identity theft, data theft and breach, malware attacks, phishing” (C2.1).*

*“Users will be vulnerable to a long list of cyberthreats, data loss, identity theft, phishing, just to mention but a few” (C3.2).*

*“It is a long list of cyberthreats that often mature into attacks. The list can include phishing, spear-phishing, ransomware, data theft, identity theft, malware attacks, catfishing” (C4.1).*

The responses above revealed the horrendous possibilities that come into play when there is an absence of appropriate cybersecurity governance measures in broadband expansion projects. According to reports by SAPA (2013) and BusinessTech (2014) discussed in Chapter 2, there are many victims of cybercrime in South Africa. South Africa was ranked third globally on the list of the number of cyber victims, with Russia and China topping that list for the year 2013.

The Cybercrimes Act has provisions to ensure that cybersecurity perpetrators are charged and jailed, if need be, which is a very positive move on the path to reducing cyber offences, cyberattacks and cybercrimes.

Because of the absence of clear legal requirements as far as reporting cybercrimes is concerned, cybercrime in South Africa has not been quantified as of 2015. However,

research does indicate that there are many victims of cybercrime in South Africa. There is a clear need for effective cybersecurity governance in community broadband projects or else cyberattacks and cybercrimes will increase.

Williams (2019) stresses the importance of having a structure and strategies that deal with cybersecurity, stating that, in the absence of security strategies, cyberattacks are most likely to happen and the organisation will take long to respond to and to address such threats. Broadband expansion and the increase in Internet usage fuelled by the current advancements in technology have seen cybersecurity becoming complex and very challenging. Hackers, attackers, and scammers to take advantage of the ignorance and vulnerabilities to launch successful cyberattacks (Mashiane et al., 2019). The researcher sought to understand the status of cybersecurity governance in practice at broadband expansion projects from the research respondents.

5.3.6 Cybersecurity awareness and training Research sub-question 6: How can cybersecurity awareness and training help alleviate occurrences of cyberattacks and cybercrimes?

The researcher sought to understand how cybersecurity awareness and training helps to alleviate occurrences of cyberattacks and cybercrimes.

All the respondents shared the same views and the researcher combined them together as follows:

- Reduced costs related to cyber-related loss-incidents on users as well as the institution providing broadband access
- Time that can potentially be wasted on post cybersecurity incidents by trying to understand what transpired as well as restoring service
- Reduced possibility of occurrence of cybersecurity related risks
- Reduced cases of data and information theft
- Enable users protect themselves against cyberattacks and respond to cyberthreats

The responses indicate that cybersecurity awareness training for users has tremendous benefits that vary from one environment to another. Some of these benefits include reducing cyberthreats and the vulnerability of users. Cybersecurity awareness will ensure that users are more careful when using computer systems and the Internet. This will reduce cybersecurity incidents and the costs and effects

associated with them. As a result, time wasted post-cybersecurity incidents on gathering facts on what occurred, taking corrective action and dealing with recovery is saved.

User training promotes increased compliance to legislation as users become knowledgeable and aware of the reasons why there is certain legislation in place and the repercussions of lack of compliance. Education is power. This is in line with what Chandarman (2016) indicated, cybersecurity awareness is a very important aspect of the protection of people and systems and there is a need for user awareness and training to achieve cybersecurity.

More studies have been conducted by other academics over time and they indicate the possibility of misalignment between cybersecurity attitudes, knowledge and behaviour. It is, thus, imperative that there are relevant and appropriate cybersecurity training and awareness initiatives implemented in different communities. Clearly, there is no one size fits all as far as cybersecurity is concerned. There is a need for a cybersecurity governance framework that addresses community broadband expansion and emphasises the need for proper, adequate, relevant and appropriate cybersecurity training and awareness.

#### **5.4 Summary of findings**

By and large, after presenting the findings of this study, the researcher concludes that more needs to be done regarding cybersecurity. Most issues that were raised in the above discussion require solutions. In Chapter 5, the researcher has sought to clarify the research findings in relation to the research questions and the identified research objectives. There is a serious need to consider user training in community broadband projects. A framework that ensures a balance between network security, information security, data security and user training and awareness is the ideal framework to ensure cybersecurity governance in broadband expansion projects.

People are the weakest link in cybersecurity, hence, there is a need for a cybersecurity governance strategy that focuses on humans who are the users in the system; governance strategies that empowers, equip and adequately train the user (Ramluckan, 2019). In this light, the researcher concurs that there is a need for cybersecurity awareness, training and education that is appropriate, relevant and directly addresses broadband expansion projects.



Quite a few projects are currently in place and broadband access is, indeed, spreading all over the country. The literature reviewed indicates that, over the years, more and more people have gained broadband access, not just in South Africa, but globally (Wallace & Philip, 2019). Cybersecurity is a growing concern in South Africa in both the public and private sector and there is in urgent need of an appropriate and effective strategy to curb cyberthreats, to educate users and to create cybersecurity awareness. To achieve cybersecurity in any environment there is a need for all components involved, namely people, processes and technology, to complement one another in the creation of an effective defence system (Grobler, Jansen van Vuuren & Zaaiman, 2011).

The comments by Pretorius and van Niekerk (2015) indicate that the challenge is the fact that cybersecurity approaches concentrate mostly on the best technology that can be used to decrease, or even eliminate, cybersecurity threats and risks, and protect hardware and the software, but very little is done regarding training and the management of users and support staff involved in cybersecurity. All these factors culminate in the rather urgent need for a cybersecurity governance strategy for community broadband expansion projects, on the rise in South Africa, to ensure the safety and protection of users, ordinary South African citizens and the IT infrastructure granting them broadband access.

Indeed, broadband providers have strategies in place, but the emphasis seems to be only on network security or, rather, ensuring that the networks and the infrastructure is secure. Little is in place to ensure user awareness and engagement (Jones et al., 2019). Several academics who have conducted research in the same area concur that the effectiveness of cybersecurity should be a collective effort, both on the side of cybersecurity administration and on the side of user awareness (Jones et al., 2019; Eeten et al., 2019; Cecil et al., 2019). In this chapter, a literature review and analysis provided the theoretical underpinning for this study.

To date, in South Africa, cybersecurity regulation is being enforced though provisions contained in the Electronic Communications and Transactions Act 25 of 2002 (ECTA) (South African Government Gazette, 2018). In 2002 a South African law was promulgated to regulate the interception of communications, together with related processes. This law now gets further support from the Cybercrimes Act, which has the primary objective of imposing penalties that have a bearing on cybercrime; to

criminalise the distribution of data messages that are harmful; to provide for interim protection orders; to further regulate jurisdiction in respect of cybercrimes; to further regulate the powers to investigate cybercrimes; to further regulate aspects relating to mutual assistance in respect of the investigation of cybercrime; to provide for the establishment of a twenty-four hours a day seven days a week point of contact; to further provide for the proof of certain facts by affidavit; to impose obligations on electronic communications service providers and financial institutions to assist in the investigation of cybercrimes and to report cybercrimes; to provide for the establishment of structures to promote cybersecurity and capacity building; to regulate the identification and declaration of critical information infrastructures and measures to protect critical information infrastructures; to provide that the Executive may enter into agreements with foreign States to promote cybersecurity; to delete and amend provisions of certain laws; and to provide for matters connected therewith (South African Government Gazette, 2018).

There is need for a joint approach to cybersecurity governance and protection and it should include hardware and software protection as well as providing adequate training for people involved in cybersecurity. According to the literature review and data collected from various cases, the consensus that emerges is that user engagement, awareness training and education are vital for cybersecurity as well as to eliminate poor online security behaviour.

## **5.5 Chapter summary**

In this chapter, data collected was presented and analysed. The results were presented using quotes from the respondents. References to other researchers were also highlighted where necessary. The degree to which the research questions and problem statements have been achieved from the findings, as well as conclusion drawn from the information gathered from the interviews, will be emphasised in the next chapter.

## CHAPTER 6: CONCLUSIONS, LIMITATIONS AND RECOMMENDATIONS

### 6.1 Overview

This chapter concludes this study by providing specifics about the research implications. It also details the input of this study and recommendations informed by the findings and conclusion that the researcher considered to be potentially useful to academia and policy makers.

The main research question to achieve the research, aim and objective was formulated as follows: - What is effective governance for broadband expansion projects?

### 6.2 Summary of chapters

This study is summed up in six chapters as follows:

*Chapter 1:* The research problem statement was thoroughly discussed to provide motivation on the importance of this research study in this chapter. Considering the problem statement, in South Africa it is evident that the current legislation does not make direct and specific provision for cybersecurity governance in broadband expansion projects at community level, as affirmed by the South African Government Gazette (2015). From the problem statement, the research objective was formulated, which was to examine how cybersecurity legislation in South Africa is adopted and applied on broadband expansion projects. Chapter 1 presented a preliminary discussion on the research questions and objectives; the research procedures followed; and concluded with a summary of the study.

*Chapters 2 and 3:* These chapters presented the hypothetical outline of the study. In Chapter 2 an in-depth literature review was presented that focussed on the concepts related to cybersecurity; broadband expansion projects; cybersecurity policies and governance strategies; community broadband project governance; and other related matters, such as cybersecurity awareness, cyberthreats, training, and education, together with their impact on community broadband expansion initiatives. In Chapter 3, the research design and methodology were discussed, outlining how the study was conducted and how data was collected.

*Chapter 4:* This chapter provided a description of the multiple cases used in this study. It also included the data collection methods, case by case.

*Chapter 5:* This chapter provided an analysis, discussion, presentation and interpretation of the collected data and results. The relevant recommendations and conclusions will be derived.

### **6.3 Inferences of the study**

*First objective:* The first objective was to review and evaluate how cybersecurity legislation in South Africa is adopted and applied in broadband expansion projects. According to literature gathered and the findings in Chapter 5, each of the sites under observation, indeed, have their own policies and strategies that have been implemented. Respondents did not mention the national legislation at any time, and how they deduce policies implemented is evidence that legislation exists on a high level and does not address issues related to their projects. As much as there is legislation in place, enforced at national level, this legislation is not being complied with at community level.

*Second objective:* The second objective was to review and evaluate cybersecurity governance strategies currently in existence that support broadband expansion projects. From the findings in Chapter 5, based on the responses to the interview questions, there are many solutions being implemented for security. That being the case, it can be concluded that there is no one size fits all scenario in cybersecurity. Two respondents mentioned that whatever policy is in place is customised to suit the organisation's budget and hardware. Network monitoring solutions are used to ensure that users and devices are registered and profiled, which provides streamlined network visibility and policy enforcement that makes it easy to manage, monitor and control user and device network access and activities. However, all these options leave the human element still vulnerable to cyberattacks as they do not ensure that users are cyber aware or informed on good practices regarding cyber usage.

*Third & fourth objective:* These objectives were to investigate cybersecurity threats and risks that arise during the implementation of broadband expansion projects and the cybersecurity challenges faced by broadband expansion projects. According to the research findings, there are many benefits to broadband expansion. As respondents from all the sites agree, more and more people who did not have access to Internet

before, now have access and there is also an increase in the number of users who bring their own devices to sites to connect to the network. From the evidence, however, users are not cyber ready and often leave passwords on shared computers. This hinders the objective to ensure safety and broadband access without users becoming victims of cyberattacks and cybercrime or data and identity theft. The major reason for the lack of readiness and awareness regarding cybersecurity emanates from the absence of suitable cybersecurity policies governing cybersecurity at different levels. It is extremely important to ensure that, when users get Internet access, they are properly trained and educated.

*Fifth objective:* The fifth objective of this research was to understand what more can be done beyond what is already being implemented to improve the governance of cybersecurity in broadband expansion projects. Apart from having state of the art IT technologies and solutions for cybersecurity, it is imperative that there are relevant and appropriate cybersecurity training and awareness initiatives available in the different communities. Clearly there is no one size fits all as far as cybersecurity is concerned. There is a need for a cybersecurity governance framework that addresses community broadband expansion and emphasises the need for proper, adequate, relevant and appropriate cybersecurity training and awareness.

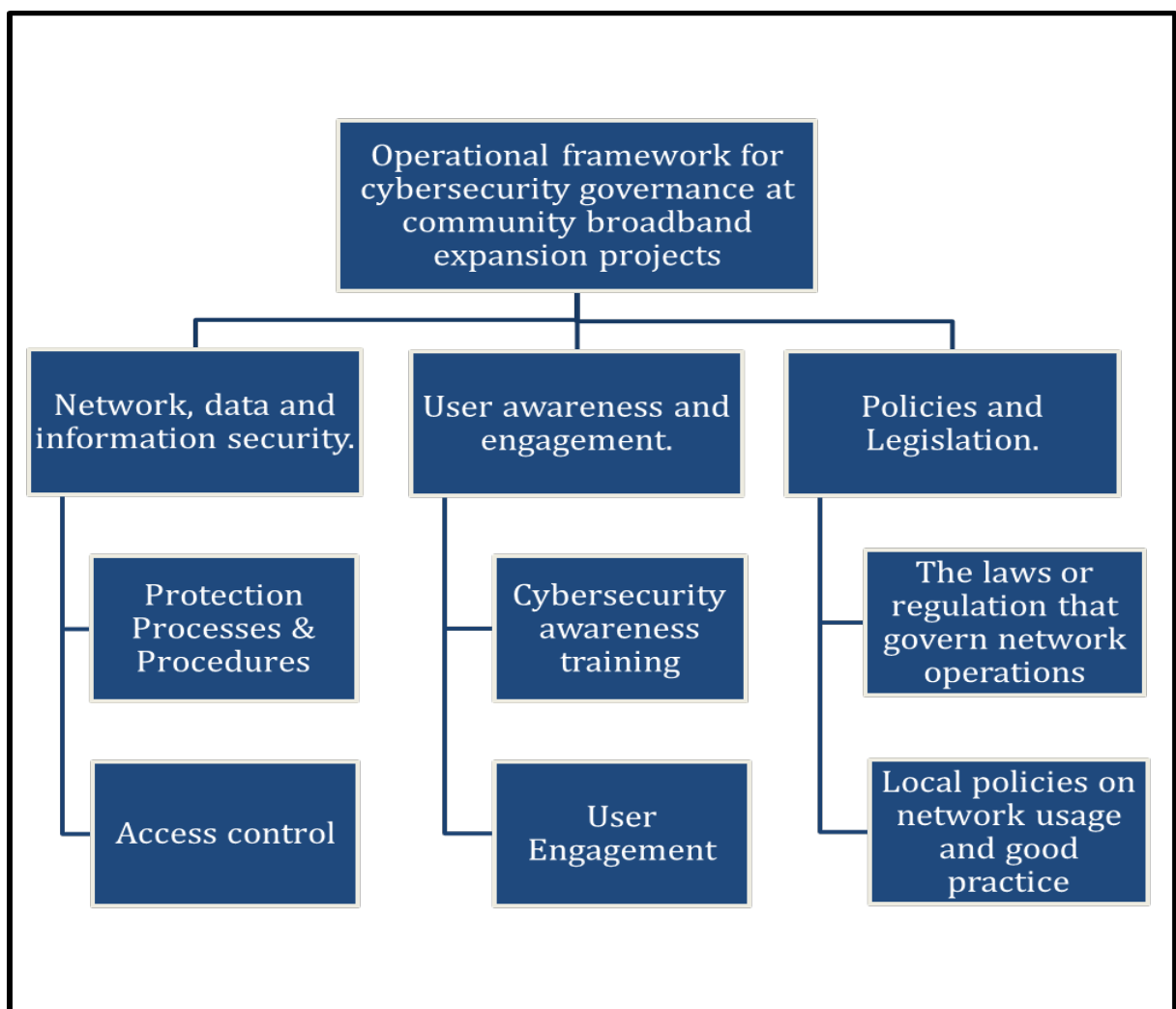
*Sixth objective:* The sixth objective was to understand the implications if there is no proper or effective cybersecurity governance in community broadband projects. From the research findings discussed in Chapter 5, if there is no effective cybersecurity governance at broadband expansion projects, cyberattacks and cybercrimes will increase. There is the need for a balance between network, information and system security, on the one hand, and user awareness, on the other. Consistent adequate training regarding cybersecurity for users and support staff is important. Securing computer systems alone is inadequate.

#### **6.4 Recommendation**

The researcher recommends the establishment of an operational framework that informs appropriate cybersecurity practices on broadband expansion projects is an expected outcome of this research. This framework will potentially be used by broadband expansion projects to implement effective cybersecurity governance strategies. This operational framework will potentially assist in bridging the gap that seems to be there between cybersecurity policies and legislation approved and

implementation and could be adopted by broadband expansion projects for strengthening cybersecurity and best practices. There is a need for a project specific operational framework, as opposed to the adoption of generic frameworks because these have become insufficient to train and educate users and to create awareness, according to the study conducted by Chandarman (2016). An evaluation of the target population is vital prior to crafting an operational framework to explicitly identify the cybersecurity awareness inadequacies of the target population.

Figure 6.1 illustrates a potential operational framework that can be adopted by broadband expansion projects for strengthening cybersecurity and best practices.



**Figure 6.1: The Proposed Operational framework  
(Source: Researcher)**

#### **6.4.1 Description of the operational framework**

The operational framework illustrated in Figure 6.1 addresses all the aspects of security without overemphasis on some of the aspects and side-lining others. An operational framework should address network, data and information security; user awareness and engagement; as well as policies and the legislative aspects of cybersecurity. The framework should inform best practices and guide the usage of resources, as well as stipulate adequate and appropriate procedures and user engagement in community broadband expansion projects.

#### **6.4.2 Network, data and information security**

The primary mission of network, data and information security programs is to secure organizational information assets and ensure they remain secured, reliable, available as well as useful. Information assets include:

- Data and information
- Operational procedures
- Hardware
- Software
- Communication networks
- People

As part of network, data and information security programs, access control systems and methods are used to enable systems to specify which users who may use a particular resource and how they may use it in a system. The four functions of access control are:

- Identification of users of a system ideally with logon credentials (usernames and passwords)
- Authentication of the user to access the network/system
- Authorization of users to access and use specific resources in specific ways
- Accountability of users in a system to track their activities.

Access control mechanisms are put through to protect the system and network resources and not necessarily the user.

As much as network, data and information security are crucial, it is critical to consider the weakest link in any security solution, which is the human factor.

### **6.4.3 User awareness and engagement**

From the study, it can be concluded that user awareness, training and engagement should be given the same priority as all other aspects of security. The user needs to be aware of the risks, threats and vulnerabilities that are found within the cyberspace in the organisations in which they operate. This is the kind of awareness that they require, and they also need to be adequately and appropriately trained to ensure their personal security, as well as the security of the network and resources at their disposal.

Cybersecurity awareness campaigns to educate users with the knowledge to interact safely online are indisputably vital to a secure foundation in cybersecurity. There is a need for appropriate and relevant cybersecurity awareness, training and education campaigns that need to focus on broadband expansion projects. The basis of these cybersecurity awareness, training and education campaigns should be local policies, procedures and perceived threats. There is a need for emphasis to ensure that users take responsibility for and understand their role in securing their information and computer systems. Users need to be trained and it is of the utmost importance that the training be simple, clear and easy to understand, with the training material benchmarked against best practices and continuously updated to remain relevant.

For policy and legislation to be enforced and be effective these five things are vital:

- Policies and legislation need to be disseminated so users have access to them
- Users need to read and review the policies and legislation
- Users need to understand the policies and legislation
- Users need to comply with the policies and legislation
- There should be uniform enforcement of the policies and legislation

When broadband expansion projects are initiated, it is important that policies are put forward to form the basis of cybersecurity as legislation can tend to very high level and not address the requirements of these projects. These policies are meant to be communicated to users once they are registered on the institutional databases and can access broadband access provided through these projects. However, this rarely happens. Users do not access these policies that can potentially assist them to ensure that they are cybersafe and aware.



Having policies and legislation is one thing, for them to be effective user awareness and training comes into play, users need to be educated and trained on the importance of security.

#### **6.4.4 Policies and legislation**

Security policies function as organizational laws that determine acceptable behaviour within an organization and they need to be crafted and implemented with care to ensure they are complete, appropriate, and fairly applied to everyone within a specific organization. Policies relating to cybersecurity are put into use at organisational level to ensure cybersecurity. Legislation refers to rules that mandate or prohibit certain behaviour and are enforced by the state, it is important that the legislation has realistic provisions for enforcement else it remains top-level laws that are not exactly useful. Local policies on network usage and good practice should be formulated and implemented in the fight of cybersecurity.

The researcher drew inspiration to formulate the recommended operational framework from the NIST Cybersecurity Framework for Improving Critical Infrastructure Cybersecurity (NIST, 2019). This is a US government guidance framework for private sector organisations owning, operating or supplying critical infrastructure. The recommended operational framework should be a uniform set of best practices, standards and recommendations that help community broadband projects to improve cybersecurity measures.

The operational framework could potentially assist to strengthen cybersecurity as it should not only emphasise one aspect of security because many other solutions do just that by focussing attention on network, data and information security only. There is need for balanced policies, user training and awareness, as well as network security, in order establish a more formidable cybersecurity solution.

After conducting this study, the researcher discovered that there is no generic cybersecurity solution and that, to achieve good results, there is a need for a unique framework that applies to specific projects or organisations that experience the same security threats, risks and vulnerabilities. For the proposed operational framework to be effective there is a need for enforcing compliance with it and having guidelines in place for best practice implementation. It is one thing to have an operational framework in place for good practice, but it is another thing again for such a framework to be

complied with, hence, compliance is crucial. Furthermore, it is of critical importance that there be a customised operational framework available that directly addresses the needs of individual organisations.

To remain relevant, this study recommends that the operational framework indicated in Figure 6.1 should be continually improved, with advancements in technology and for it to remain useful and relevant.

### **6.5 Research limitations**

In assessing the findings of this study, it is important to note that the study had its own limitations. It took a long time before the researcher was granted access to collect data from the initial case that was to form the basis for the study. The researcher spent over a year trying to get consent and to set up appointments to no avail. Eventually the researcher was given access to the site, but the data collected was insufficient for a master's degree, hence the researcher had to undertake further research and decided to use three more sites that are also involved in broadband expansion. It was not easy to get people to interview as the relevant people were involved in the security side of the broadband expansion projects.

One of the challenges the researcher encountered was to locate an accurate sample for the study. This was a daunting challenge; hence, the researcher resorted to using convenience sampling to generate the initial sample. Future studies in this research area could, potentially, use other sampling techniques. Another limitation was the method of data collection because the researcher relied solely on the responses of the respondents. The responses could have been biased.

There is a lack of a benchmark standards and a framework for cybersecurity governance in broadband expansion projects that addresses issues of network, computer and information security. This poses a threat to users in the affected communities (Jansen van Vuuren, Phahlamohlaka, & Leenen, 2012).

### **6.6 Future research**

Future research should be geared towards:

- i. Investigating the attitudes and behaviours of Internet users. The researcher sees it important that the attitudes and behaviours of Internet users be investigated as this is important for developing a cybersecurity culture in any

community. The attitudes and behaviours of users contribute to making them vulnerable to cyberattacks and cybersecurity; therefore, it is important for this to be investigated to determine adequate ways in which to ensure protection of these users.

- ii. Investigating the contribution of user awareness and training towards improving cybersecurity. The researcher concluded from this study that cybersecurity is not achieved by employing top notch controls, mechanisms and strategies, but is achieved by addressing the weakest part of any system, the user. That said, user awareness and training are major contributors to improving cybersecurity. More research should be done to determine just how much user awareness and training can improve cybersecurity and how best these can be done to ensure the best results.
- iii. Investigating the intensity of cybercrimes, cyberattacks and cyberthreats in South Africa. The research discovered that cybercrimes, cyberattacks and cyberthreats are on the increase in South Africa, which ranks high on the list of cyber victims, according to various sources consulted and referenced in this study. It is imperative that studies are conducted to discover the intensity of cybercrimes, cyberattacks and cyberthreats in South Africa and their effects on South African communities, as well as on the country's economy. This will help to build a solid national cybersecurity culture.
- iv. Validation of the proposed operational framework for cybersecurity governance in broadband expansion projects. In this study, an operational framework for cybersecurity governance in broadband expansion projects was proposed. It is important that further research be conducted to validate the framework.

## **6.7 Contributions of the research**

Cybersecurity is a fundamental aspect of ICT globally (Wallace & Philip, 2019). Because of broadband expansion, more and more people are connecting to the Internet and using cyber resourcing; even becoming dependant on them, it is, therefore, important that users acquire cybersecurity knowledge and skills as attackers take advantage of user ignorance and launch successful cyberattacks. Popular and recent cyberthreats are the Facebook data privacy scandal, Ster-Kinekor and ViewFines license scam, to mention a few (Mohapi, 2018; Niselow, 2018; Shapshak, 2018). This is a clear indication of how crucial it is to ensure systems are

technologically secure and the importance of training users and making them cyber aware, so they can defend themselves should cyberattacks occur.

Unfortunately, South Africa is yet to implement an effective cybersecurity governance framework that can be adopted and utilised by similar broadband projects. Williams (2019) suggests that there seems to be a focus at a national level only, which neglects broadband projects. That being the case, it is important to reveal the shortfalls of current cybersecurity governance strategies resulting from lack of an effective cybersecurity governance framework that directly address the needs of broadband expansion projects. This may be achieved by means of the outcomes of this research study.

The outcome of this study is an understanding of cybersecurity governance of broadband projects in South Africa. Broadband expansion could cause potential harm to the community if nothing is done to ensure security and protection of users, network systems, user devices and data (Jansen van Vuuren, Grobler, Leenen & Phahlamohlaka, 2014).

## **6.8 Chapter summary**

Briefly, this chapter has concluded the study by drawing conclusions from the findings and proposing recommendations based on these conclusions. Conclusions from this research were based on the research findings presented, analysed and discussed in Chapter 4. The findings and conclusions informed the recommendations. The contribution of the current study, limitations of this research and suggested areas that future research could focus on were mentioned.

This study explored the emphasis on cybersecurity governance in broadband expansion projects. From the literature review conducted, it is evident that the current legislation does not make direct and specific provision for cybersecurity governance in broadband expansion projects.

## REFERENCES

- Abdulrauf, L.A. 2020. *Data protection in the Internet: South Africa*. Cham: Springer International.
- Abiodun, O.P., Anderson, D. & Christoffels, A. 2020. *Exploring the influence of organizational, environmental, and technological factors on information security policies and compliance at South African higher education institutions, with a focus on implications for biomedical research*. *Multidisciplinary Digital Publishing Institute Proceedings*, 45(1):2.
- Academy of Science of South Africa. 2020. *The Smart City initiatives in South Africa and paving a way to support cities to address frontier issues using new and emerging technologies*. <http://dx.doi.org/10.17159/assaf.2019/0059>.
- Adams, R., Fourie, W., Marivate, V. & Plantinga, P. 2020. *Introducing the series: Can AI and data support a more inclusive and equitable South Africa?* Report for the Policy Action Network (PAN) Topical Guides: AI & Data Series 1, March.
- Ahmed, S.R. 2020. *Preventing identity crime: Identity theft and identity fraud: an identity crime model and legislative analysis with recommendations for preventing identity crime*. Brill.
- Balakrishna, P. & Soman 2020. Deep learning approach for enhanced cyber threat indicators in Twitter Stream. *arXiv preprint arXiv:2004.00503*.
- BDO. 2016. *BDO Launches cyber and forensic lab to help combat cyber related crimes*. [Online]. Available at: <https://www.bdo.co.za/en-za/insights/2016/insights/bdo-launches-cyber-and-forensic-lab-to-help-combat> [Accessed: 10 September 2016].
- Bernard, H.R. 2006. *Research methods in anthropology: Qualitative and quantitative approaches*. 4<sup>th</sup> ed. New York: Altamira Press.
- Betts, L.R. 2018. *The nature of cyber bullying behaviours*. In *Encyclopedia of Information Science and Technology*. 4<sup>th</sup> ed. IGI Global: 4245-4254.
- Bidram, A., Poudel, B., Damodaran, L., Fierro, R. & Guerrero, J.M. 2019. *Resilient and cybersecure distributed control of inverter-based islanded microgrids*. *IEEE Transactions on Industrial Informatics*, 16(6):3881-3894.
- Bingham, S.J. 2019. *2019. Malware detection and prevention system. Level 3 communications LLC*. US Patent Application 16/259,164.
- Bote, D. 2019. *The South African National Cyber Security Policy Framework: A critical analysis*. Doctoral dissertation, North-West University, South Africa.
- Bure, M. & Tengeh, R.K. 2019. *Implementation of internal controls and the sustainability of SMEs in Harare in Zimbabwe*. *Entrepreneurship and Sustainability Issues*, 7(1):201-218.

- BusinessTech. 2014. *Internet fraud and phishing costs SA R2.2 billion*. September 14. [Online]. Available at: <http://businesstech.co.za/news/general/68212/sa-internet-fraudand-phishing-costs-r2-2-billion> [Accessed: 5 February 2019].
- Cardona, M., Schwarz, A., Yurtoglu, B.B. & Zulehner, C. 2009. Demand estimation and market definition for broadband Internet services. *Journal of Regulatory Economics*,
- Cecil, J., Gupta, A., Pirela-Cruz, M. & Ramanathan, P. 2019. *An IoMT based cyber training framework for orthopaedic surgery using next generation internet technologies*. ScienceDirect.
- Chadwick, D.W., Fan, W., Costantino, G., De Lemos, R., Di Cerbo, F., Herwono, I., Manea, M., Mori, P., Sajjad, A. and Wang, X.S., 2020. *A cloud-edge based data security architecture for sharing and analysing cyber threat information*. *Future Generation Computer Systems*, 102, pp.710-722.
- Chandarman, R. 2016. *Cybersecurity awareness of students at a private higher education institute in South Africa*. Master's Dissertation, University of KwaZulu-Natal, Westville, Durban.
- Chuprova, D., Gudkova, S. and Marinets, I., 2019, October. *Personnel safety as a tool for leadership in public administration*. In 4th International Conference on Social, Business, and Academic Leadership (ICSBAL 2019) (pp. 51-55). Atlantis Press.
- Cisco. 2019b. *Cisco identity services engine data sheet*. [Online]. Available at: <https://www.cisco.com/c/en/us/products/collateral/security/identity-services-> [Accessed: 6 February 2019].
- CLIR. 2004. *E-Powering the People: South Africa's Smart Cape Access Project*. Available at: <https://www.clir.org/pubs/reports/pub125/>. [Accessed: 30 June 2018].
- Craigen, D., Diakun-Thibault, N. & Purse, R. 2014. *Defining cybersecurity*. *Technology*
- Dahabiyeh, L., 2021. *Factors affecting organizational adoption and acceptance of computer-based security awareness training tools*. *Information & Computer Security*.
- Da Veiga, A. 2019. Achieving a security culture. In *Cybersecurity education for awareness and compliance*. IGI Global, 72-100.
- De Bruijn, H. & Janssen, M. 2017. *Building cybersecurity awareness: The need for evidence-based framing strategies*. *Government Information Quarterly*, 34(1):1-7.
- De Bruin, R. & Von Solms, S.H. 2016. *Cybersecurity Governance Maturity Model: A look at current maturity affairs*. *Proceedings*. The Global Humanitarian Technology Conference (GHTC 2016), Seattle, Washington, USA, 13-16 October 2016.

- Dean, B. 2016. *Natural and quasi-natural experiments to evaluate cybersecurity policies*. *Journal of International Affairs*, 70(1):139-160.
- Dennehy, R., Meaney, S., Walsh, K.A., Sinnott, C., Cronin, M. & Arensman, E. 2020. *Young people's conceptualizations of the nature of cyberbullying: A systematic review and synthesis of qualitative research*. *Aggression and Violent Behavior*, 101379.
- Dennehy, R., Meaney, S., Cronin, M. and Arensman, E., 2020. *The psychosocial impacts of cybervictimisation and barriers to seeking social support: Young people's perspectives*. *Children and youth services review*, 111, p.104872.
- Dickson. S & Bokhari. B. 2016. *Cyberspace – the world's largest crime zone - why it is essential for South Africa to establish and implement cybersecurity measures and legislation*. [Online]. Available at: <https://www.cliffedekkerhofmeyr.com/en/news/publications/2016/Technology/technology-and-sourcing-alert-11-may-cyberspace-the-worlds-largest-crime-zone-why-it-is-essential-for-south-africa-to-establish-and-implement-cybersecurity-measures-and-legislation-.html> [Accessed: 12 August 2016].
- Diwan, T.D., 2021. *An investigation and analysis of cyber security information systems: latest trends and future suggestion*. *INFORMATION TECHNOLOGY IN INDUSTRY*, 9(2), pp.477-492.
- Dlamini, I.Z., Taute, B. & Radebe, J. 2011. *Framework for an African policy towards creating cybersecurity awareness*. South African Cyber Security Awareness Workshop (SACSAW) 2011, Gaborone, Botswana, 12 May 2011.
- Dlamini, Z. & Modise, M. 2013. *Cybersecurity awareness initiatives in South Africa: a synergy approach*. 7th International Conference on Information Warfare and Security, University of Washington, Seattle, USA, 22-23 March 2012
- Doyle, K. 2015. *SA security policy trails Africa*. *IT Web*. May 19. [Online]. Available at: [http://www.itweb.co.za/index.php?option=com\\_content&view=article&id=143303](http://www.itweb.co.za/index.php?option=com_content&view=article&id=143303) [Accessed: 17 May 2017].
- Durodolu, O.O. & Mojapelo, S.M. 2020. *Contextualisation of the information literacy environment in the South African education sector*. *Electronic Journal of e-Learning*, 18(1):57-68.
- Dwivedi, S., Vardhan, M. & Tripathi, S. 2020. *Incorporating evolutionary computation for securing wireless network against cyberthreats*. *The Journal of Supercomputing*, 76(3): 6-38.
- Etikan, I. Musa, S.A. & Alkassim, R.S. 2016. *Comparison of convenience sampling and purposive sampling*. *American Journal of Theoretical and Applied Statistics*, 5(1):1-4.
- Fichardt. C. 2015. *Just how big a threat is cybercrime to SA?* [Online]. Available at: <http://www.bdlive.co.za/business/technology/2015/06/08/just-how-big-a-threat-is-cybercrime-to-sa> [Accessed: 10 September 2016].

- Fontana, A. & Frey, J. 1994. The art of science. *The handbook of qualitative research*, 361376.
- Gcaza, N. & Von Solms, R. 2017. *A strategy for a cybersecurity culture: A South African perspective. The Electronic Journal of Information Systems in Developing Countries*, 80(1):1-17.
- Goddard, W. & Melville, S. 2004. *Research methodology: An introduction*. 2<sup>nd</sup> ed. USA: Juta and Company.
- Grobler, M., Jansen van Vuuren, J & Leenen, L. 2011. *Implementation of a Cyber Security Policy in South Africa: Reflection on progress and the way forward*. [Online]. Available at: [https://www.researchgate.net/publication/290617492\\_Implementation\\_of\\_a\\_Cyber\\_Security\\_Policy\\_in\\_South\\_Africa\\_Reflection\\_on\\_Progress\\_and\\_the\\_Way\\_Forward](https://www.researchgate.net/publication/290617492_Implementation_of_a_Cyber_Security_Policy_in_South_Africa_Reflection_on_Progress_and_the_Way_Forward). 10th IFIP TC9 International Conference on Human Choice and Computers, HCC10 2012At: Amsterdam, Netherlands . September 2012. [Accessed: 8 September 2016].
- Grobler, M., Jansen van Vuuren, J. & Zaaiman, J. 2011. *Evaluating cybersecurity awareness in South Africa*. [Online]. Available at: <https://researchspace.csir.co.za/dspace/handle/10204/5108?show=full>. Proceedings of the 10th European Conference on Information Warfare and Security. The Institute of Cybernetics at the Tallinn University of Technology Tallinn, Estonia, 7-8 July 2011, pp 9pp
- Gudkova, D., Vergelis, M., Shcherbakova, T., & Demidova, N. (2018). *Spam and phishing in 2017*. Securelist (2018).
- Helyes, M., 2021. *Cyberterrorism and the protection of critical information infrastructures: A snapshot of the current state of certain regulatory issues*. *Lélektan és hadviselés*, 3(1), pp.51-68.
- Henriques, D., Pereira, R., Almeida, R. & Da Silva, M. 2020. *IT governance enablers: A systematic literature review*. *Foresight and STI Governance* 14(1):48-59
- Hollstein, B., 2011. *Qualitative approaches*. The Sage handbook of social network analysis, pp.404-416.
- International Telecommunication Union ( ITU ) World Telecommunication/ICT Indicators Database. *Increase in individuals using the Internet - Sub-Saharan Africa from 2000 to 2020*. International Telecommunication Union ( ITU ) World Telecommunication/ICT, no date, <https://data.worldbank.org/indicator/IT.NET.USER.ZS?end=2020&locations=ZG&start=2000&view=chart>. [Accessed: 13 May 2022].
- Irshad, S. and Soomro, T.R., 2018. *Identity theft and social media*. *International Journal of Computer Science and Network Security*, 18(1), pp.43-55.
- Iqbal, Z. & Anwar, Z. 2020. SCERM—A novel framework for automated management of cyber threat response activities. *Future Generation Computer Systems*.



- Jahankhani, H., Kendzierskyj, S., Chelvachandran, N. and Ibarra, J. eds., 2020. *Cyber defence in the age of AI, smart societies and augmented humanity*. Springer Nature.
- Jang-Jaccard, J. & Nepal, S. 2014. *A survey of emerging threats in cybersecurity*. *Journal of Computer and System Sciences*, 80(5):973-993.
- Jansen van Vuuren, J.J., Grobler, M. & Zaaiman, J. 2012. *The influence of cyber security levels of South African citizens on National Security*. Proceedings of the 7th International Conference on Information Warfare and Security, Center for Information Assurance and Cybersecurity University of Washington, Seattle, USA, 22-23 March 2012
- Jansen van Vuuren, J.C., Leenen, L., Phahlamohlaka, L.J. and Zaaiman, J.J., 2013. *Development of a South African cybersecurity policy implementation framework*. Academic Conferences and Publishing International.
- Jansen van Vuuren, J.C., Leenen, L. and Zaaiman, J., 2014, March. *Using an ontology as a model for the implementation of the National Cybersecurity Policy Framework for South Africa*. In The 9th International Conference on Cyber Warfare and Security (pp. 107-115).
- Jansen van Vuuren, J.J., Phahlamohlaka, J. & Brazzoli, M. 2010. *Impact of the increase in broadband access on South African national security and the average citizen*. *The Journal of Information Warfare*, 9(3):1-13.
- Jansen van Vuuren, J.J., Phahlamohlaka, L.J. & Leenen, L. 2012. *Governance of cybersecurity in South Africa*. [Online]. Available at: [http://researchspace.csir.co.za/dspace/bitstream/10204/6207/1/JansenVanVuuren\\_2012.pdf](http://researchspace.csir.co.za/dspace/bitstream/10204/6207/1/JansenVanVuuren_2012.pdf) [Accessed: 2 September 2016].
- Jones, S.L., Collins, E.I., Levordashka, A., Muir, K. & Joinson, A. 2019, May. *What is cyber security? Differential language of cyber security across the lifespan*. In *Extended Abstracts of the 2019 CHI Conference on Human Factors in Computing Systems*, 1-6.
- Joshi, K. & Akhilesh, K.B. 2020. *Role of cyber security in retail*. In *Smart technologies*. Singapore: Springer, 233-247.
- Kalash, M., Rochan, M., Mohammed, N., Bruce, N., Wang, Y. & Iqbal, F. 2020. *A deep learning framework for malware classification*. *International Journal of Digital Crime and Forensics (IJDCF)*, 12(1):90-108.
- Karlidag, S. & Bulut, S. 2020. *Cyber-attacks from the political economy perspective and Turkey*. In *Handbook of research on the political economy of communications and media*. IGI Global, 305-321.
- Kempen, A. 2019. *Fighting cybercrime requires an integrated and international effort - the SAPS's envisaged approach*. *Servamus Community-based Safety and Security Magazine*, 112(1):50-54.

- Keshk, M., Turnbull, B., Sitnikova, E., Vatsalan, D. and Moustafa, N., 2021. *Privacy-preserving schemes for safeguarding heterogeneous data sources in cyber-physical systems*. *IEEE Access*.
- Labuschagne, J., Ferentinou, M., Grobler, M. 2020. *Smart slope monitoring through the use of fibre optic sensors*. *ResearchGate*. Conference: 17th AFRICAN REGIONAL CONFERENCE ON SOIL MECHANICS AND GEOTECHNICAL ENGINEERINGAt: Cape Town (October 2019). [Accessed: 20 August 2020].
- Lamba, A. 2020. *A thorough analysis on protecting cyberthreats and attacks on CPS embedded subsystems*. Available at SSRN 3517474.
- Lewis, J.A. 2015. *US–Japan cooperation in cybersecurity*. Washington, DC: Center for Strategic & International Studies.
- Mabunda, S. 2021. *Cybersecurity in South Africa: Towards best practices*. CyberBRICS (pp.227-270)
- MacQueen, K.M., McLellan, E., Metzger, D.S., Kegeles, S., Strauss, R.P., Scotti, R., Blanchard, L. & Trotter, R.T. 2001. *What is community? An evidence-based definition for participatory public health*. *American Journal of Public Health*, 91(12):1929-1938.
- Malm, M.K. & Toyama, K. 2021. *The burdens and the benefits: Socio-economic impacts of mobile phone ownership in Tanzania*. *World Development Perspectives*, 21:100283.
- Mardis, M.A., Jones, F.R. & McClure, C.R. 2019. *Assessing IT educational pathways that support rural broadband: Strategies for aligning IT curricula, policy, and employer needs*. *Community College Journal of Research and Practice*, 43(9):625-630.
- Maree, K. 2010. *First steps in research*. Pretoria: Van Schaik.
- Mashiane, T., Dlamini, Z. & Mahlangu, T. 2019. *A rollout strategy for cybersecurity awareness campaigns*. *Proceedings*. 14<sup>th</sup> International Conference on cyberwarfare and Security (ICCWS 2019), Stellenbosch, South Africa, 28 February- 1 March 2019, 243-250.
- Massey, R. 2020. *Urban renewal in South African cities*. In *Urban geography in South Africa*. Cham: Springer, 265-282.
- Medlock, M.C., Wixon, D., Terrano, M., Romero, R. & Fulton, B. 2002. *Using the RITE method to improve products: A definition and a case study*. *Usability Professionals Association*, 51.
- Methmali, S. 2016. *Perception of internet usage and its impact on cyber-crime in Sri Lanka internet usage and relationship with cyber-crime*. *Proceedings*. 2016 International Conference on Signal Processing, Communication, Power and Embedded System (SCOPEs 2016), October 2016. IEEE, 674-690.

- Meyer, N. & Hamilton, L. 2020. *Female entrepreneurs' business training and its effect on various entrepreneurial factors: Evidence from a developing country*. *International Journal of Economics and Finance Studies*, 12(1):135-151.
- Miracle, V.A., 2016. *The Belmont Report: The triple crown of research ethics*. *Dimensions of Critical Care Nursing*, 35(4), pp.223-228.
- Mohapi, T. 2018. *4 things about the ViewFines website that shocked us*. [Online]. Available at: <https://www.iafrikan.com/2018/05/30/viewfines-security-popular-passwords/> [Accessed: 6 April 2021].
- Morgan, S. 2018. *Cybersecurity Business Report - Top 5 cybersecurity facts, figures and statistics for 2018*. [Online]. Available at: <https://www.csoonline.com/article/3153707/security/top-5-cybersecurity-facts-figures-and-statistics.html> [Accessed: 15 March 2018].
- Moyo, A. 2019. *Joburg hack: City refuses to pay Bitcoin ransom*. ITWeb | Business Technology News. [Online]. Available at: <https://www.itweb.co.za/content/DZQ587VJ33m7zXy2> [Accessed: 6 April 2021].
- Mozid, A. & Yesmen, N. 2020. *Term paper on the nature of cybercrime and cyberthreats: A criminological review*. *Journal of Advanced Forensic Sciences*, 1(1):1.
- Mukherjee, S. 2019. *Overview of the importance of corporate security in business*. *International Journal of Innovative Research in Science, Engineering and Technology* 8(4) April 2019.
- Munro, E. & Hardie, J. 2019. *Why we should stop talking about objectivity and subjectivity in social work*. *The British Journal of Social Work*, 49(2):411-427.
- Murthy, V. 2019. *Regulatory wrap: Cybersecurity-related regulatory considerations for medical devices*. *Biomedical Instrumentation & Technology*, 53(4):312-314.
- MyBroadband. 2015. *South African Electricity Prices – 1994 to 2015*. [Online]. Available: <http://mybroadband.co.za/news/energy/130320-south-african-electricity-prices1994-to-2015.html>. [Accessed 12 October].
- National Institute of Standards and Technology (NIST). 2019. *Building an information technology security awareness and training program*. NIST Special Publication 800-50. Washington, DC: US Department of Commerce.
- Niselow, T. 2018. *Five massive data breaches affecting South Africans*. [Online]. Available at: <https://www.fin24.com/Companies/ICT/five-massive-data-breaches-affecting-south-africans-20180619-2> [Accessed: 6 April 2021].
- OECD. 2015. *Digital security risk management for economic and social prosperity*. Paris.
- Pandu, V., Mohan, J. & Kumar, T.P. 2019. *Network intrusion detection and prevention systems for attacks in IoT Systems*. In *Countering cyber attacks and preserving the integrity and availability of critical systems*. IGI Global, 128-141.

- Patel, I.V. 2021. *The necessity of cyber threat intelligence*. Doctoral dissertation, Utica
- Poy, S. & Schüller, S. 2020. *Internet and voting in the social media era: Evidence from a local broadband policy*. *Research Policy*, 49(1):103861.
- Pramod, D. & Raman, R. 2014. *A study on the user perception and awareness of smartphones*. *International Journal of Applied Engineering Research* 9(23):19133-19144
- Press Association. 2016. *One in 10 suffering fraud or cybercrime, figures show*. [Online]. Available at: <http://www.dailymail.co.uk/wires/pa/article-3700643/Cyber-crime-stats-published-time.html> [Accessed: 21 September 2016].
- Pretorius, B. & Van Niekerk, B. 2015. *Cybersecurity and governance for ICS/SCADA in South Africa. Proceedings*. The 10<sup>th</sup> International Conference on cyberwarfare and Security, Reading, UK. [Accessed: 10 August 2017]. ACP, 241-251.
- Pretorius, B. & Van Niekerk, B. 2020. Cyber-security for ICS/SCADA: A south African perspective. In *cyberwarfare and terrorism: concepts, methodologies, tools, and applications*. IGI Global, 613-630.
- Project Isizwe. 2018. *Free Wi-Fi for South Africa*. Available at: <https://www.commscope.com/globalassets/digizuite/470-300-cs-project-isizwe.pdf>. [Accessed: 29 September 2019].
- Quinlan, C., Babin, B., Carr, J. & Griffin, M. 2019. *Business research methods*. South Western Cengage.
- Raddon, A. 2010. *Early stage research training: Epistemology & ontology in social science research*. [Online]. Available at: <https://www2.le.ac.uk/colleges/ssah/documents/research-training-presentations/EpistFeb10.pdf> [Accessed: 10 August 2016].
- Rajabiun, R. 2020. *Technological change, civic engagement and policy legitimization: Perspectives from the rise of broadband Internet as an essential utility in Canada*. *Government Information Quarterly*, 37(1):101403.
- Ramluckan, T. 2019. *The Applicability of the Tallinn Manuals to South Africa. Proceedings*. 14<sup>th</sup> International Conference on cyberwarfare and Security (ICCWS 2019), Stellenbosch, South Africa, 28 February – 1 March 2019 348.
- Roškot, M., Wanasika, I. & Kroupova, Z.K. 2020. *Cybercrime in Europe: Surprising results of an expensive lapse*. *Journal of Business Strategy*, 7(7): 102.
- Reuters. 2016. *Obama says U.S. government must improve cyber security*. [Online]. Available at: <http://www.reuters.com/article/us-usa-cybersecurity-obama-idUSKCN0ZQ0MN>. [Accessed: 1 September 2016].
- Rubeis, G. & Ketteler, D. 2020. *Who benefits from the app? Internet- and mobile-based interventions (IMIs) and the tension between autonomy and patient well-being*. *Psychotherapie, Psychosomatik, Medizinische Psychologie*, 70(11):467-474

- Ryen, A., 2016. *Research ethics and qualitative research*. Qualitative research, 3, pp.31-48.
- Ryan, M., Antoniou, J., Brooks, L., Jiya, T., Macnish, K. and Stahl, B., 2021. *Research and practice of AI ethics: A case study approach juxtaposing academic discourse with organisational reality*. Science and Engineering Ethics, 27(2), pp.1-29.
- Shoab, S. & Mujtaba, B.G. 2016. *Use it or lose it: Prudently using case study as a research and educational strategy*. American Journal of Education and Learning, 1(2):83-93.
- SAPA. 2013. *70% of South Africans have fallen victim to cybercrime*. [Online]. Available at: <http://www.timeslive.co.za/scitech/2013/11/04/70-of-south-africans-have-fallen-victim-to-cyber-crime>. [Accessed: 16 September 2016].
- Sarre, R., Lau, L.Y.C. & Chang, L.Y. 2018. *Responding to cybercrime: current trends*. Police Practice and Research, 19(6):515-518.
- Saunders, M., Lewis, P. & Thornhill, A. 2009. *Research methods for business students*. Harlow: Pearson Education.
- Scotland, J., 2012. *Exploring the philosophical underpinnings of research: Relating ontology and epistemology to the methodology and methods of the scientific, interpretive, and critical research paradigms*. English language teaching, 5(9), pp.9-16.
- Seldon. A. 2016. *Cyber security outlook*. [Online]. Available at: <http://www.securitysa.com/8562a> [Accessed: 1 September 2016].
- Shafqat, N. and Masood, A., 2016. *Comparative analysis of various national cyber security strategies*. International Journal of Computer Science and Information Security, 14(1), p.129.
- Shapshak, T. 2018. *Liberty hack the 'biggest breach yet'*. [Online]. Available at: <https://www.businesslive.co.za/fm/fm-fox/2018-06-21-liberty-hack-the-biggest-breach-yet/>. [Accessed: 06 April 2021].
- Sharikov, P. 2020. *Cyberthreats and Euro-Atlantic security*. In *Threats to Euro-Atlantic security* Cham: Palgrave Macmillan, 51-68.
- Shin, B. & Lowry, P.B. 2020. *A review and theoretical explanation of the 'Cyberthreat-Intelligence (CTI) capability that needs to be fostered in information security practitioners and how this can be accomplished*. Computers & Security, 101761.
- Song, C., 2018, September. *Learning tensor-based representations from brain-computer interface data for cybersecurity*. In Joint European Conference on Machine Learning
- South Africa. Department of Communications (DoC). 2020. *Review report: E-commerce, cybercrime and cybersecurity – status, gaps and the road ahead*. Pretoria: Government of South Africa. [Online]. Available at: [https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/Review\\_Report\\_e](https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/Review_Report_e)

–commerce \_cybercrime%20and%20cybersecurity\_final\_0.pdf Accessed: 03 October 2021].

South Africa. Department of Communications (DoC). 2014. *National Broadband Policy South Africa Connect*. [Online]. Available at: <http://wiki.lib.sun.ac.za/images/c/c7/Doc-bb-policy.pdf> [Accessed: 08 July 2016].

South Africa. Minister of Justice and Correctional Services. 2015. *Cybercrimes and Cybersecurity Bill*. Draft for public comments. Republic of South Africa.

South African Government Gazette. 2019. *Protection of Personal Information Act. November 2019*. [Online]. Available at: <http://www.gov.za> [Accessed: 20 September 2016].

South African Government Gazette. 2015. *South African National Cyber Security Policy (No. 609)*. [Online]. Available at: [http://www.gov.za/sites/www.gov.za/files/39475\\_gon609.pdf](http://www.gov.za/sites/www.gov.za/files/39475_gon609.pdf) [Accessed: 10 July 2016].

South Africa. Department of Communications. 2015. *National Cybersecurity Policy Framework for South Africa. Pretoria: Communications*.

Statista. 2021. *Digital population in South Africa as of January 2021*. [Online]. Available at: <https://www.statista.com/statistics/685134/south-africa-digital-population/>. [Accessed : 10 January 2022].

Sterlini, P., Massacci, F., Kadenko, N., Fiebig, T. & Van Eeten, M. 2019. *Governance challenges for European cybersecurity policies: Stakeholder views*. *IEEE Security & Privacy*, 18(1):46-54.

Strover, S., Whitacre, B., Rhinesmith, C. & Schrubbe, A. 2020. *The digital inclusion role of rural libraries: Social inequalities through space and place*. *Media, Culture & Society*, 42(2):242-259.

Sutherland, E., 2017. *Governance of cybersecurity-the case of South Africa*. *The African Journal of Information and Communication*, 20, pp.83-112.

Sutherland, E. 2020. *The Fourth Industrial Revolution –The Case of South Africa. Politikon*, 1-20.

Symantec. 2019. *2019 Norton report: Cost per cybercrime victim up 50 percent*. [Online]. Available at: [http://www.symantec.com/en/za/about/news/release/article.jsp?prid=20131029\\_01](http://www.symantec.com/en/za/about/news/release/article.jsp?prid=20131029_01) [Accessed: 10 July 2020].

Techsmart. 26 March 2020. *SA networks face a 10-fold increase in attacks as workforce shifts to remote access*. Available at: <http://www.techsmart.co.za/news/SA-networks-face-a-10-fold-increase-in-attacks-as-workforces-shift-to-remote-access>. [Accessed: 16 January 2021].

- Thomas, T., Vijayaraghavan, A.P. & Emmanuel, S. 2020. *Machine learning and cybersecurity*. In *Machine learning approaches in cyber security analytics*. Singapore: Springer, 37-47.
- Thulin, J. 2015. *Could POPI help curb the rising tide of cybercrime in South Africa?* [Online]. Available at: <http://memeburn.com/2015/03/could-popi-help-curb-the-rising-tide-of-cybercrime-in-south-africa/> [Accessed: 30 August 2016].
- Tikk, E. and Kerttunen, M. eds., 2020. *Routledge Handbook of International Cybersecurity*. Routledge.
- Uçtu, G., Alkan, M., Doğru, İ.A. and Dörterler, M., 2021. *A suggested testbed to evaluate multicast network and threat prevention performance of Next Generation Firewalls*. *Future Generation Computer Systems*, 124, pp.56-67.
- Van Heerden, R., Von Solms, S. & Vorster, J. 2018. *Major security incidents since 2014: an African perspective*. In 2018 IST-Africa Week Conference (IST-Africa), May 2018, Gaborone, Botswana. IEEE, 1.
- Von Solms, R.V. & Van Niekerk, J.V. 2013. *From information security to cyber security. Cybercrime in the Digital Economy*, 38:97-102.
- Wallace, C.D. & Philip, L.J. 2019. *Written evidence submitted to the House of Commons Environment, Food and Rural Affairs Committee Rural broadband and digital only services inquiry*. University of Aberdeen.
- Warburton, D & F5 Labs. 2020. *2020 PHISHING AND FRAUD REPORT Phishing During A Pandemic*. <https://www.f5.com/labs/articles/threat-intelligence/2020-phishing-and-fraud-report> [Accessed: 23 September 2022].
- Weicheng, C.U.I., 2021. *On the philosophical ontology for a general system theory*. *Philosophy*, 11(6), pp.443-458
- Williams, I. 2019. *Community broadband networks and the opportunity for e-government services*. In *Advanced Methodologies and Technologies in Government and Society*. IGI global, 173-185.
- Wong, P., & Ragothaman, V. & Cisco Technology Inc. 2020. *Encrypted traffic analysis control mechanisms*. U.S. Patent Application 16/037,511.
- Yin, R.K. 2003. *Case study research: Design and methods*. London: Sage.
- Zaza, S., Wright-De Agüero, L.K., Briss, P.A., Truman, B.I., Hopkins, D.P., Hennessy, M.H., Zhao, X., Miers, I., Green, M. & Mitrani-Reiser, J. 2019. *Modeling the cybersecurity of hospitals in natural and man-made hazards*. *Sustainable and Resilient Infrastructure*, 4(1):36-49.

## APPENDIX A: ETHICS APPROVAL



---

P.O. Box 652 • Cape Town 8000 South Africa • Tel: +27 21 469 1012 • Fax +27 21 469 1002  
80 Roeland Street, Vredehoek, Cape Town 8001

Office of the Research Ethics Committee	Faculty of Informatics and Design
--	-----------------------------------

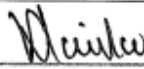
19 October 2016

Ethics approval was granted to Ms Rebecca Dzidzai Mapfumo, student number 211222062, for research activities related to the MTech: Information Technology at the Faculty of Informatics and Design, Cape Peninsula University of Technology (CPUT).

Title of thesis:	Cyber security governance strategies in support of community broadband expansion in the Western Cape: A case study of Interactive Community Access Network (ICAN)
------------------	---

### Comments

Research activities are restricted to those details in the research proposal.

 Signed: Faculty Research Ethics Committee	<u>19/10/2016</u> Date
--	---------------------------



## APPENDIX B: CONSENT LETTER



FACULTY OF INFORMATICS AND DESIGN  
OFFICE OF THE HEAD: DEPARTMENT OF INFORMATION TECHNOLOGY

---

PO Box 652 Cape Town 8000 • Corner of Keizersgracht and Tennant Streets 8001  
Tel: 021-460-3010 / 021-460-3780 • Fax: 086-519-0683 • E-mail: AlexanderB@cput.ac.za

17 January 2018

The Manager  
Interactive Community Access Network (ICAN)  
Elsies River Rd, Saiberau  
Cape Town  
7490

**Rebecca Mapfumo – Letter of Introduction & Permission for Data Collection**

I hereby confirm that Rebecca Dzidzai Mapfumo (211222062) is bona fide registered Master of Technology in Information Technology student at the Cape Peninsula University of Technology.

Rebecca Dzidzai Mapfumo's research is titled – "A cybersecurity governance framework for community broadband projects". The aim and objectives of her study are:

- To explore the salient dimensions (framework) of cybersecurity administration (governance) and user engagement (awareness) at community broadband centres
- To investigate cybersecurity governance at community broadband centres.
- To investigate cybersecurity awareness levels of users at community broadband centres.

It is a requirement of the Higher Degrees Committee (HDC) of the university that students meet all the provisions of its Code of Ethics and obtain prior consent from any organisation where research data is to be collected.

We are grateful for your support. If you are willing and able to facilitate the collection of data within your organisation then we request that you kindly confirm this in writing. A pro forma letter of consent is provided below for this purpose.

Please email your letter of consent to the research supervisor:  
Prof Bennett Alexander at [AlexanderB@cput.ac.za](mailto:AlexanderB@cput.ac.za)

For further clarification, please feel free to contact Ms Veda Naidoo, Secretary of the Faculty Ethics Committee at [NaidooVe@cput.ac.za](mailto:NaidooVe@cput.ac.za) or at 021-469-1012. Yours sincerely,

A handwritten signature in black ink, appearing to read 'Bennett Alexander'.

Prof Bennett M Alexander PrEng  
DTech IT, MSc Tech HRD, BSc EE, MDP, SMSAIEE, MIITPSA Head:  
Department of Information Technology

---


I, LEWELLYN SCHOLTZ in my capacity as Executive Director at 1-CAN Centre give consent in principle to allow Rebecca Dzidzai Mapfumo (211222062) a student at the Cape Peninsula University of Technology, to collect data in this company as part of his/her Master of Technology in Information Technology research. The student has explained the nature of his/her research and the nature of the data to be collected.

This letter of consent in no way commits any individual staff member to participate in the research, and it is expected that the student will get explicit consent from any participants. I reserve the right to withdraw this permission at any future time.

In addition, the company's name may or may not be used as indicated below:

Tick as appropriate

	THESIS	CONFERENCE PAPER	JOURNAL ARTICLE	RESEARCH POSTER
YES	✓	✓	✓	✓
NO				

  
LEWELLYN SCHOLTZ

Insert name

17/01/2018  
 Insert date

## APPENDIX C: QUESTIONNAIRE

Questionnaire used for data collection for this study.

### Research Information

#### Research Title:

- A cybersecurity governance framework for broadband expansion projects in the Western Cape.

#### 1. Background: Why have I decided to do this?

- This is research on cybersecurity governance strategies in support of the broadband expansion projects.
- The aim of this research is to explore the salient dimensions (framework) of cybersecurity administration (governance) and user engagement (awareness) for broadband expansions projects.
- It is envisaged that the findings could relate to broadband expansions projects in general.
- This research will include thorough analysis of South Africa's current cybersecurity environment and the National Cybersecurity Policy Framework (NCPF).

#### 2. Approach: How do you hope to deliver the research?

- Investigate how the NCPF is adopted and applied for community broadband projects.
- Investigate cybersecurity governance strategies currently in existence that supports broadband expansion for broadband expansions projects.
- Investigate cybersecurity threats and risks that arise during broadband expansion.
- Investigate the cybersecurity challenges being faced for broadband expansion projects.

#### 3. Contribution: What is the value proposition of your research?

- This research will potentially contribute to improved cybersecurity administration (governance) and user engagement (awareness) for broadband expansions projects.

**By Cybersecurity I mean:** Tools, governance strategies, risk management plans, security guidelines, processes, technologies and practices that are designed to ensure protection of the cyberspace.

## Questions

**Kindly give a brief description of your broadband expansion project; why established and its purpose.**

**How does broadband expansion affect cybersecurity?**

**What measures are in place to provide cybersecurity to users accessing the Internet through your project? For example: cybersecurity awareness and training, intrusion detection.**

**With regards to the PoPI Act, how do you understand it and how do you ensure Protection of Personal Information of the people utilising the free Wi-Fi facilities you are providing?**

**Do you ever get reports of cybercrimes, cyberthreats or cyberattacks from people getting Internet access through your projects?**

**Of late data mining has become very common; how do you understand data mining and what are you doing to make sure the data of users getting Internet access through your project is safe from it?**

**The National Cybersecurity Policy Framework; what does it mean to you and how does it affect broadband expansion?**

**What cybersecurity regulation/ legislation and policies are you currently complying with?**

**What do you think is the best practice for Community Broadband Centres like yours to ensure cybersecurity?**

**Can you tell me more details about your project regarding network security, firewalls, domains (public and private) and access?**

**Have you experienced any cybersecurity attacks before in this project? If yes what did you do, how did you deal with it?**

**What are the possible dangers or threats when one is using the internet and what do you think can be done to protect the users?**

**What structures or guidelines are in place to provide security during broadband expansion?**

**How are citizens prepared to ensure safety whilst using the internet?**

**From your opinion, what do you think is the best practice for broadband expansion projects like yours to ensure cybersecurity?**

**Is there any additional information you can give me or suggestions?**

**Thank you so much for your participation. I truly value your input and the time you spared to answer all these questions.**