The effects of stakeholder perceptions on the outcomes of the Computer Crime and Cybersecurity Bill:

A case of Lesotho

A research Design presented to the

Department of Information Systems

University of Cape Town

Submitted by:

Khotso Clement Mohale mhlkho035

Research Supervisor: Wallace Chigona and Ayanda Pekane

In partial fulfilment of the requirements for the course:

Master of Commerce specialising in Information Systems

Plagiarism Declaration

I know that plagiarism is wrong. Plagiarism is to use another's work and pretend that it is one's own.

I have used the American Psychological Association (APA) convention for citation and referencing. Each contribution and quotation in this dissertation from the work(s) of other people has been attributed, cited, and referenced.

This dissertation, 'The Effects of Stakeholder Perceptions on the Outcomes of the Computer Crime and Cybersecurity Bill: A Case of Lesotho,' is my own work.

I have not allowed, and will not allow, anyone to copy my work with the intention of passing it off as his or her own work.

I acknowledge that copying someone else's assignment, essay or paper, or part of it, is wrong, and declare that this is my own work.

Signature: Signed by candidate Date 21/ 08/2024

Acknowledgements

All the glory and thanks to God Almighty for strength and his faithfulness throughout this degree, nothing is indeed impossible with God. To my supportive wife M'abohlokoa Mohale, thank you for the prayers, for your advice and all the sacrifices you had to endure to support me throughout this Journey. I truly appreciate you.

To my supervisor, Professor Wallace Chigona, thank you for your guidance throughout this journey; you did not lose faith in me even when, at times, the conclusion seemed blurry. To my supervisor, Ayanda Pekane, your affirmation and reassurance have gone a long way; thank you for believing in me. I was truly privileged to have you both as my supervisors, I couldn't have asked for a better support team.

To the Road Fund Management, thank you for the opportunity and support you afforded me to conduct my study. You have contributed to making me a better person. Furthermore, to the research participants who took time out of their busy schedules to attend the interview sessions, thank you for your time; your input has been invaluable.

ABSTRACT

Problem Statement: Cybersecurity legislation formulation is an agenda item for many governments due to data privacy, cyberbullying, financial fraud, and other cybercrimes. This initiative must account for the stakeholders' understanding of cybersecurity to be effective. Without the stakeholders' understanding of cybersecurity, cybersecurity control initiatives such as legislation and policies may not be able to effect the required behaviour changes. Very little is known about stakeholders' perception of cybersecurity and their impact on cybersecurity controls.

Purpose of the research: This study aims to determine how stakeholders' perceptions about cybersecurity affect the outcomes of the Computer Crime and Cybersecurity Bill.

Design/methodology: The study used qualitative methods and was based on the case study; purposive snowballing was used to identify 17 participants for the study. The data was gathered through semi-structured interviews and document analysis of the Bill and the SADC Model Law Documents. The study used an inductive approach, and thematic analysis was used to analyse the data to achieve the research objectives.

Findings: The findings indicated that stakeholders' perceptions had minimal effect on the outcomes of the Computer Crime and Cybersecurity Bill. The Bill was drafted from the SADC Model Law on cybersecurity, and the outcome of the Bill seems to have been primarily shaped by the model law. It was also determined that there was minimal contextualisation and customisation done on the Bill.

Contributions of the study: The study contributes to the gap in research in terms of investigating the effect of stakeholder perceptions on the development of legislation. In addition, the study contributes new knowledge by providing insights into the source of cybersecurity stakeholders' perceptions. The knowledge may be used to support future studies in humanistic cybersecurity control initiatives. The study may inform stakeholder engagements to assist in accommodating stakeholders' perceptions and inclusion of local expectations in cybersecurity control initiatives. The findings in the study may also guide countries that are in the process of harmonising and transposing cybersecurity legislation to improve their stakeholder expectations in the process.

Keywords: Cybersecurity Legislation, stakeholder's Perceptions, Outcomes of a Bill.

Table of Contents

List of Tables

List of Figures

LIST OF ACRONYMS

AU	African Union
SADC	Southern African Development Community
ITU	International Telecommunication Union
CSIRT	Cybersecurity Incident Response Team
C3SA	Cybersecurity Capacity Centre for Southern Africa
CCCC	Catholic Comprehensive Community College.
CCNA	Cisco Certified Network Associate
COBIT	Control objectives for information and related technology
UAE	United Arab Emirates
ABC	All-Basotho Convention
DC	Democratic Congress
RFP	Revolution for Prosperity

Chapter 1: Introduction

1.1 Introduction

Cybercrime is a global problem, the African continent is no exception. The rapid growth of the Internet and increased adoption of ICT across Africa have not only spurred economic development but have also created new opportunities for perpetrating cybercrime (Kshetri, 2019). Cyberattacks have evolved to become more advanced and have changed in magnitude and complexity. According to Gaillard (2021), cybercrime involves illegal behaviour using electronic means that target computer systems and data. Organised multinational criminal organisations implement cyber-attacks by sharing intelligence to conduct assaults (Brewer et al., 2019). Africa has experienced a sharp increase of 300% in cyberattacks between the years 2018 to 2021 (Gaillard, 2021).

The development of cybersecurity legislation is an agenda item for many governments due to data privacy, cyberbullying, financial fraud, and other cybercrimes (Feroz, Zulfiqar, Noor, & Huo, 2022; Poshai, Chilunjika, & Intauno, 2023). These control measures require an understanding of the underlying attitudes and perceptions of people to change existing online behaviour (Haney & Lutters, 2018; Rohan, Funilkul, Pal, & Chutimaskul, 2021).

In a 2021 cybersecurity maturity assessment by C3SA, 9 of 16 African countries lacked cybersecurity legislation, including Lesotho, Angola, Namibia, and Zimbabwe (C3SA, 2022). It is evident from the study that even countries with cybersecurity legislation in place are encountering challenges in effectively implementing it. Lesotho, like many African countries, has not succeeded in developing a cybersecurity regulation to criminalise cybercrime; as a result, the country has become vulnerable to malicious cyber activity (Mosola, Moeketsi, Sehobai, & Pule, 2019).

This study aims to determine how stakeholders' perceptions about cybersecurity affect the outcomes of the Computer Crime and Cybersecurity Bill. The stakeholders chosen to take part in the study were those who were involved in consultations that took place in the formulation of the Computer Crime and Cybersecurity Bill in Lesotho.

1.2 Context of the Study

Between 2010 and 2020, there was a 44% increase in people accessing the Internet in Lesotho. In the same period, there was a 52% increase in mobile phone subscribers in the country (World Bank, 2022). This resulted in an increased attack surface for cyber-criminals to exploit. This is especially true due to the absence of laws to regulate the safe use of technology (Mosola et al., 2019). There has already been incidents of Cybercrime in the country, resulting in financial losses for individuals and businesses (Mosola et al., 2019; Thuraisingham, 2023).

Lesotho is a member of the international community; as such, the country has committed to several International conventions on cybersecurity. Some of these agreements include the African Union (AU) Convention on Cyber Security and Personal Data Protection of 2014 (Makulilo & Mophethe, 2016). As a member of the Commonwealth, Lesotho is also required to implement directives in the Commonwealth Convention on Cybersecurity (Commonwealth, 2018). As a member of SADC, Lesotho is also expected to benefit from the 2012 SADC Model Law on Computer Crime and Cybersecurity. The Model Law was created to harmonise legislation in the region (MISA, 2021). Due to these and other agreements, the country is required to regulate cybercrime using legal instruments.

The Telecommunications Act of 2012 established the Lesotho Telecommunications Authority, which requires licensed Telecommunications companies to protect the privacy and integrity of the user's information while being transmitted through their networks (Makulilo & Mophethe, 2016). The Lesotho ICT Policy of 2005 provides for IT security in the country's infrastructure (ITU, 2021). The country also developed the Data Protection Act, No. 5 of 2012, the act provides for the regulation of personal information and recognises the values of personal privacy under the act (Makulilo & Mophethe, 2016). Even though the act provides for the investigation of data breaches, it is limited in terms of the enforcement of certain violations. The act does not issue binding penalties and fines against violators (Makulilo & Mophethe, 2016).

The Computer Crime and Cybersecurity Bill's purpose is to regulate issues of cyber terrorism, computer-related forgery, fraud, and identity theft, among others (Mpaki, 2022). The Bill was formulated and presented to parliament in 2022. It was declined by parliament, and it was subsequently reviewed with the guidance of a consultant. At the moment, it has not been passed into law, as a result, the country does not have a law regulating cybercrime (Mosola et al., 2019). Some of the Civil organisations, such as the Media Institute of Southern Africa and the

Transformation Resource Centre, publicly cited that there was insufficient consultation during the drafting of the Bill. They also stated that the Bill violates some of the basic human rights, such as the right to privacy (Media Statement on Computer Crime and Cyber Security Bill, 2021).

The Bill was rejected due to insufficient consultations and engagements with critical stakeholders such as security agencies and telecommunication agencies (National Assembly, 2021). It was reviewed and presented to Parliament for the second time in 2023 (Ndebele, 2023). The Bill has been waiting for Royal assent, after which it will become a law.

1.3 Problem Statement and Purpose of the Study

In recent years, there has been a surge in cybersecurity research efforts. Nevertheless, numerous unexplored insights still exist at the intersection of cybersecurity and social aspects (Du Toit, Hadebe, & Mphatheni, 2018). Understanding factors that influence human behaviour and the decision-making process can contribute to more effective cybersecurity legislation and policies (Jadhav, Haggag, & Haggag, 2022). Few studies have investigated people's perceptions of cybersecurity globally and specifically in the African context (Ani, He, & Tiwari, 2019). Little is known about the public's understanding of cybersecurity and its impact on legislation formulation.

The current academic focus primarily centres around macro security dynamics rather than individuals' perceptions of cybersecurity. As a result, there is an evident lack of data to inform cybersecurity legislative initiatives (Kostyuk & Wayne, 2021). Table 1.1 summarises studies on cybersecurity controls, such as laws and policies. Most of these studies focus on technical aspects of cybersecurity controls instead of the human side. Some studies have focused on the human side of perceptions of cybersecurity in Europe and the UAE context. These studies don't attempt to link people's perceptions to their effect on the formulation and implementation of cybersecurity legislation. Most of these studies also use document analysis as a source of data instead of primary data. The use of primary data in the African context may yield new insights.

Table 1.1: A summary of studies about cybersecurity studies in the African Context

Reference/Year	The focus of the Study	Country
Malatji, Marnewick, & von Solms (2021)	Cybersecurity policy and the legislation	South Africa
Gaillard (2021)	Cybersecurity Challenges and Governance Issues	Nigeria and South Africa
Media Institute of Southern Africa (2021)	Cybercrime Laws and Human Rights	SADC region
Mosola et al., 2019 (2019)	Cybersecurity Protection Structures	Lesotho
de Barros & Lazarek (2018)	Cybersecurity Policies	Mozambique and South Africa
Maisikeli (2020)	Understanding of cybersecurity perceptions and Risk assessment	United Arab Emirates
Yalin (2018)	How cybersecurity perceptions affect cybersecurity in a university setting	Turkey

Understanding human factors is paramount when addressing cybersecurity legislation and policies (Ani et al., 2019). These human aspects may include awareness and people's understanding of cybersecurity. Generally, there is a poor perception of cybersecurity among African decision-makers and leadership, this has led to poor cybersecurity legislation and policies (Ani et al., 2019). In Lesotho, research shows a poor understanding of cybersecurity and the threats of using Internet services (Mosola et al., 2019). People play an important role in cybersecurity; hence, understanding what influences their behaviour and decision-making process will contribute to effective cybersecurity control measures (Jadhav et al., 2022)

Research has proven that altering people's beliefs and attitudes may lead to desired compliance to policies and legislation (Alshaikh & Adamson, 2021)**.** The Study seeks to determine the relationship between stakeholder perceptions and their effects on the outcomes of the Computer Crime and Cybersecurity Bill.

1.4 Research questions and objectives

This section explains the research questions and objectives. Table 1.2 shows the research questions and the corresponding objectives. An explanation of the research questions is also provided.

Table 1.2: Research Questions and Objectives

Research Question And Objectives	**Research question**	**Research Objectives**
Primary Research Question and Objective	How do stakeholder's perceptions about cybersecurity affect the outcomes of the Computer Crime and Cybersecurity Bill?	To determine how stakeholder's perceptions about cybersecurity affect the outcomes of the Computer Crime and Cybersecurity Bill.
Sub-Questions and Sub-Objectives	What are the stakeholder perceptions about cybersecurity?	To determine stakeholder perceptions about cybersecurity.
	What factors influenced stakeholder perceptions about cybersecurity?	Describe factors that influence stakeholder perceptions about cybersecurity.
	What are the outcomes of the Computer Crime and Cybersecurity Bill?	Determine the outcomes of the Computer Crime and Cybersecurity Bill.

1.5 Explanation of Research Questions

The central focus of this study is to contribute to the understanding of cybersecurity perception in the specific context of the legislation formulation process. The research aims to address the following question: "*How do stakeholders' perceptions about cybersecurity affect the outcomes of the Computer Crime and Cybersecurity Bill?"* Cybersecurity legislation is created to enforce the safe use of technology in cyberspace and to discourage and penalise cyber criminals. These corrective measures require a change in human behaviour. Understanding

cybersecurity perceptions among stakeholders is critical to achieving these controls. The study, therefore, examines the relationship between the stakeholders' perceptions of cybersecurity and the outcomes expected in the Computer Crime and Cybersecurity Bill. As a result, the objectives and sub-questions of the study align with the perspective outlined.

The following sub-questions have been addressed to answer the research question. *What are the stakeholders' perceptions about cybersecurity?* Because stakeholder perceptions in the context of the Computer Crime and Cybersecurity Bill of Lesotho are being investigated, the initial step is to identify the existing perception of cybersecurity among stakeholders. The second sub-question is: *What factors influenced stakeholder perceptions about cybersecurity?* The sources of the perceptions are being investigated from the stakeholders' standpoint; the research determines how the perceptions about cybersecurity were created. The last sub-question is*: What are the outcomes of the Computer Crime Cybersecurity Bill?* An investigation of the issues being addressed by the Computer Crime and Cybersecurity Bill has been carried out. The outcomes of the Bill consist of the problems in the cybersecurity environment in Lesotho that necessitated the formulation of the proposed Law.

1.6 Overview of the research approach

The study used a constructivist approach and followed an interpretive paradigm. A qualitative research approach was also used. The study followed the case study method, following a single case study approach. The case used is the development of Lesotho's Computer Crime and Cybersecurity Bill formulation process. The case was selected because Lesotho is in the process of formulating the Bill; the process has taken more than 10 years. The researcher will have ample opportunities to engage with stakeholders who participated in this process, enabling a comprehensive grasp of the process. Purposive sampling was used to target a sample of 17 participants involved in the Bill's formulation. Snowballing was also used because the initial list of participants provided by the organisers of the formulation process was insufficient. Additional participants were identified based on the recommendations provided by participants already interviewed.

The data for the study was obtained through semi-structured interviews conducted in early 2023. This approach assisted the researcher in delving deeper into the respondents' perspectives by enabling follow-up inquiries during the interviews. The study also used the Computer Crime and Cybersecurity Bill document and the SADC Model Law on Cybersecurity document for

secondary data. A combination of semi-structured interviews and document review was adopted to strengthen the research findings and gain a deeper understanding of cybersecurity perceptions. Thematic analysis was also used to review and analyse the interview and Document review data to develop themes. The data from the themes and relevant literature was used to answer the research questions. Due to the limited time available to complete the study, the researcher used cross-sectional studies (Dubé & Paré, 2003).

1.7 Significance of the Study

The focus and emphasis of previous cybersecurity research has been on the technical issues of cybersecurity rather than on the humanistic side of cybersecurity. This meant that less research has been done in this area, especially in the African context (Ani et al., 2019). The study may benefit law and policy-makers and international organisations like SADC, ITU, and AU. These organisations are interested in cybersecurity; the role of stakeholder perceptions may influence their efforts to assist countries in harmonising and transposing cybersecurity legislation effectively.

In the African continent, out of 54 countries studied, only 24 had developed cybersecurity legislation (Orji, 2018). In the SADC region, 9 out of 16 countries had formulated cybersecurity legislation in 2021 (C3SA, 2022). This suggests that many countries may be developing their cybersecurity legislation. The study may inform stakeholder engagements to assist in accommodating stakeholders' perceptions and contextualising the formulation to local expectations.

1.8 Explanation of the key terms

This section provides definitions for the key terms used in this study within the context of formulating Lesotho's Computer Crime and Cybersecurity Bill.

Stakeholder

Stakeholders are the individuals or groups who are impacted by, or who have an impact on, a given situation or issue (Pedrini & Ferri, 2018). Computer crime and Cybersecurity Bill stakeholders can be broadly categorised as the Government that owns the Bill, all those who the proposed law will act upon, lawmakers, the private sector, international organisations, and the general public (Kasper, 2020).

Cybersecurity Perceptions

Perception is the process by which individuals interpret and organise information to produce meaning in the world. People interpret stimuli based on meaningful prior experiences and beliefs (Pickens, 2005).

Bill

Draft legislation that has been presented to the Parliament for approval becomes a law after the approval (Royal assent) of the Head of State, the King. The Cybersecurity Bill is currently awaiting Royal Assent after approval of Parliament, which was done in 2023.

Computer Crime and Cybersecurity Bill

The draft law known as the Computer Crime and Cybersecurity Bill encompasses formal, legal regulatory measures aimed at preventing and managing the violation of rights and privileges in cyberspace (Nwankwo & Ukaoha, 2019; Snail Ka Mtuze & Musoni, 2023). The law also provides a platform and a standard for the investigation of cybercrime, and the prosecution of crimes committed online, while also facilitating cooperation between countries on cybercrime matters (Nwankwo & Ukaoha, 2019).

Outcomes of the Bill

These are agenda items in the Bill; they include the challenges that necessitate the development of a law. In the context of cybersecurity, they include the prevention of cybercrimes that may have occurred in the country, the creation of Critical infrastructure protection measures, and the creation of cybersecurity management functions such as the CSIRT and the Cybersecurity Advisory Council.

1.9 Assumptions of the study

This study is based on the following assumptions:

- The respondents interviewed were knowledgeable in the subject of cybersecurity, even though they may not be experts.
- Respondents voluntarily and honestly provided responses to the research question in the interview, and respondents would not withhold any information due to a lack of trust.
- All respondents in the study understood the English Language and the questions being posed to them.

1.10 Organisation of the Dissertation

The research study consists of the following chapters.

Chapter 1 (the current chapter):

This chapter introduces the research topic and justifies the need to conduct the study; it consists of research questions and research objectives. The context of the study and the problem statement provide the background and justification upon which the study is founded. The assumptions, significance, and limitations of the study are also outlined.

Chapter 2: Literature Review

This chapter reviews the existing literature on legislation formulation and how it relates to participants' perceptions. It also briefly reviews the perception formulation process and legislation outcomes. The legislation formulation process objectives are also outlined, and the challenges that many countries encounter while formulating cybersecurity legislation are also reviewed.

Chapter 3: Research Methodology

This chapter covers the philosophical considerations made while designing the research approach, and the methodical assumption upon which the study will be conducted has also been outlined. It discusses the approach followed for the population and sampling method, data collection, data analysis, and strategy used to conduct the study, the ethical considerations being observed during the research processes are also discussed.

Chapter 4: Case Description

This chapter describes the case study used for the study. This description includes the technology, cybersecurity, political, and legal environment. The context also includes issues around the international environment that influenced the formulation of the Computer Crime and Cybersecurity Bill. This context provides a basis for the study and the environment in which it is conducted.

Chapter 5: Research Findings and Discussion

This chapter presents the findings of the data collected through semi-structured interviews and document review. This chapter also discusses the implications of the findings on a theoretical and practical basis. Analysis and interpretation of the findings was also carried out relative to the research questions and objectives.

Chapter 6: Conclusions

This section summarises the conclusions and contributions, along with the study's constraints. It also presents suggestions for future research. Additionally, it outlines how the study addressed the research inquiries and goals, emphasising the holistic value it provided.

Chapter 2: Literature Review

2.1 Introduction

In the United Nations Conference on Least Developed Countries in 2011, Information Technology was afforded the same priority status as other essential services like electricity, water, and transport (UN, 2021). However, most African countries have low technological skills. Due to English language barriers, disseminating computer literacy information to the general population poses a significant obstacle (UN, 2021). This has inevitably led to numerous users being exposed to online risks, notably misinformation and spam (UN, 2021). According to research, there is a growing trend of cybercrime targeting economically vulnerable regions due to the ease of execution and inadequate security measures. As a result, these regions have become susceptible to frequent cyberattacks (Kshetri, 2019).

Across the world, many nations have developed cybersecurity legislation and policies to regulate and criminalise cybercrime, to promote safe cyberspace behaviour (de Barros & Lazarek, 2018). Controlling cybercrime through legal measures is still considered one of the most practical measures. This approach includes the establishment of laws and policies that dictate the desired behaviour in cyberspace (Orji, 2018).

Effective controls persuade people to comply. These controls require an understanding of the underlying attitudes and perceptions of people in order to change existing behaviour (Haney & Lutters, 2018; Rohan et al., 2021). Human psychology is highly complex and subjective, yet humans are the weakest link when dealing with any cybersecurity reality. Understanding human behaviour and attitudes toward cybersecurity is critical to any cybersecurity scenario (Rohan et al., 2021).

2.2 Cybersecurity

Cybersecurity is about the protection of people and digital assets from criminal activity in cyberspace; it provides a set of measures to ensure cyber resilience (Tomšů, 2021). Cybersecurity is also a practice by which information and other assets are protected and defended against criminal attacks or destruction (Navajas-Adán, Badia-Gelabert, Jiménez-Saurina, Marijuán-Martín, & Mayo-García, 2024). The principles of cybersecurity include data, Technology, and human beings (Rohan et al., 2021). Technology stores and manipulates

the data, while human beings are responsible for the ownership of data and its manipulation through the use of technology (Rohan et al., 2021).

Cybersecurity involves using advanced tools, policies, security standards, safety guidelines, risk management approaches, and compliance with laws to ensure protection against cyber threats. Mitigating cybercrime requires technology solutions, citizen awareness, and the establishment of effective policies and laws, both at the organisational and national levels (Navajas-Adán et al., 2024). Cybersecurity protects people and hardware in addition to information, unlike information security, which is limited to the safeguarding of information (Yalin, 2018). Cybersecurity has no boundaries; it goes beyond organisational and national boundaries. It is a broad subject that includes individuals, organisations, states, and the international community.

2.3 Objectives of Cybersecurity

The following section describes some of cybersecurity's objectives in the context of a country. Table 2.1 provides a summarised description of these objectives.

Table 2.1: Objectives of cybersecurity

Objective	**Summary Description**
Personal data protection	Protection of information and persons who use the Internet through laws and policies established by governments.
Cyber stability	Controls established by agreements between countries to limit transborder crimes over the Internet.
Critical Infrastructure Protection	Protection of Infrastructure that provides essential services in a country. These services may provide health, telecommunications, financial and banking, and national security, among others.

2.3.1 Personal Data Protection

Cyberspace represents an open-access platform where numerous untrusted participants engage in business, communication, and social interactions (Karim, Bonhi, & Afroze, 2019). Internet

users can impact each other through their online interactions, potentially causing harm, such as fraud or unauthorised access to private information (Karim et al., 2019). Internet users often worry that their online activities are being monitored or that their data is being used for hidden agendas (Sunkpho, Ramjan, & Oottamakorn, 2018). People or organisations freely share information and take part in transactions and interactions in an unregulated environment (Karim et al., 2019). Governments must ensure Internet communication's confidentiality, integrity, and availability for user safety. This is achieved through the implementation of regulatory frameworks, encompassing policies and legislation, aimed at ensuring adherence to favourable behavioural standards (Sunkpho et al., 2018).

2.3.2 Cyber stability

Cyber stability is a state where all internet users can enjoy its benefits without fearing harm (Klimburg & Almeida, 2019). The creation of this state is the result of international agreements aimed at guaranteeing the desired conduct in cyberspace and fostering collaborative controls among nations (Klimburg & Almeida, 2019; Yan, 2022). The agreements control cyber activities occurring within and outside national borders. Cyber stability requires countries to take proactive measures to limit cybercrime across their borders. Given the transborder nature of cybersecurity and the closed national legislation nature of cybersecurity laws, it is difficult to establish Cyber stability without international cooperation (Yan, 2022).

Cyber stability ensures that cyberspace is secure and open, fostering economic activity between countries and organisations (Klimburg & Almeida, 2019). When using the Internet for transactions, it is important for individuals to have protection from potential harm. This helps them focus on their business and innovation (Klimburg & Almeida, 2019). Through cyber stability, nations are also able to prevent cybercrime that may occur across their borders through coordinated international cybercrime prevention (Klimburg & Almeida, 2019).

2.3.3 Critical Infrastructure Protection

It is necessary to prioritise Critical Infrastructure to ensure the safety of the public, maintain national security, and promote economic growth (Thuraisingham, 2023). One of the priorities of many countries is to protect important facilities and assets from cyber threats. This requires using good cybersecurity practices to identify and safeguard these assets (C3SA, 2022; Karim et al., 2019). Developing and enforcing national cybersecurity laws also protects critical

infrastructure (C3SA, 2022; Karim et al., 2019). The all-hazard approach is normally used to protect critical infrastructure; this method assists in determining a wide range of risks, and plans are developed for mitigation (Orji, 2018).

2.3.4 Perceptions of Cybersecurity

Perception can be defined as a cognitive process through which individuals interpret sensory information and organise it to generate meaning and understanding within the world. This process is influenced by an individual's prior experiences, beliefs, and expectations, which shape how new stimuli are interpreted and processed (Pickens, 2005). Perception is shaped through a process that involves stimulation, registration, organisation, and interpretation, as shown in Figure 2.1. An individual typically chooses to interpret information relevant to their knowledge and beliefs when presented with multiple sources of information (Sherif & Cantril, 1945). Perceptions may be created from past experiences, values, and external sensory stimuli (Niosi, 2021).

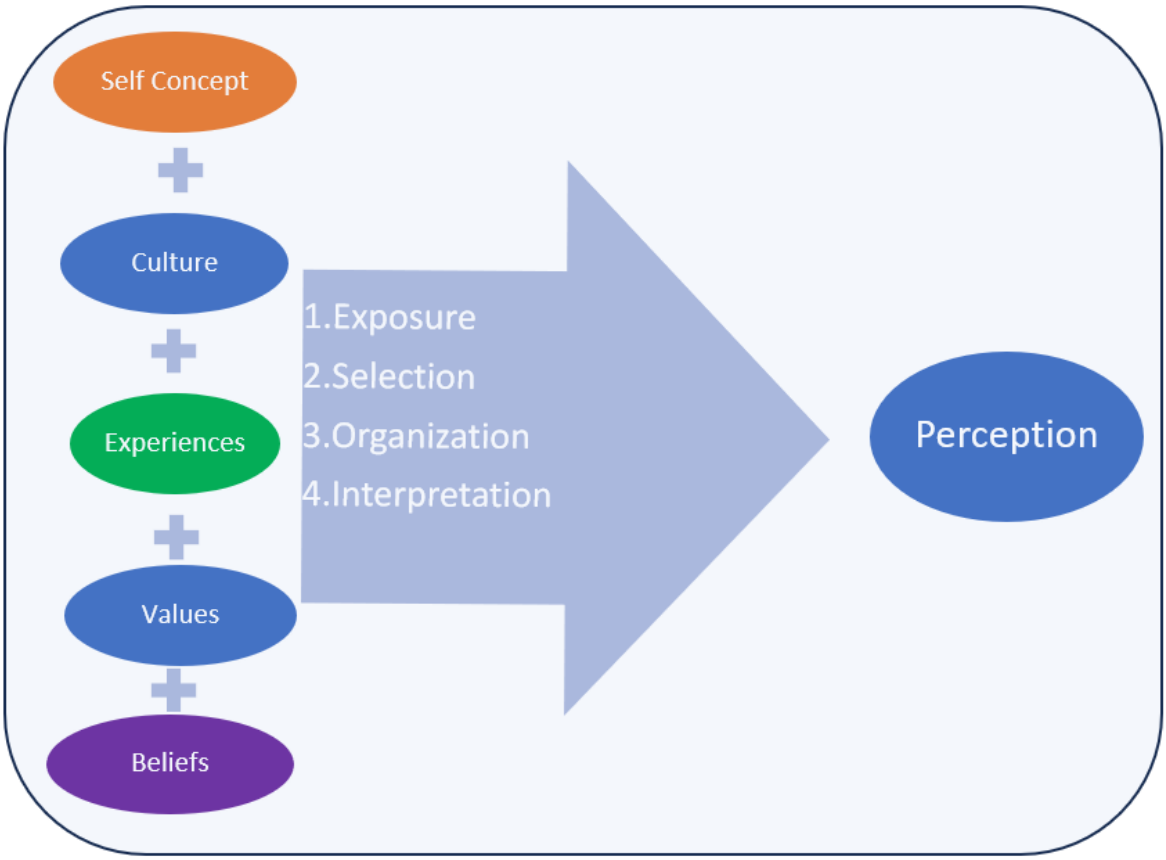


Figure 2.1: Perception Process (BrainGymmer, 2020; Niosi, 2021)

Humans play an important role in cybersecurity; hence, understanding what influences their behaviour and decision-making process will contribute to effective cybersecurity controls (Jadhav et al., 2022)**.** Cybersecurity is perceived to be fear-evoking, generally regarded as a scary, dull, and confusing subject (Haney & Lutters, 2018). On the one hand, it has been demonstrated through research that a change in behaviour is not only achieved through awareness initiatives. Efforts to change people's beliefs and attitudes have been shown to have a greater impact on achieving desirable cybersecurity conduct among users (Alshaikh & Adamson, 2021)**.** On the other hand, legislation and policy formulation strategies play a big role in controlling cybercrime. These efforts must be supplemented by funding to enable cybersecurity awareness initiatives implementation and capacity building for technology users (Adomako, Mohamed, Garba, & Saint, 2018).

2.4 Cybersecurity Perceptions in Africa

In numerous SADC countries, cybersecurity is often viewed unfavourably and is not seen as a top national concern. In reality, most governments consider cybersecurity to be an expendable expense rather than a critical investment (Adomako et al., 2018). Many regional governments have failed to address security threats and implement modern security measures (Adomako et al., 2018). African nations continue to encounter significant obstacles to effective communication, which obstruct the dissemination of cybersecurity awareness information (Kshetri, 2019). The primary reason for this is that a significant number of Internet users on the continent are not proficient in English, which happens to be the predominant language for conveying cybersecurity information (Kshetri, 2019).

It is essential for not only technocrats but also for leaders and lawmakers to grasp cybersecurity (Adomako et al., 2018). This understanding plays a crucial role in strategic decision-making and planning processes to combat cybercrime (Ron, Fuertes, Bonilla, Toulkeridis, & Díaz, 2018). Insufficient knowledge and skills in cybersecurity are frequently identified as key shortcomings among decision-makers, government officials, and academic researchers on the continent. This has led to a limited comprehension of cyber threats, as well as the necessary cyber hygiene practices and controls. Proficiency in cybersecurity is recognised for its positive impact on analytical capabilities and preparedness necessary for cybersecurity risk management and control efforts (Ani et al., 2019).

2.5 Legislation

Legislation is a control measure by which a government, with its legislative function, issues directives to implement its policies (Rubin, 1989). The implementation of legislation generally lies in the hands of the police, prosecution, and the courts of law in the case of criminal legislation (Rubin, 1989). Other forms of legislation may be implemented by the arms of government, such as the government agencies and courts of law, to ensure that the policy direction is actioned (Rubin, 1989). In the absence of cybersecurity legislation, some countries often resort to applying the principles of common law to enforce cybercrime prevention. While common law may apply to some cases, its application is limited and narrow in scope (Snail Ka Mtuze & Musoni, 2023).

2.5.1 Cybersecurity legislation

Cybersecurity legislation encompasses the formal legal and regulatory measures put in place to prevent and manage cyber infringements on the rights and privileges of users in digital environments (Nwankwo & Ukaoha, 2019; Snail Ka Mtuze & Musoni, 2023). Cybersecurity Law achieves this by creating sanctions to protect ICT Infrastructure, systems, information, and users and their rights in cyberspace. The law also provides a platform and a standard for the investigation and prosecution of crimes committed online, while also facilitating cooperation between countries on cybercrime matters (Nwankwo & Ukaoha, 2019).

2.5.2 Stakeholder Engagement in Cybersecurity Legislation

Stakeholders are individuals or groups impacted by, or impacting, a specific situation or issue (Pedrini & Ferri, 2018). Computer Crime and Cybersecurity Bill stakeholders can be broadly categorised into the Government, which is the custodian of the Bill, all those who the proposed law will act upon, lawmakers, the private sector, international organisations, and the general public (Kasper, 2020). Figure 2.2 explains the roles of the stakeholders in the development of cybersecurity legislation. These stakeholders are considered core to the law's development due to their unique understanding of the subject. Some of these stakeholders also play a role in its implementation.

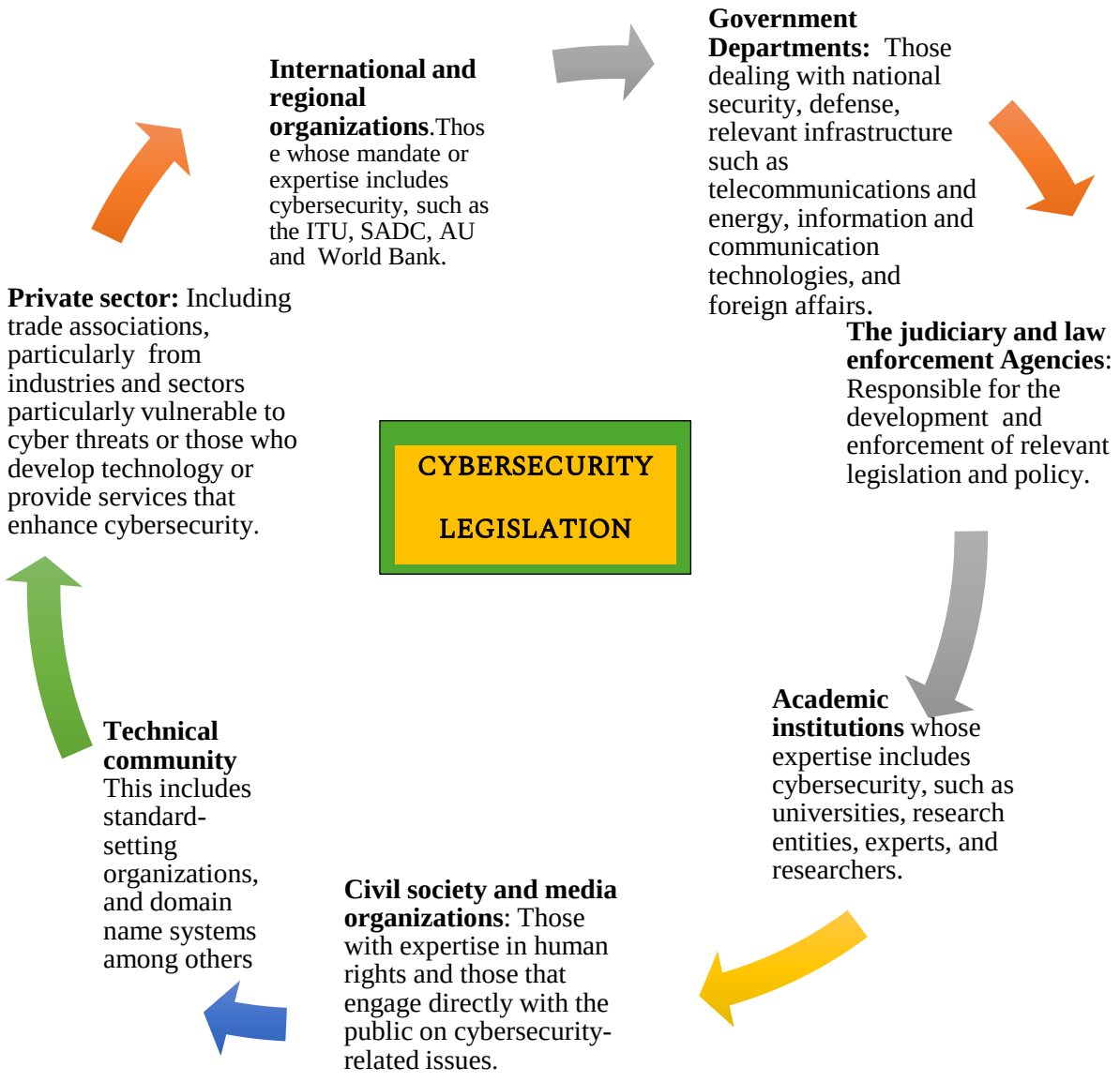


Figure 2.2: Cybersecurity legislation stakeholders (global partners digital, 2020)

Cybersecurity legislation is a document which manages the risk in cyberspace, where the government collaborates with the private sector and other stakeholders (Lebogang, Tabona, & Maupong, 2022). The collaboration efforts could also be between government and local stakeholders, such as the private sector, or between International stakeholders, such as other governments and International organisations (van der Spuy & Oolun, 2018). Mauritius provides an excellent example of this collaborative approach; the country's cybersecurity Strategy of 2014- 2019 contains objectives with a focus on collaboration with the private sector. Many African countries are lagging behind in ensuring a collaborative approach to cybersecurity efforts due to the limited understanding of the nature and benefits of such a

collaboration (van der Spuy & Oolun, 2018). Collaboration between government, academia, research, and innovation facilities is also lacking in many African countries (Ikuero, 2022; (Malatji et al., 2021).

At the International level, countries need to collaborate in their cybersecurity efforts; it has been noted that many African countries lack the necessary commitment to collaborate on issues of cybersecurity (Malatji et al., 2021). Lesotho is a member of the international community, and as such, the country has committed to several international conventions on cybersecurity. Some of these stakeholders include the African Union, SADC, Commonwealth, and ITU (Commonwealth, 2018; ITU, 2007; Media Institute of Southern Africa, 2021). As a member of SADC, Lesotho is also expected to transpose the 2012 SADC Model Law on Computer Crime and Cybersecurity, which was created to harmonise legislation in the region (MISA, 2021).

2.6 Challenges in Legislation Development

In 2021, C3SA assessed cybersecurity maturity in 16 countries. The findings, shown in Table 2.2, revealed that 9 of these countries, including Lesotho, Angola, Namibia, and Zimbabwe, did not have cybersecurity laws in place (C3SA, 2022). A study conducted by the African Union on 54 African countries found that 24 of them did not have any laws to address cybercrime (Orji, 2018). The results of these two studies also indicate that countries with cybersecurity laws are finding it challenging to enforce them properly. This suggests that there are obstacles in creating and executing cybersecurity legislation in numerous African nations.

Table 2.2: Cybersecurity Policy and Strategies in Africa (C3SA, 2022)

Country	National Cybersecurity Strategy / Policy	Year Adopted
Angola	-	-
Botswana	National Cybersecurity Strategy[87]	2020
Comoros	-	-
DRC	Draft	-
eSwatini	Eswatini National Cybersecurity Strategy 2020 - 2025[88]	2020
Lesotho	-	-
Madagascar	-	-
Malawi	National Cybersecurity Strategy (2019 - 2024)[89]	2019
Mauritius	National Cybersecurity Strategy (2014-2019)[90]	2014
Mozambique	Estratégia Nacional de Segurança Cibernética de Moçambique - (Proposta) Versão 2[91]	
Namibia	-	-
Seychelles	-	-
South Africa	National Cybersecurity Policy Framework	2015
Tanzania	-	-
Zambia	National Cybersecurity Policy 2021[92] and Implementation Plan (2021 – 2015)[93]	2021
Zimbabwe	-	-

2.6.1 Cybersecurity Awareness Challenges

Cybersecurity is poorly perceived in many African countries; as such, it is not regarded as a national priority; most governments have a lux mentality when addressing cybersecurity challenges (Adomako et al., 2018). Many governments in the region have failed to address security threats and implement up-to-date security measures as a result (Adomako et al., 2018). The understanding of cybersecurity has been identified as a key factor that could lead to the development of laws and policies essential for combating cybercrime (Orji, 2018).

A lack of awareness on the subject could be the reason why African countries are considered to have limited cybersecurity capability (C3SA, 2022). Cybercriminals exploit the limited cybersecurity knowledge of technology users to carry out cyberattacks. Techniques like social engineering allow cybercriminals to trick individuals who lack awareness of cybersecurity. Additionally, individuals who neglect good cybersecurity practices also contribute to the prevalence of cybercrime (Ani et al., 2019). In Africa, cybersecurity awareness is generally low, and there are limited incentives to tackle the issue. Nevertheless, some governments in the region are moving towards implementing initiatives to raise awareness and enforce legislative controls (C3SA, 2022).

2.6.2 Cybersecurity Budget Allocation and Funding

Despite the increasing need for countries in Africa to develop cybersecurity laws, many of them face significant financial challenges when it comes to implementing crucial cybersecurity measures (de Barros & Lazarek, 2018; Jaquire & Von Solms, 2015). The development of laws and regulations to manage cybercrime is hindered by this limitation. Other government spending priorities, such as poverty reduction and HIV/AIDS, contribute to the limited funding for cybersecurity (C3SA, 2022). The formulation of laws requires financial resources, as does the implementation of these laws and the pursuit of cybercriminals (Adomako et al., 2018). The lack of adequate funding hampers research and development, training, education, and scholarship in the cybersecurity domain (Orji, 2018). Governments can address the budget limitations impeding cybersecurity efforts by prioritising funding for the implementation of cybersecurity and ensuring its efficient use.

2.6.3 Inadequate cybersecurity education and training

African countries, especially those with weak economies, are highly susceptible to cyberattacks because they have quickly adopted new technologies. However, they lack the necessary training and education in cybersecurity to develop legislation that would protect them from cyber threats (Bada, Von Solms, & Agrafiotis, 2019; Mogoane & Kabanda, 2019). Inadequate education leads to low ICT literacy, which is a result of insufficient knowledge in cybersecurity.

There is also a lack of education among many Internet users, and the lack of resources and funding required to facilitate cybersecurity education are also some of the most prevalent challenges hampering cybersecurity efforts. Rapid technology changes and adoption also result in teachers and education providers requiring more frequent retraining to keep up with changes in technology. Low ICT literacy among many African countries leads to a limited understanding of cybersecurity risks and challenges. This hinders awareness campaign designs and the achievement of the development of cybersecurity control measures (Bada et al., 2019; Vakulyk, Petrenko, Kuzmenko, Pochtovyi, & Orlovskyi, 2020).

2.6.4 Lack of Cybersecurity Expertise and Skills

African nations face challenges in developing cybersecurity laws due to the lack of necessary skills and expertise for creating and enforcing cybersecurity regulations (Adomako et al.,

2018). The estimated number of certified cybersecurity professionals in Africa was only 7,000 by 2020, despite the continent's population being approximately 1.24 billion. This shortage of skills was believed to be around 100,000 individuals (Malatji et al., 2021).

The scarcity of cybersecurity professionals in African countries has been attributed to economic and institutional obstacles. This affects the development and implementation of national cybersecurity legislations (Orji, 2018). Moreover, researchers in many African nations also face a shortage of cybersecurity capacity. Research is seen as a valuable tool that can provide lawmakers with the necessary insights for formulating legislation (Orji, 2018). The solution to scarce cybersecurity skills is dependent on the government's investment in capacity building, which includes education and training (Orji, 2018).

2.7 Gaps in Literature

Numerous studies have been carried out regarding cybersecurity laws globally. In Africa, research concentrated on evaluating cybersecurity readiness from a regional viewpoint, including the African continent and the SADC region (Adomako et al., 2018; C3SA, 2022; Orji, 2018). Many of the insights are still to be discovered, especially when it comes to the relationship between cybersecurity and human factors such as perceptions (Du Toit et al., 2018).

Several studies in the African context have concentrated on the technical elements of cybersecurity, specifically policies, governance, and legislation, rather than human factors, such as people's perceptions. While there have been studies on cybersecurity perceptions in Europe and the UAE, none of them have endeavoured to establish a correlation between cybersecurity perception and legislation (Maisikeli, 2020; Yalin, 2018).

Perception of cybersecurity among individuals has been the focus of only a small number of research studies (Ani et al., 2019). The public's understanding of cybersecurity is not well-documented. Academic research primarily examines broader security trends rather than public perceptions and attitudes towards cybersecurity. As a result, there is inadequate data on public perceptions of cybersecurity risks to inform legislative efforts (Kostyuk & Wayne, 2021). The process of creating laws must be adjusted to fit the unique context of each country, and it must take into account the input of local communities in order to achieve positive results (Kunyenje & Chigona, n.d.; Onyango, 2021).

Additionally, there are constraints when it comes to the data collection methods utilised in cybersecurity studies. Many of the studies conducted on cybersecurity legislation have utilised document analysis as a data-gathering method (Adomako et al., 2018; C3SA, 2022; de Barros & Lazarek, 2018; Orji, 2018; Osho & Onoja, 2015). The current studies on cybersecurity legislation development lack sufficient utilisation of empirical data to substantiate the practicality of the obtained results. Furthermore, the majority of cybersecurity research has been centred around Western communities, making it inappropriate to apply these findings to other cultural contexts. Therefore, it is crucial to understand the human dimensions of cybersecurity within the African context (Rohan et al., 2021).

Chapter 3: Research Methodology

The study investigates how stakeholders' perceptions about cybersecurity affect the outcomes of the Computer Crime and Cybersecurity Bill. This section describes a systematic approach to how the researcher goes about discovering knowledge (Creswell & Clark, 2007).

3.1 Research Philosophy

The research adopts a subjectivist ontological stance, as the constructs under investigation, such as perceptions and outcomes, rely on the interpretations of social actors and their perception of reality. The chosen Ontological stance describes the nature of existence and being; it aligns with the belief that the views of the participants in the study directly influence the study, and their experiences form part of the study (Creswell & Clark, 2007).

This study is based on an interpretive epistemological belief. This approach to understanding knowledge allows the researcher to take into account the environment of the individuals being examined to comprehend the subject being studied (Saunders, Lewis, Thornhill, & Bristow, 2019). In this context, it was more suitable to adopt an interpretive paradigm as it helped the researcher to understand the thoughts and actions of the participants. Interpretive epistemology also enabled the participants to reveal various interpretations of what they perceived about cybersecurity. The research is based on the view that reality is composed of social components expressed in language, consciousness, shared meaning, and values (Walsham, 2006). Interpretivism is suitable for this study because it reveals insights about the subject of the study and enables the researcher to understand the participants' thoughts, feelings, and beliefs (Klein & Myers, 1999).

3.2 Research Methods

Qualitative research methods were employed in this study. In qualitative research, insights into the research topic are derived from the experiences of the participants (Gerring, 2017). The research question seeks to understand how perceptions about cybersecurity affect the outcomes of the Computer Crime and Cybersecurity Bill. Qualitative research methods allowed the researcher to make sense of people's experiences within the study setting.

The qualitative research method also enabled the researcher to bring insights beyond the evidence and provided an understanding of the phenomenon holistically (Myers, 2013). Relationships between research subjects were uncovered to justify the "why and the how" questions in the study (Myers, 2013).

3.3 Approach to Theory

There are three main ways to develop theories: deductive, inductive, and abductive. The deductive approach involves deriving patterns from observations to form explanations and theories (Mitchell, 2018) .

The inductive approach begins with a series of specific observations from the data, which leads to a general conclusion (Mitchell, 2018). The abductive approach addresses shortfalls in both the deductive and inductive approaches while also using the same advantages of both approaches of reasoning and logical inference. It also follows a pragmatist philosophy (Mitchell, 2018).

This study utilised an inductive or bottom-up approach. The rationale behind this choice is that the inductive approach places significant emphasis on interpreting the subject and observations to develop an understanding of cybersecurity perceptions and their impact on the outcomes of the Computer Crime and Cybersecurity Bill. The inductive approach is preferred in interpretive research (Saunders et al., 2019).

3.4 Research Strategy

The research strategy outlines the methodical approach to accomplishing the research goals; it serves as a strong foundation for research (Farquhar, 2012). The chosen research approach for this study is a case study. Case study research involves the use of various data collection methods from several sources to examine the research subject within its natural environment (Yin, 2015). A case study is appropriate for this study because the research objective was to understand the process of the Computer Crime and Cybersecurity Bill development in Lesotho.

A case study is appropriate where the researcher seeks to establish causal links between actors in their environment; it is also appropriate when seeking to answer the 'where' or 'how' type of questions (Yin, 2015). A case study also provides an opportunity to gather a holistic understanding of a phenomenon due to its emphasis on focusing on a single group or a single instance (Yin, 2015). One of the criticisms of the case study method is its lack of

generalisability. In this study, this shortfall was minimised by ensuring that the sample was composed of individuals from different groups within the population (Yin, 2015).

3.5 Sampling

The following section outlines the sampling methodology employed in the study. Sampling involves the systematic selection of a subset of the total population to gather data and draw conclusions about the entire population (Bhattacherjee, 2012).

3.5.1 Sampling techniques

This study used purposive sampling with snowballing. Purposive sampling is used to provide conclusive results on time (Etikan, 2016). This sampling technique was used to identify and select participants to include in the study who provided information about the research phenomenon. These participants needed to have had prior exposure to the phenomenon being investigated in the study (Sekaran & Bougie, 2013). Additional participants were included in the study based on the recommendations of those who had already participated in the study (Biernacki & Waldorf, 1981).

The participants of the study had good knowledge of the phenomenon; hence, they provided rich information. Purposive sampling results in “the most productive sample” to answer the research question (Marshall, 1996). Purposive sampling has its limitations, as it can be challenging to justify the representativeness of the sample employed (Sharma, 2017). To minimise this shortfall, maximum variation sampling was employed to ensure that the sample chosen was representative.

3.5.2 Unit of Analysis

The unit of analysis is what the researcher is interested in saying something about; it is the focus of the study (DeCarlo, 2018; Grünbaum, 2007). In this study, the unit of analysis is the stakeholders of the Computer Crime and Cybersecurity Bill, since this study seeks to understand the effects of stakeholder perceptions about cybersecurity on the outcomes of the Computer Crime and Cybersecurity Bill.

3.5.3 Target Population

The target population is the individuals who were stakeholders in the development of the Computer Crime and Cybersecurity Bill process. The population was composed of only the stakeholders who participated in the development of the Computer Crime and Cybersecurity Bill. They included stakeholders from the Government in the Ministry of Communications, Science, Technology, and Innovation. Some of the participants also included legal experts, the educational sector, Private sector organisations, non-government organisations and telecommunications companies. The sample was drawn from this population based on the sampling method used in the study and the research strategy employed.

3.5.4 Sampling size

The sample for the study was composed of stakeholders from different organisations with different responsibilities. In qualitative research with fewer than 20 participants, the researcher establishes and sustains a direct connection with the participants, which enhances the free flow of information (Crouch & McKenzie, 2006). A total of 35 stakeholders from different organisations, such as private and government, were contacted to request an interview. Of the 35, 17 agreed to participate. Some participants were willing to take part in the Interview, while others did not participate due to the unavailability of time. The 17 participants used in the study formed the sample size. There were no new insights acquired from the participants between the 15th and 17th interviews, hence, no further interviews were conducted. Research demonstrated that in a qualitative study, where 60 participants were interviewed, saturation was reached at the 12th Interview (Vasileiou, K., Barnett, J., Thorpe, S., & Young, T., 2018). While another study showed that saturation was reached by the 9th Interview (Hennink, Kaiser, and Marconi 2017).

Conclusions reached about the sample were applied to the rest of the population. Participants were invited telephonically or via email to participate in the study. The process of seeking additional participants was repeated until saturation was reached.

3.6 Data Collection

The study used two data collection techniques: semi-structured interviews and documentary review. Data was collected between February and June 2023. Only 8 out of 17 interviews were

conducted in person, while 9 were conducted using Microsoft Teams. The sources of data were from Interviews and from two documents, as per Table 3.1.

Table 3.1: Sources of data used in the research

Description	Total Number
Total number of contacted stakeholders	35
Total number of conducted interviews	17
Total number of documents used	2

3.6.1 Semi-structured Interviews

The respondents to the interviews were from different organisations. Table 3.2 lists the organisations to which the respondents belonged. They range from Government Ministries to government agencies to private companies such as Internet service providers and security agencies, and one respondent was from a higher education background.

Table 3.2: Organisations of the respondents

Type of Organisation	Number of Participants
Government Ministry	6
Government Agency	3
Internet Service Provider	3
Civil Society	2
Security Agency	2
Tertiary Education	1

Each interview lasted from 30 minutes to one hour. Two documents, the Computer Crime and Cybersecurity Bill and the SADC Model Law on Cybersecurity, were used to acquire additional data for the study and form the basis for secondary data gathering.

Interviews provided an opportunity for the researcher to collect rich data that cannot be collected by other data collection techniques, such as surveys (Denzin & Lincon, 2011). The interviews in this study consisted of pre-defined questions and follow-up questions, which solicited clarity and deeper understanding from the participants (Gill, Stewart, Treasure, & Chadwick, 2008).

Semi-structured interviews were preferred because of their ability to provide detailed and clear information due to the option they provide to drill deeper by using follow-up questions. Meeting recordings were made to capture the responses of the interviews, and the data from the recording was transcribed into text for analysis. The objectives of the study guided the research questions. The interview questionnaire was divided into three main sections: stakeholder's perceptions about cybersecurity, sources of perceptions, and the relationship between perceptions and the sources of perceptions. The method of data collection utilised in the research aligns with the interpretive paradigm, the inductive approach, and the qualitative method employed in the study (Tanner & Du Toit, 2015).

3.6.2 Document Review

Secondary data was collected through the Computer Crime and Cybersecurity Bill document and the SADC Model Law on Cybersecurity document to supplement the primary interview data. Document review involves an analysis of data to extract significance and valuable insights from various documents (Bowen, 2009; Myers, 2013). Table 3.3 shows the documents used in the study and how they were used to derive data to achieve research objectives.

Table 3.3: Documents used in document review

Document name	Source	How it was used
Computer Crime and Cybersecurity Bill	(Lesotho Senate, 2022)	This document was transcribed into themes. Outcomes of the Bill were derived from this document
SADC Model Law on Cybersecurity	(ITU, 2013b)	This document is the basis of the Computer Crime and Cybersecurity Bill. Its contents were compared with the Bill

		to determine the degree of contextualisation performed on the Bill.

3.6.3 Pre-test the research instrument

In this study, a pre-test was conducted with a group of five participants. The participants were asked to review the questions and recommend improvements. This was necessary to measure the amount of available information on the research topic.

The participants reviewed the questions and suggested improvements in terms of wording and relevance to the study. Revisions were made to the questions to align them with the recommendations from the participants. Further changes were also made to the structure the wording of the questions; these changes were incorporated before conducting full-scale interviews. The data gathered from the pre-test was only used to improve the research instrument, and the participants who took part in the pre-test also participated in the data-gathering interviews.

3.7 Data Quality

To ensure the quality of data in the study, reliability and validity were verified. Patton (2002) states that research validity is the extent to which data collected is credible and accurate. Reliability of data refers to the consistency of the data from multiple sources using different techniques (Bernard, 2011).

3.7.1 Data Validity

To ensure validity of the data, the accuracy of the data was checked using triangulation, where data collected from interviews was checked against the document review data to ensure accuracy. The purpose of using this method was to mitigate the limitations that may arise from using a single data collection method (Maxwell, 2018). Care was also taken to ensure that the researcher's biases did not influence the results; the original data collected from the interviews and document review were used without alterations and in a traceable manner (Oates, McLean, and Griffiths 2022).

3.7.2 Data Reliability

The reliability of the data was monitored throughout the study to ensure consistency of the findings with other similar studies and other data sources, such as the data from the document review process (Baumann, 2016; Bernard, 2011, Oates, McLean, and Griffiths 2022). The researcher also conducted interviews with a sufficient number of participants until there was no new information from the Interviews. Data was also coded several times to ensure consistency of codes. Data collection methods used were also defined clearly. A verification of the relevance of the research objectives and data gathering methods was also conducted (Morse, Barrett, Mayan, Olson & Spiers, 2002).

3.8 Data Analysis

Qualitative data analysis was employed in this study, which is a systematic method for extracting knowledge and understanding from qualitative data. This serves as an approach to share and pass on available knowledge to others (Leech & Onwuegbuzie, 2007). Thematic Analysis is a qualitative data analysis technique. It was used to analyse data from the interviews and the document review in this study. The steps followed in Thematic analysis are shown in Table 3.4

Table 3.4: Stages of the thematic analysis process (V. Braun & Clarke, 2006)

Stage of thematic analysis	**Description**
Familiarisation with data	This is a process of transcribing the data, getting familiar with it, and creating meaning out of it.
Generating initial codes	Interesting and relevant data is organised into meaningful groups.
Searching for themes	Different codes are sorted into potential themes. Coded data extracts within the identified themes are grouped.

Reviewing themes	The themes are checked to ensure that they form a coherent pattern, they are also checked against the coded extracts.
Defining and naming themes	The themes are renamed based on their intended meaning and their content to ensure that the true meaning is captured accurately.
Producing report	A report is produced consisting of the coherent logical non-repetitive representation of the data, the report also provides linkages and relationships between the themes in relation to the research.

Thematic analysis is well-suited for interpretive research as it allows for the examination of various interpretations of a research phenomenon (Saunders et al., 20019). This process assists the researcher in developing theory and answering the research questions. The approach is flexible and allows for large and small data sets to be studied (Saunders et al., 2019).

Thematic analysis is also suitable for case study research; it is easy to perform and quick to analyse data, and it is therefore appropriate for new researchers (Thomas, 2006). It helps to summarise and generalise large amounts of data, provide meaning, and reveal insights (Thomas, 2006). The interview data was transcribed and saved in NVIVO software. The software facilitated the coding process, the categorisation of the data, and the production of meaningful insights from the data (Altuna & Lareki, 2015).

3.9 Ethical Considerations

Ethical conduct is necessary in conducting research, as it ensures truthfulness, thoroughness, objectivity, and relevance in the research process (McNabb, 2002). In this study, ethical considerations were made to guide the study. The University of Cape Town's Faculty of Commerce Ethics Board approved the research design before data collection commenced. There was a formal letter that was issued to participants seeking the participants' voluntary

participation in the study. The letter also stated that the participants were free to opt out of the study without notice.

The semi-structured interviews were designed to gather insights from individuals without requesting any personally identifiable information. The data collected was handled with confidentiality, and the anonymity of the participants was also ensured. The information collected from the study did not expose the security stance and weaknesses of any entity or organisation. The researcher funded the study, thereby avoiding any potential conflict of interest..

3.10 Summary

The study adopted a constructivist approach and employed an interpretive paradigm. A qualitative research approach was also used. The study followed the case study method of the development of Computer Crime and Cybersecurity in Lesotho. Purposive sampling was used to target a sample of 17 participants who were involved in the formulation of the Bill. Snowballing was used because the initial list of participants provided by the organisers of the formulation process was small; additional participants were identified from the recommendations provided by participants already interviewed.

Data was collected using semi-structured interviews in early 2023. The study also used the Computer Crime and Cybersecurity Bill and the SADC Model Law document for secondary data. Thematic analysis was also used to review and analyse the interview and document review data to come up with themes from the data. The data from the themes and relevant literature was used to answer the research questions.

Chapter 4: Case description

This chapter describes the development of the Computer Crime and Cybersecurity Bill of Lesotho, which is the case chosen for this study.

4.1 The Country of Lesotho

Lesotho is a small nation in the Southern part of Africa, landlocked within the borders of South Africa, at an altitude of 1,400 meters above sea level (World Bank, 2022). The population of Lesotho is 2.3 million, and 25% of the country's population lives in urban areas (World Population Review, 2024). The GDP per capita was $1,045.9 in 2022. Almost 40% of the population resides beneath the global poverty threshold of $1.25 USD per day (World Bank, 2022). Lesotho is a least developed country, characterised by severe economic barriers and poor quality of life and human development (UN, 2021). Least developed countries are defined as nations with an extremely low per capita income. They are the most vulnerable and weakest countries (Maksimov, Wang, & Luo, 2017). Lesotho has deficient health and very low economic activity (ITU, 2021).

4.2 Technology Usage in Lesotho

Lesotho has a literacy rate of 85%, higher than most countries; the majority of the literate population is female (World Bank, 2022). The use of technology in Lesotho has grown rapidly with the introduction of mobile money platforms and online transactions. This study has shown that more and more citizens have relied on technology for some of their regular activities. In 2010, only 4% of Lesotho's population had access to the internet (World Bank, 2022). This percentage increased to 48% in 2020. Additionally, the number of mobile phone subscribers in the country increased from 985,000 in 2010 to 1.5 million in 2020 (World Bank, 2022).

4.3 Cybercrime in Lesotho

As a result of this rise in technology usage, the attack surface for cybercrime has significantly increased (Mosola et al., 2019). There have been reports of cybercrime occurring in the country. Some of these crimes are financial fraud, social media harassment, and politically motivated crimes to destabilise the government (Respondent 14 and Respondent 15).

"*Recently, there was a cyber-attack on the government financial system that almost paralysed our systems; this could have driven the urgency of the Bill"* [Respondent 1].

An assessment of the country's cybersecurity maturity was conducted in 2022. The findings were that Lesotho was still in the startup stage regarding cybersecurity capability (C3SA, 2023). The country lacked the required basic capabilities, such as a law on cybercrime.

4.4 International Agreements on Cybersecurity

Lesotho is a signatory to many international agreements, as per Table 4.1; these agreements focus on cybersecurity as a priority area. This suggests that the collaboration of nations on issues of cybersecurity is critical to fighting cybercrime. These agreements include the African Union Convention on Cybersecurity, the ITU Global Cybersecurity Agenda (GCA) of 2007, and the Commonwealth Cyber Declaration 91 of 2018 (African Union, 2015; Commonwealth, 2018; UN, 2021). These agreements promote cooperation on cybersecurity through the provision of technical and financial support for the development of cybersecurity controls and capacity-building initiatives. As a member of SADC, Lesotho is also expected to benefit from the SADC Model Law on Computer Crime and Cybersecurity of 2012, which was created to harmonise legislation in the region (MISA, 2021).

Table 4.1: International cybersecurity Agreements that Lesotho participates in

Regional Organisation	**Agreement or Tool**	**Year of commencement**	**Objective**
International Telecommunication Union (ITU)	ITU Global Cybersecurity Agenda (GCA)	2007	Promotes global cooperation on cybersecurity issues, including skills and information sharing and legislation interoperability (ITU, 2007).
Southern African Development	Model Law on Computer	2012	Providing guidance for member countries to create harmonised cybersecurity laws (MISA, 2021).

Community (SADC)	Crime and Cybersecurity		
African Union (AU)	Convention on Cyber Security and Personal Data Protection	2014	It implies obligations on member countries to develop domestic laws on cybersecurity to control cybercrime in the region (African Union, 2015).
Commonwealth	Commonwealth Cyber Declaration 91	2018	Requires member countries to create a secure cyber environment for the purpose of promoting sustainable development (Commonwealth, 2018).

4.5 SADC Model Law on Cybersecurity

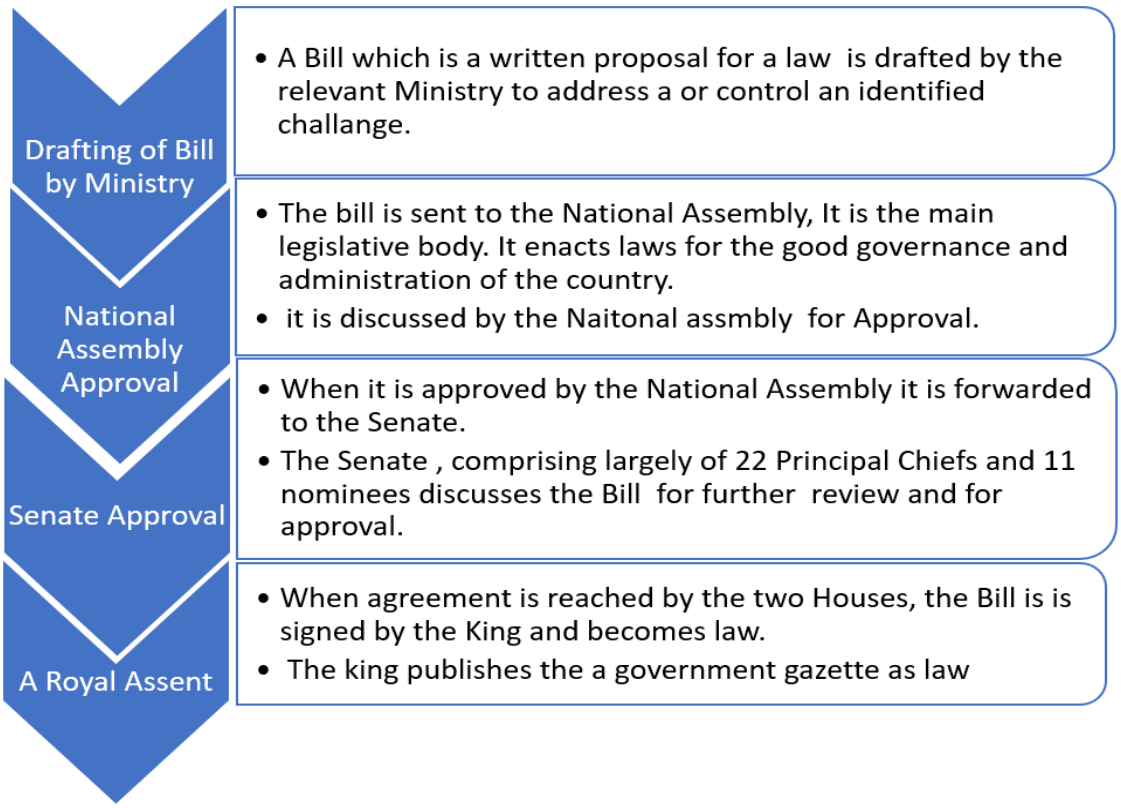
The SADC ICT Ministers adopted the Computer Crime and Cybersecurity model law at an annual meeting held in Mauritius from 6-8 November 2012 (ITU, 2013a). The objective of the model law was to harmonise legislation on cybercrime for mutual legal assistance (MISA, 2021). The model law was designed to guide member countries in developing their domestic cybersecurity laws by transposing the model law. In March and April 2013, SADC held two workshops to guide Lesotho on how to transpose the Model Law (ITU, 2013b).

Lesotho used the model law provided by SADC to create the Computer Crimes and Cybersecurity Bill. One of the study's respondents pointed out that "We used a model that was developed by SADC and other international organisations" (Respondent 17). ITU provided a consultant to Lesotho to assist with the expertise needed to develop the Bill. In 2013, the country embarked on the journey to formulate the Computer Crimes and Cybersecurity Bill, as shown in Figure 4.1.

4.6 Lesotho's Cybersecurity Legislation Development Process

The legislation development process originates from a draft law (Bill) developed by the relevant Ministry, the process of which is provided in Figure 4.1. The process of formulating a law in Lesotho is aimed at formally addressing a common unfavourable condition in the

country that affects citizens. The problem is then presented to the state for attention and resolution (Mohammed, 2020). The draft is presented to the National Assembly by the Minister responsible for the subject of the Bill (Machepha, 2010). Upon approval by the National Assembly, the Bill is presented to the Senate for review and approval. The two approvals form a basis for the King to give a Royal assent, and the publication of the Bill into Law follows hereafter (Machepha, 2010).



***F*igure 4.1: Process of Developing a Law from a Bill in Lesotho (Machepha, 2010)**

4.7 The Computer Crime and Cybersecurity Bill

Lesotho does not have a cybersecurity Law at present; there is, however, a draft law, namely the Computer Crime and Cybersecurity Bill. The objective of the Bill is to create a safe cyber environment for the country by criminalising cybercrime (Mosola et al., 2019; Mpaki, 2022). Due to the increased usage of technology, Lesotho is already experiencing incidents of cybercrime, which have led to financial loss and leakages of information (Mosola et al., 2019; Thuraisingham, 2023).

From the year 2013 to 2019, Lesotho drafted the Computer Crime and Cybersecurity Bill, as shown in Figure 4.2. The first draft of the Bill was presented in Parliament in 2021. Parliament rejected this draft due to insufficient consultation. The security agencies, media houses, and telecommunications agencies were not consulted sufficiently on the formulation of the Bill (National Assembly, 2021). Parliament also directed that security agencies be included in the Cybersecurity Advisory Council membership. Parliament further suggested that the Bill should distinguish between Computer crime and Cybercrime to avoid being vague and complicated to implement (National Assembly, 2021).

The Bill was reviewed and presented to Parliament for the second time in 2022 after additional review and engagement (Ndebele, 2023). The Bill has been waiting for Royal assent, after which it will become a law.

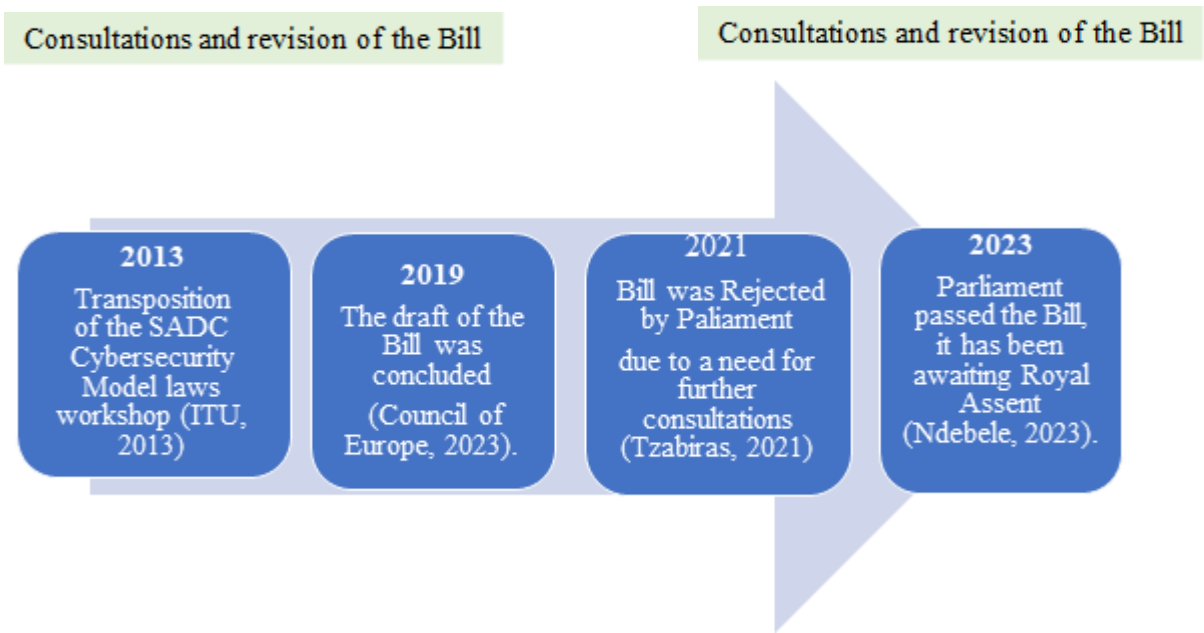


Figure 4.2: Timeline of the Bill's formulation

4.8 Political Environment Impact on the Development of the Bill

Lesotho had frequent changes in government administrations between 2012 and 2023 due to political instability ('Nyane, 2022). The government leadership changed between the All-Basotho Convention party (ABC), Democratic Congress (DC), and Revolution for Prosperity (RFP) party, as shown in Figure 4.3. The process for the development of the Bill was delayed

by the need for new consultations for every government change (Respondent 17 and Respondent 6). The findings also indicated that there was a lack of political will to see the Bill formulation process completed.

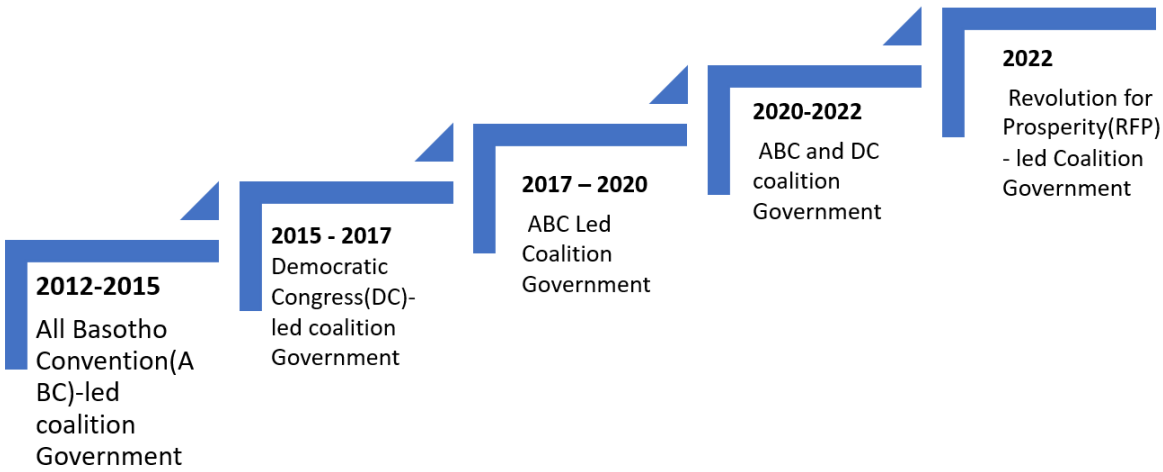


Figure 4.3: Government Changes in Lesotho since 2012 *('Nyane, 2022)*

4.9 Summary

In this section, the context of the study, which is Lesotho's Computer Crime and Cybersecurity Bill development process, was introduced. The country's unique geographic, population, economic and technological environment was described. The process taken to develop the Computer Crime and Cybersecurity Bill was also shown; this also included the challenges that the country faced. The formulation process was heavily supported and influenced by international community stakeholders such as SADC and ITU, with technical resources assisting in the process. There was insufficient consultation with important local stakeholders in the process. This stakeholder included the security and telecommunications agencies. The unstable political climate caused frequent changes in government administrations, resulting in the need for repeated consultation, thus delaying the formulation of the Bill.

Chapter 5: Research Findings and Discussions

5.1 Introduction

The following section outlines the primary findings derived from the research, along with an analysis and interpretation of the results. The discussion highlights the implications of the findings while also aligning them with the existing literature. The study's objective is to investigate how stakeholders' perceptions about Cybersecurity influenced the outcomes of the Computer Crime and Cybersecurity Bill in the context of Lesotho. The research also determined stakeholders' perceptions about cybersecurity and investigated the causes of those perceptions while assessing the challenges encountered in the Bill's development process.

5.2 Stakeholder perceptions about cybersecurity

Stakeholders' perceptions about cybersecurity have been grouped into three categories:

- Descriptive perceptions: respondents explained what cybersecurity is about in the context of Lesotho;
- Functional perceptions: explains what cybersecurity is useful for;
- Administrative perceptions: describes the measures and processes that make up a secure cyber environment.

5.2.1 Descriptive perceptions of cybersecurity

Descriptive perceptions are about how stakeholders define cybersecurity and understand its meaning. The participants had various perceptions of cybersecurity. Table 5.1 summarises how the respondents understood the concept.

Table 5.1: Descriptive perceptions of cybersecurity

Themes	**Sample Quotes**
cybersecurity is about the protection of people and information	*"Cybersecurity must be looked at from the point on what we can do to protect our people*" (Respondent 4). *"Protection of personal information, here at home there are people who have access to personal information, especially for those people such as communication agencies, even the idea of registering our SIM cards is also adding to that protection"* (Respondent 16).
Cybersecurity is about National Security	*"I define it as the state of national security in terms of the country's information"* (Respondent 1).
Cybersecurity is borderless	"*Borderless threat, cybersecurity crosses geographic regions, it is an international problem"* (Respondent 5).

The respondents perceived cybersecurity to be about ensuring that information is protected, whether in transit or at rest (Respondent 1). One respondent notes, *"It will have a protection in terms of usage of technologies*" (Respondent 12). Cybersecurity enables the protection of assets in cyberspace by creating layers of defence around the networks, computers, application software, information, and people (Sheth, Bhosale, & Kurupkar, 2021). The information may belong to a private citizen, an organisation, or the state.

Research indicates that the protection of information falls within the scope of a subset of cybersecurity called Information security, which deals with protecting information in all its forms: digital, physical, and otherwise (Ezumah & Adekunle, 2012). The basic premise of cybersecurity is the protection of people and digital assets from criminal activity in cyberspace (Tomšů, 2021). It may be implemented through means such as awareness and application of controls, such as laws and policies. It may also be implemented through the application of technological measures such as firewalls and antimalware.

The findings indicated that cybersecurity is a component of the overall national security of a country (Respondent 1). "*Security in terms of national security*" (Respondent 5). This view is also supported by some studies that claim that promoting a secure cyberspace ensures the

country's overall national security (Vakulyk et al., 2020). Unlike on land, air, and sea, where governments have predefined territories and barriers that define control boundaries, cyberspace is more complex to defend (Sheth et al., 2021). The biggest threat to national security for most countries in the 21st century comes from cyberspace because traditional security measures are not applicable to cyberspace (Reveron & Savage, 2020).

Cybersecurity is also essential for a country to achieve its strategic interests through the use of technology (Vakulyk et al., 2020). This suggests that strategic national interests may require a secure cyberspace. These interests could range from international trade to investments and donor funding. Some nations, such as South Africa, have strategies that proactively anticipate cybersecurity challenges. This is done to protect the country against cyber warfare and to safeguard the country's information and Infrastructure (Fonseca & van Wyk, 2021).

The respondents perceived that cybersecurity is borderless, extending beyond physical and geographic barriers (Respondent 5). "*But we all know that cyber issues are the same everywhere; it is borderless. It happens everywhere*" (Respondent 7). Participants' understanding of the transborder nature of cybercrime seems to be accurate. It has become necessary that countries collaborate their efforts and harmonise legislation to effectively combat cybercrime (Klimburg & Almeida, 2019; Yan, 2022). Challenges faced by one country may not differ from those faced by the next country. A country with a weak cyber environment may become an easy target for cybercriminals (Kshetri, 2019). Criminals may conduct cybercrime from any country in the world, which may affect users in multiple countries.

5.2.2 Functional perceptions of cybersecurity

Functional perceptions describe how cybersecurity can be applicable to the country and its different areas of utilisation. Table 5.2 summarises functional perceptions of cybersecurity gathered from participants in the Computer Crime and Cybersecurity Bill's formulation process.

Table 5.2: Functional perceptions of cybersecurity

Themes	**Sample Quotes**
Basotho are at risk	*"We are exposed as a country due to risk; we need to focus and address those issues"* (Respondent 5).
Cybercrimes in Lesotho	*"People are being harassed and abused online for political gains; the social media platforms are being misused"* (Respondent 2).
Dealing with crime	*"For people to be free and have the understanding that if I do anything, I will be exposed, and they could be caught"* (Respondent 2).
Safe use of technology	*"It is relevant because of our increasing number of people using technology and smartphones using the Internet"* (Respondent 7).
Privacy and information rights	*"For instance, the registration of SIM cards has elements of invasion of privacy, even though it would help the police or the ministry"* (Respondent 15).
Lesotho's attractiveness to cyber criminals	*"Maybe we are not so attractive as a country. But we need to be cyber-ready in case anything happens in the future"* (Respondent 4).

The finding indicated that Lesotho is rapidly expanding its use of technology, and as a result, it has become exposed to many risks in cyberspace (Respondent 5). These may imply that the country is becoming more vulnerable to cyberattacks. *"We are exposed as a country due to risk; we need to focus and address those issues*" (Respondent 5).

Research shows that increased use of technology in a country without laws to manage the risks promotes cybercrime (Mosola et al., 2019). The risks range from children being exposed to pornography on the Internet, cyberbullying, leaking of private and confidential information online, and financial crimes (Respondent 10 and Respondent 11). The risks could be a result of the user's lack of knowledge of cybersecurity. Research shows that Lesotho, like many

African nations, is fertile ground for cyberattacks, and it is vulnerable to malicious cyber activity (Mosola et al., 2019)**.**

There have been some incidents of cybercrimes in Lesotho, and according to the respondents, some of these crimes occur over social media. *"The other issues have to do with badmouthing on social media because this conflicts with human rights, so there is a lot of cyberbullying*" (Respondent 10). Studies also indicated that there has been incidents of cybercrime activities in Lesotho reported in recent years, including hacking, phishing, identity theft, and fraud (C3SA, 2023; Mosola et al., 2019; Thuraisingham, 2023). The very presence of these crimes may indicate that cybercrime is a real challenge to Lesotho. This may be why participants perceived cybersecurity as about preventing these crimes.

The findings indicated that cybersecurity is about providing the means to combat cybercrimes. This is achieved by assisting in the investigations and prosecution of offenders by empowering law enforcement authorities. *"It is something that we do require as Basotho, especially in the issues of investigating internet-related crimes; these cases were not able to be admissible in courts of law due to a lack of law to support the evidence*" (Respondent 15).

Lesotho does not currently have a law that regulates and criminalises cybercrimes, even though the country is threatened by cybercrime. Cybersecurity law formalises preventive measures to prohibit cybercrime (Nwankwo & Ukaoha, 2019; Poshai et al., 2023). It is likely that law enforcement agencies such as the police and the prosecution have no guidance for investigating cyber incidents in the absence of a law. The proposed cybercrime law will enable the country to regulate crimes such as Cyber Terrorism, Computer forgery, and Identity theft, among others (Mpaki, 2022). Studies show that Lesotho has to fast-track the development of the law due to the increasing need to assist in investigations and the prosecution of cyber criminals (Mosola et al., 2019).

The findings showed that many citizens have been using technology in many areas of their lives, ranging from buying and selling goods online to using mobile money platforms. "*To make sure that Internet service usage is promoted, ensure that it's secure enough to participate, develop an environment that is conducive for Basotho to live well and interact*" (Respondent 2).

Respondents perceived that the increase in technology usage exposed them to the threat of cybercrime (Respondent 15). Between the years 2012 and 2020, the percentage of Basotho who had access to the Internet increased by 48%, and mobile subscribers increased by 52% in

the same period (World Bank, 2022). Individuals and other entities who use the Internet share information and transactions in an environment that is neither regulated nor governed to protect their interests (Karim et al., 2019). Even though the Internet is very beneficial for improving the nation's economic activities, it may enable unethical activities such as cyberstalking, illegal trade, and many other crimes (Tomšů, 2021).

The findings also indicated that Internet users require protection from malicious activities while using the Internet through the implementation of cybersecurity. "*To conduct business in cyberspace, I need my privacy, or even if I buy online, I still need that privacy"* (Respondent 11). Cybersecurity is the protection of people and digital assets from criminal activity in cyberspace, it provides a set of measures to ensure cyber resilience (Tomšů, 2021). All participants and actors in cyberspace require safety and comfort to enjoy the benefits of cyberspace without fear of harm (Klimburg & Almeida, 2019). Cybersecurity assures Internet users by enabling controls such as policies and laws to enforce desirable behaviours (Sunkpho et al., 2018; Tomšů, 2021). Some participants believed that Lesotho is not considered a very attractive target for cybercrimes due to the high levels of poverty in the country (Respondent 4). "*The impact is minimal to us because Lesotho is not the main target due to poverty*" (Respondent 2).

This perception is not supported by research, since there has already been reports of cybercrime activities in the country (Thuraisingham, 2023). Additionally, research has shown that cybercrime has been shifting towards weak economies due to the ease of implementing crime because of a lack of controls (Kshetri, 2019). Studies also show that the absence of cybersecurity laws to support investigations and prosecution of cybercrimes enables cybercriminals to thrive (Mosola et al., 2019).

5.2.3 Administrative Perceptions

Administrative perceptions are about cybersecurity management and the measures and structures that respondents believe are required to ensure a secure cyber environment. Table 5.3 summarises the findings for administrative perceptions of cybersecurity.

Table 5.3: Administrative perceptions of cybersecurity

Themes	**Sample Quotes**
Formation of Cybersecurity Incident Response Team (CSIRT)	*"The main objective is the establishment of cybersecurity management, by establishment of cybersecurity advisory council and establishment of CSERT*" (Respondent 7).
Cybersecurity Advisory Council	*"The biggest outcomes are that we would have a council that focuses on issues of cybersecurity. It could sit now and then, and it would advise on the country's direction. It also provides pieces of advice from the financial sector and the communication sector"* (Respondent 6).
Critical Infrastructure Protection	*"That's why we are talking about critical infrastructure to be protected; if it were affected, it would affect national security*" (Respondent 6).
Compliance with international standards	*"We are also part of the global community, we need to be part of that space, we have multinational companies, we also have multinational banks, without that comfort of protection of cyberspace, we might struggle to have those players in the country"* (Respondent 13).

It was the perception of the participants that the need for cybersecurity necessitates the creation of a Cybersecurity Incident Response Team (CSIRT) in a country. "*It would be good to have such a response team also for information sharing of incidents*" (Respondent 16). The CSIRT coordinates cybersecurity intelligence information sharing (Respondent 16). CSIRT also becomes the focal point for proactive and preventive cybersecurity initiatives; the team reports to the Cybersecurity Advisory Council (Lesotho Senate, 2022). The CSIRT is also responsible for ensuring that the country has adequate plans and capacity to respond to cybersecurity incidents (Mosola et al., 2019).

Without a binding requirement for reporting cyber incidents through the CSIRT structure, organisations may hide information about their cybersecurity incidents to protect their security

vulnerabilities. It is also the responsibility of CSIRT to enforce reporting of cybersecurity incidents, to gather and disseminate this information for the purpose of proactive security improvement (Dutton, Creese, Shillair, & Bada, 2019). Research confirms that there are limited reporting mechanisms in Lesotho on cybersecurity incidents, hence the need for CSIRT (C3SA, 2022).

Participants believe that the Cybersecurity Advisory Council is necessary to manage cybersecurity at a governance and strategic level.

> "*Establishing a central governing structure that deals with cybersecurity in general, the other issue would be dealing with cybercrime using our different security agencies" (Respondent 10).*

The responsibility of the Advisory Council is to become the focal point for various national entities and to provide strategic oversight for cybersecurity matters in the country between the government and other entities (Lesotho Senate, 2022). In South Africa, the National Cybersecurity Advisory Council was established in 2013 to advise the government on policy issues and cooperation between the government and other stakeholders to tackle cyber threats (Government of South Africa, 2013).

The findings have shown that cybersecurity controls are required to ensure the continued provision of essential services by protecting Critical Infrastructure (Respondent 2). "*We talk about the resilience of the country's critical infrastructure"* (Respondent 17). Critical infrastructure may support services such as electricity, water, and health facilities (ITU, 2013b). Research also shows that these assets are protected through the identification, prioritisation, and implementation of good cybersecurity practices such as policies and laws (C3SA, 2022; Karim et al., 2019).

Critical infrastructure protection is a desired capability; it is continual monitoring and protection of essential services to prevent interference that could crimple a country (Klimburg & Almeida, 2019). Deliberate and accidental disruptions to critical infrastructure may become costly to a country's economy. They may also affect national security or threaten the lives of citizens.

Respondents also understood that Lesotho, as part of the global community, must comply with international conventions on cybersecurity.

> ” *Lesotho is a member of international organisations such as SADC, which requires that the country should have institutions and bodies responsible for cybersecurity”* (Respondent 2).

Lesotho is a signatory to agreements such as the African Union Convention on Cybersecurity, the ITU Global Cybersecurity Agenda (GCA) of 2007, Commonwealth Cyber Declaration 91 of 2018 (African Union, 2015; Commonwealth, 2018; UN, 2021). These agreements support international cooperation on cybersecurity and provide technical and financial support for developing cybersecurity controls and capacity-building initiatives. As a member of SADC, Lesotho is also expected to transpose and domesticate the SADC Model Law on cybersecurity (MISA, 2021).

5.2.4 Implications of Stakeholders' Perceptions

The findings indicated that the language barrier has been a challenge for the communication of cybersecurity information in African countries (Kshetri, 2019). Due to the language barrier, most Basotho may have a limited understanding of cybersecurity. Policies, laws, and awareness communication should be provided in the two official languages, Sesotho and English, to ensure buy-in and understanding among Basotho. It is necessary to ensure that all cybersecurity information, including Laws, awareness information, and all other communication, is received by users irrespective of their language abilities (Ngo, Deryol, Turnbull, & Drobisz, 2024).

Cybersecurity also has economic implications on the country in the form of financial loss and investor confidence (Vakulyk et al., 2020). The findings indicated that the presence of a secure cyberspace may improve foreign direct investments and donor funding. Research has shown that 54% of investors and 67% of CEOs believed that a lack of cybersecurity was a big factor when investors make investment decisions. There is, therefore, a requirement for cybersecurity for the protection of investments and to enable sustainable business (PricewaterhouseCoopers, n.d.). Lesotho, as one of the least developed countries, depends on foreign investments and donor funding to support its development (Mukherjee et al., 2020). These findings may also raise the government's awareness of the necessity of cybersecurity for the country’s economic development.

As a result of a lack of Cybersecurity regulation, law enforcement authorities have a difficult time conducting investigations and presenting electronic evidence about cybercrime, resulting in a safe haven for cybercriminals (Mosola et al., 2019). According to the findings, the courts

of law do not have strong grounds to admit evidence brought forward through digital means. Even though this perception is valid, it is limited because there cannot be a vacuum in law. In the absence of cybersecurity legislation in a country, it is practical to resort to applying the principles of common law to enforce cybercrime prevention, though it may apply to some cases, common law application is limited and narrow in scope (Snail Ka Mtuze & Musoni, 2023).

The findings indicated a scarcity of reports of cybercrime incidents in the country (C3SA, 2023), which may lead to ignorance and inaction from the government to create preventive controls such as awareness campaigns and legislation. The intelligence information that CSIRT provide could create awareness among relevant stakeholders, such as the government, to allocate resources toward combating cybercrime (ITU, 2024). A lack of awareness and information about the risk of cybercrime could be attributed to the absence of a coordinating body, such as a CSIRT in the country.

Since Lesotho has not implemented Cybersecurity legislation, as a result, the country is not compliant with international agreements that it has committed to uphold. These agreements include the ITU Global Cybersecurity Agenda (GCA), the Convention on Cyber Security and Personal Data Protection, and others (African Union, 2015; Commonwealth, 2018; UN, 2021). This lack of compliance could result in the country losing credibility, suffering reputation loss, and risking sanctions from the international community (Guzman, 2005). International agreements are contractual in nature; they define expected conduct and expectations between countries, and a lack of compliance is a breach of contract (Guzman, 2005).

5.3 Sources of Perception about Cybersecurity

The sources of perceptions about cybersecurity were gathered from the interview and document analysis process. These are factors that may have influenced the participants' perceptions about cybersecurity. They were grouped into four categories.

- Training and Education
- Awareness of cybersecurity
- Social-Cultural context
- Political environment's influence on Perceptions

5.3.1 Training and Education

At least 7 out of 17 respondents received training and education opportunities in cybersecurity before attending the Computer Crime and Cybersecurity formulation workshops. The training allowed those who received it to participate meaningfully in developing the Computer Crime and Cybersecurity Bill. The forms of training received by participants are shown in Table 5.4.

Table 5.4: Training and Education on Cybersecurity

Themes	**Quotes**
Cybersecurity Education	*"I also did my Masters in Internet Law and Policy. I also became more interested, and I completed an information security qualification; I also went further and became certified in cybersecurity. I also realised that the area has a lot of potential to grow and become very big" (Respondent 8).*
Learning from work	"*The nature of the work that one does requires research and self-knowledge, and hence, people who work more on security will have to know more"* (Respondent 2).
Training	"*What made me interested in the Bill was that I was also in the space, I wrote CISSP, and I am doing CISM, I am also doing CISCO cybersecurity, I am also doing AWS in cybersecurity"* (Respondent 8).
Self-Learning	*"No formal education, just informal upskilling, personal research out of interest, I'm appointed as a systems security officer, nothing real happens on the ground, way too limited considering what security is about"* (Respondent 1).
Learning through workshops	*"I attended some workshops in SADC, cybersecurity drills, and also took a course in Japan"* (Respondent 2).

Respondents identified training as a source of cybersecurity perception. They believed that providing cybersecurity training could enable a secure cyberspace in Lesotho (Participant 12).

> *"One of the main objectives of COBIT 2019 is to manage security from their IT operations. I have attended courses relating to firewalls, and I also did CISCO and ethical hacking*" (Respondent 10).

Training and education require resources such as financial resources and experts to transfer skills and knowledge about cybersecurity (Dutton et al., 2019). It has also been suggested by research that training and education are the means to empower societies with information that enables them to reach their goals of reducing cybersecurity risk (Creese, Dutton, & Esteve-González, 2021).

Knowledge acquired through education may also affect how people view cybersecurity and change their behaviour while using technology. The behaviourism learning theory may be used to explain how capacitation affects people's perceptions of cybersecurity. The theory posits that information provided to an individual is coded in memory, and it is responsible for affecting decision-making and a person's behaviour (Bryant, Vincent, Shaqlaih, & Moss, 2013). This suggests that through training and education, society may gain knowledge of cybersecurity, understand the risks present in cyberspace, and change their behaviour while using technology online.

Most African nations' education systems lack a cybersecurity curriculum, which is a requirement for security control development (Bada et al., 2019; Mogoane & Kabanda, 2019). The best way to enable people to understand cyberspace risks is to impart education and awareness (Haney & Lutters, 2018). Education has also been said to be necessary to promote the required cybersecurity culture in a country (Creese et al., 2021).

There is a lack of skills in the field of cybersecurity in the country, like in many other African countries (Adomako et al., 2018). In a study conducted by the African Union Commission and United Nations Development Programme in 2020, African countries had an average of 21% competence in cybersecurity (Cheimbi, 2023). The Findings indicated that participants in the formulation of the Bill could have been more effective in the discussion leading to the development of the Bill if they had prior training on the subject (Respondent 15). Cybersecurity skills are critical for strategic thinking and planning for activities to combat cyber risks (Ron et al., 2018).

Some higher education institutions in the country have introduced some short courses in cybersecurity. These institutions are the National University of Lesotho, Lerotholi Polytechnic, and the Catholic Comprehensive Community College (C3SA, 2023). The short courses on offer in these institutions are yet to gain popularity amongst employers and the public (C3SA, 2023). The reason may be that these courses are currently not aligned with the demand for cybersecurity professionals in the country (C3SA, 2023). It may be necessary to offer more such courses to more schools, especially at the High school and primary levels, to promote cybersecurity to younger users since the youth are already exposed to online threats.

5.3.2 Awareness of Cybersecurity

Respondents were exposed to cybersecurity through different experiences and sources of information; this influenced their understanding and knowledge of cybersecurity. *"Exposure to what is happening in the world news channels, you hear of attacks on systems from a certain country, these raised my awareness on issues of cyber* "(Respondent 1). Table 5.5 summarises the forms of exposure that participants had to cybersecurity.

Table 5.5: Awareness of cybersecurity

Themes	**Quotes**
Technology usage	*"I am part of the nation that utilises digital systems such as banking platforms and others. We must understand what security is behind these systems before we can trust these systems"* (Respondent 4).
Information on news and media	*"Exposure to what is happening in the world news channels, you hear of attacks on systems from a certain country, which raised my awareness on issues of cyber* " (Respondent 1).
Work Experience	*"As one is in the IT sector, both private and public, we still have some sort of awareness, and we learn formally and informally"* (Respondent 1).

It was evident from the findings that participants identified cybersecurity sensitisation as a source of their perception of cybersecurity. Participants noted that awareness is also required for effective participation in the development of the Bill (Respondent 1). Sensitisation may have assisted the participants in understanding the requirements for the formulation of the Bill.

Research indicates that there is minimal awareness of cybersecurity in Lesotho in the government, private sector, and the general public (C3SA, 2023). Knowledge about cybersecurity has been said to influence the assumptions, values, and behaviours that people may have while using technology; knowledge affects perceptions about cybersecurity (Reegård, Blackett, & Katta, 2019).

Some of the respondents indicated that they learned about cybersecurity from news and social media platforms such as Facebook (Respondent 1). The information that comes from Facebook and other news platforms has been known to be prone to misinformation (Chang & Coppel, 2020). If information from news and social media platforms does not originate from reliable experts in the field, this may mislead those who listen. Some of the news may not always be a reliable source of cybersecurity information.

Research conducted in 2018 by Kaspersky indicates that 52% of cyberattacks in organisations were due to weaknesses in employees' knowledge; further studies conducted in 2021 also indicated that 85% of cybersecurity breaches were successfully implemented due to a lack of awareness (Corallo, Lazoi, Lezzi, & Luperto, 2022). This suggests that cybersecurity awareness is crucial to any prevention initiative to combat social Engineering threats.

One of the challenges that may account for the lack of awareness is the immense communication barriers that hinder the distribution of cybersecurity information. This is primarily because many Internet users on the continent do not understand English. English is the main language used to communicate cybersecurity information over the Internet (Kshetri, 2019). Some participants also cited the limited understanding of cybersecurity as a subject that is not commonly discussed.

The understanding of cybersecurity has been cited as one of the factors that could positively contribute to the establishment of laws and policies necessary to fight cybercrime (Orji, 2018). The lack of understanding of cybersecurity risks and challenges hinders awareness campaign designs and the formulation of cybersecurity controls (Bada et al., 2019). Research has shown that the majority of Internet users in Lesotho use it without clearly understanding the risks that accompany its usage (Mosola et al., 2019). The findings show that there was some understanding amongst the participants about cybersecurity. However, the level of understanding varied greatly among participants. This may suggest that there was a need to provide awareness to ensure improved understanding. It is the responsibility of the Lesotho

government to improve cybersecurity knowledge through awareness programs to promote the safe usage of technology to support cybersecurity initiatives (C3SA, 2023).

5.3.3 Social-Cultural context

The culture of Basotho was cited to have some influence on how participants perceived cybersecurity. Some aspects of Basotho culture may have a positive influence on Cybersecurity, while others may not align with the premises of cybersecurity.

> *"We also trust each other as Basotho; we believe in the goodness of a person, and we get surprised when people do bad things. Even now, in recent instances, they show that they are still very relaxed"* (Respondent 10).

Table 5.6. shows cultural aspects that may have influenced the perception of cybersecurity.

Table 5.6 Social Cultural Influence on Cybersecurity Perception

Themes	**Quotes**
Basotho like to share	*"As you have just talked about culture, we have a culture of sharing; we do not understand that we cannot share everything; it puts us at risk of cybercrime*" (Respondent 3).
Basotho are careless	*"We take things lightly without taking consequences into consideration"* (Respondent 7).
Basotho trust easily	*"Our culture is against cybersecurity; we are easily trusting; when we embrace technology, we take it as it is. We are struggling to understand that it has dangers"* (Respondent 17).
Some aspects of culture that embrace cybersecurity	*"Basotho are very careful people in terms of controlling their kids; if we used that, we would easily be able to escape such. We are no more like that; we can harness and utilise technology while still being Basotho"* (Respondent 1). *"I think Basotho, even though I haven't been exposed to many countries, we are a very conservative people, so if we say something is wrong, we all see it in that way, maybe it's because*

	we are a Christian nation, some nations don't have moral fibre. I have a feeling that Basotho will welcome this with two hands" (Respondent 15).

It is worth noting that culture is at the core of human-centric cybersecurity, as such, any cybersecurity initiative has to consider cultural aspects to be effective (Rohan et al., 2021). The findings showed that Basotho culture is diluted by many foreign influences. Some aspects of Basotho culture support cybersecurity principles, while others do not.

Basotho people are respectful; they subscribe to the protection of minors and respect of elders, and they are against harassment of minors (Respondent 1). These aspects of culture may positively influence how Basotho perceives controls and laws that govern behaviour in cyberspace. Culture can influence the way people perceive cybersecurity, culture also affects behaviour, thoughts, and feelings (Reegård et al., 2019). Perceptions may be created from past values and beliefs that people have (Niosi, 2021; Sherif & Cantril, 1945). The values and beliefs of Basotho form a part of their culture; they may influence how Basotho choose to understand cybersecurity and their behaviour in cyberspace.

Some aspects of the Basotho culture may not align with cybersecurity requirements, findings indicated that Basotho trust easily. They also respect people in authority, such as political figures and traditional leaders (Respondent 10). Information that originates from these public figures is more often trusted without question, making Basotho prone to misinformation. Research confirms that in some cultures, public figures are given more privileges and are trusted because of their social standing and sometimes even over the common good of the rest of the population (Dutton et al., 2019). Hofstede's cultural dimension theory posits that cultures with a high power distance index, such as those in Africa, accept unequal society, have a high respect for rank and authority and encourage bureaucracy (Thetsane et al., 2024). It is also noted that this only applies to a select few individuals with privileges because of their position in society (Dutton et al., 2019).

Basotho believe in the goodness of a person and expect people to be generally good (Respondent 10). Trust may be exploited by social engineering techniques to implement cybercrimes. Trust has to be accompanied by awareness of risk and caution while using technology (C3SA, 2023); Dutton et al., 2019). The findings also indicated that because of the

trust Basotho have, Basotho also have a culture of sharing (Respondent 3). This may be risky, especially when it comes to sharing sensitive or confidential information online.

5.3.4 The Influence of the Political Environment

Participants believed that the government perceived cybersecurity to be about controlling people's opinions on social media and other platforms to achieve political agendas. *"Governments also wanted to silence people on social media and also wanted to control the internet; that's the political perception of the laws"* (Respondent 8).

Like many African countries, Lesotho has a polarising political environment, which may shape the perceptions of the participants towards cybersecurity. Some participants believe that cybersecurity is required to serve some political gains, such as silencing some political factions (Respondent 1). Research has also shown that social and political factors have a direct impact on cybersecurity and how users may perceive cybersecurity (Creese et al., 2021). This is especially true in relation to the protection of personal information and the creation of controls and structures that can be put in place to ensure privacy (Creese et al., 2021). Different political agendas may account for the delays in the development of the Bill; conflicting political motives among participants may have polarised debates.

Lesotho had an unstable political environment between 2012 and 2023. Government leadership changed between the All-Basotho Convention party (ABC), the Democratic Congress (DC), and the Revolution for Prosperity (RFP) ('Nyane, 2022). The Bill's formulation process may have been delayed by the need for fresh consultations for every government change. In addition to these changes, the Bill could have been made to suit the government administration of the time without consideration of the inputs from stakeholders.

5.3.5 Implications of Sources of Perceptions

The study's findings indicated that some higher learning institutions in the country had a cybersecurity curriculum. These courses have been said to be out of alignment with the requirements of the industry and the market (C3SA, 2023). Research has shown that cybersecurity education is deficient, and governments need to invest more in cybersecurity education (van Vuuren & van Vuuren, 2022).

A review of the curriculum through consultations with the industry may be more helpful in creating alignment between industry expectations and learning outcomes. This would promote

cybersecurity and encourage more organisations to enrol in the programs. Additionally, it may be necessary to offer such courses to schools at the High school and primary level and to the elderly population to promote cybersecurity to a bigger portion of technology users (Ngo et al., 2024). This would ensure coverage of cybersecurity education to a bigger portion of the population and ensure the success of cybersecurity initiatives' implementation.

According to some of the participants, their primary sources of information about cybersecurity are news and social media. Some of the participants became aware of cybersecurity through self-learning. While these sources of information may provide some insights about cybersecurity, these platforms may lack credibility, leading to misinformation about cybersecurity (Chang & Coppel, 2020). This may be primarily because the information often comes from unverified sources, and in some cases, the sources may lack expertise in the field. The study also revealed that there is a general lack of cybersecurity skills in Africa (Malatji et al., 2021).

The data also suggested that there is a limited understanding of cybersecurity risks and challenges, which may negatively impact the formulation of cybersecurity controls (Bada et al., 2019). These may have led to the country relying heavily on external expertise in the efforts to control cybercrime. When external actors such as consultants and international organisations lead a policy or law agenda instead of engaging local experts to champion, the resulting instruments may not be sufficiently comprehensive. The result may also be that some local stakeholders may withdraw from the development process due to a lack of ownership (Kunyenje & Chigona, n.d.)**.** The lack of local expertise may also prevent the country from implementing measures to mitigate cybercrime at the individual, organisational, and national levels.

Participants also cited politicians' lack of political will to implement cybersecurity. This could have contributed to the delay in developing the Computer Crime and Cybersecurity Bill. This is despite SADC's requirement that the Bill needs to be implemented in Lesotho to collaborate and harmonise cybersecurity laws in the region. South Africa has also been said to be lacking in implementing Cybersecurity regulations. The government has been said to be reluctant to adopt cybersecurity, and as a result, the country is behind in implementing most required legislation (van Vuuren & van Vuuren, 2022). Governments must become proactive about managing the risk of cybercrime because the technology landscape is also changing rapidly.

5.4 Outcomes of the Computer Crime and Cybersecurity Bill

This section outlines the outcomes of the Computer Crime and Cybersecurity Bill, these outcomes are the issues that the Bill addresses to ensure a secure cyber environment in Lesotho. The outcomes were identified from the Bill and grouped into three categories. The first group is the list of offences stipulated in the Bill with their corresponding penalties. The second is the functions of the Bill, which indicate how the Bill would assist in fighting cybercrimes. The last section describes the structures and processes that the country should implement to manage cybersecurity.

5.4.1 Functions of the Bill

The objectives of the Computer Crime and Cybersecurity Bill document were defined to set a mandate for cybersecurity implementation. Table 5.7 shows these functions as defined in the Bill.

Table 5.7: Functions of the Computer Crime and Cybersecurity Bill

Themes	**Quotes**
Assist investigations	*"Provision for offences relating to the misuse of electronic communication devices and electronic networks; the jurisdiction and powers of investigation, search, access and seizure and collection of evidence in respect of computer crime*" (Lesotho Senate, 2022).
Protect citizens	*"Government has a responsibility to ensure that its citizens are protected against cyber-attacks and the enactment of the Computer Crime and Cybersecurity Bill is an effort by Lesotho to combat computer crime"* (Lesotho Senate, 2022).
Punishing offenders	*"by putting in place the appropriate punishment for it and thereby ensuring cybersecurity"* (Lesotho Senate, 2022).
Combat crime conducted using technology	*"However, with technology comes challenges, as criminals misuse technology to commit crime" (* Lesotho Senate, 2022).

Research shows that cybersecurity legislation is designed to prevent and control the infringement of rights and privileges in cyberspace (Nwankwo & Ukaoha, 2019; Snail Ka Mtuze & Musoni, 2023). The Bill will be a useful tool in the process of criminal investigation related to cybercrime; it will make electronic evidence usable in the courts of law (Lesotho Senate, 2022). Through the convictions that will be made possible, the offenders will receive

appropriate punishment as defined in the penalties, as shown in Table 5.8. The proposed law would also ensure that the government is mandated to protect its citizens by ensuring a safer cyber environment (Lesotho Senate, 2022). There may be a need for a law on cybersecurity in Lesotho due to the increased usage of technology in the country and evidence of cybercrime to protect citizens. The drafting of the Bill and its objectives may indicate Lesotho's commitment to international agreements such as the African Union Convention on Cybersecurity and the SADC Model Law on Cybersecurity.

5.4.2 Cyber Offences in the Bill

The Computer Crime and Cybersecurity Bill stipulates 35 cybercrimes. The six prominent cybercrimes in the findings are described based on the participants' experiences, as per Table 5.8. The full list of Cybercrimes is attached in Appendix F.

Table 5.8: Cyber Crimes stipulated in the Computer Crime and Cybersecurity Bill

Name of Offence	**Description of the offence**	**Penalty**
Illegal remaining	*"A person who intentionally and without lawful excuse, by infringing security measures or with the intent of obtaining computer data or other dishonest intent, remains logged in a computer system or part of a computer system commits an offence*" (Lesotho Senate, 2022).	*"A fine not exceeding M5,000,000 or imprisonment for a term not exceeding ten years or both"* (Lesotho Senate, 2022).
Illegal interception	*"Any person who dishonestly and without lawful authority, by use of technical means, intercepts a private transmission of computer data from or within a computer system commits an offence"* (Lesotho Senate, 2022).	*"A fine not exceeding M 10,000,000 or imprisonment for a term not exceeding fifteen years or both" (*Lesotho Senate, 2022).

Cyber terrorism	*"Any person who wilfully and without lawful excuse uses a computer and information system to communicate information intended to seriously intimidate a population, destabilise, or destroy the fundamental political, constitutional, economic or social structures of a country commits an offence"* (Lesotho Senate, 2022).	*"Imprisonment for a term not exceeding twenty years"* (Lesotho Senate, 2022).
Computer-related forgery	*"A person who alters authentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless of whether or not the data is directly readable or intelligible, commits an offence"* (Lesotho Senate, 2022).	*"Imprisonment for a term not exceeding seven years, or a fine not exceeding M2,000,000.00"* (Lesotho Senate, 2022).
Computer-related fraud	*"A person causes a loss of property to another person by any input, alteration, deletion or suppression of computer data; with the fraudulent or dishonest intent of procuring an economic benefit for oneself or for another person, commits an offence" (Lesotho* Senate, 2022).	*"Imprisonment for a term not exceeding ten years or a fine not exceeding M5,000,000 or both"* (Lesotho Senate, 2022).
Child pornography	*"A person who knowingly makes pornography available to one or more children through a computer system or facilitates the access by children to pornography through a computer system commits an offence"* (Lesotho Senate, 2022).	*"Imprisonment for a term not exceeding twenty years"* (Lesotho Senate, 2022).

Cybercrimes in the Bill were defined, and the appropriate maximum penalties were also set out in the Bill. Some of the crimes include Cyber fraught, Unauthorised System access, and Cyberbullying, to name a few (Lesotho Senate, 2022). The offences and corresponding fines defined in the Computer Crime and Cybersecurity Bill seem to be similar to those defined in the SADC Model Law. This similarity may be because the Bill was transposed from the SADC Model Law. However, this similarity may also indicate that there was minimal customisation and domestication of the Bill to fit Lesotho's context.

The Findings indicated that the penalties defined in the Bill were too high and did not align with the country's economic status (Respondent 6). One of the participants also noted that some of the fines were higher than what they expected; "*I remember we agreed on the fines of about M50,0000, but I'm surprised that we have the fines of about M500, 0000.00"* (Respondent 15). The penalties are the maximum that can be charged for cybercrime; the courts of law may set lower judgments given the merits of each case. However, this misalignment between the fines and the participants' expectations may imply that the fines were not entirely set by the participants. The fines may have been set by the consultant leading the process of developing the Bill.

5.4.3 Cybersecurity Management Structures

The Bill established three entities designed to assist in administering and implementing cybersecurity in the country: the Cybersecurity Advisory Council, the CSIRT, and Critical Infrastructure Protection, as shown in Table 5.9.

Table 5.9: Cybersecurity Management Structures

Themes	Quotes
Cybersecurity Advisory Council	*"There is established the National Cyber Security Advisory Council, which shall be responsible for coordinating cyber security matters among relevant parties and to advise the Government on matters regarding cyber security" (* Lesotho Senate, 2022).

	"*The team shall provide Lesotho with cyber security intelligence, alerts, warnings, technical assistance, eradication of threats and recovery from cyberattacks*" (Lesotho Senate, 2022).
Cybersecurity Incident Response Team	*"Team shall be the main focal point for various national entities and shall provide administrative oversight for sectoral cyber security incident response team structures (hereinafter referred to as "sectoral CSIRTs") as the Minister may prescribe"* (Lesotho Senate, 2022).
Critical Infrastructure protection	*"The interruption of a life-sustaining or essential service, including the supply of water, health services, energy, and transport"* (Lesotho Senate, 2022).

The Cybersecurity Advisory Council reports to the government through the Minister of Communications, Science, Technology, and Innovation and is responsible for advising the government on policy and strategic issues related to cybersecurity (Lesotho Senate, 2022). The Bill provides for the establishment of a Cybersecurity Advisory Council, which coordinates all cybersecurity activities on behalf of the government with stakeholders.

A Cybersecurity Incident Response Team (CSIRT) has also been established in the Bill, which is a body responsible for reporting and disseminating cybersecurity information (Lesotho Senate, 2022). The CSIRT is tasked with providing intelligence and technical assistance to combat cybersecurity threats (Lesotho Senate, 2022) proactively and reactively. In Africa, only 40% of the countries have incident response teams set up (Cheimbi, 2023). This suggests that even though CSIRT is an important structure for establishing a secure cyber environment, its importance may be overlooked in many African countries.

Critical Infrastructure protection has also been identified in the Bill as a function required to implement and manage cybersecurity. Protecting critical infrastructure is also a crucial function of the Bill, ensuring that essential services are protected. The country's critical Infrastructure is identified and designated by the Minister of Communications, Science, Technology and Innovation and published in a government Gazette. A country's critical infrastructure may support essential services such as water, health, telecommunication, and other services (Lesotho Senate, 2022). The criteria for selecting a critical service is based on

the impact of the service on the economy, national security of the country, and health and safety of citizens (Lesotho Senate, 2022). Those who own or manage the critical infrastructure are mandated to control access to the service and the electronic data generated by the service.

5.4.4 Implications of Outcomes of the Bill

One of the outcomes of the Bill is the cybercrime offences indicated in the Computer Crime and Cybersecurity Bill. The list of offences in the Computer Crime and Cybersecurity Bill seems to resemble the offences in the SADC Model Law. This similarity may be because the Bill was transposed from the SADC Model Law (Media Institute of Southern Africa, 2021). However, it may also indicate that the Computer Crime and Cybersecurity Bill is generic and was not contextualised to meet the country's specific cybersecurity challenges. This may also be a result of inadequate stakeholder consultations, the penalties which do not match the stakeholders' expectations, and the similarity of the Bill and the SADC Model Law.

The study's findings show that the penalties set in the Bill do not match the participants' expectations. The penalties seem to be much higher than what participants expected, to the extent that some feel that they were not set because of the consultation process. "*I remember we agreed on the fines of about M50,0000, but I'm surprised that we have the fines of about M500, 0000.00"* (Respondent 15). This may indicate that the engagement process was not effective. Some of the crucial stakeholders were not engaged in the entire process; this led to the Parliament's rejection of the Bill (National Assembly, 2021). Studies show that if stakeholder engagements are not balanced, they may create bias in the outcomes and highlight only the view of the minority and underrepresented portion of the stakeholders (C. Braun & Busuioc, 2020).

It may also be possible that the fines represent the views of the consultants, who may not have a full grasp of the context of the country in which the fines would be applied. The heavy fines may also indicate that the country's economic and social context was not considered while developing the Bill. Some media groups also suggested that the Bill did not undergo deep, inclusive, and unbiased consultation in its development, and hence it may also violate some of the constitutional rights of the citizens, such as freedom of speech (MISA, 2021).

5.5 Influence of Perception on the Computer Crime and Cybersecurity Bill

This section highlights the effects of stakeholders' perceptions on the outcomes of the Computer Crime and Cybersecurity Bill. It provides details on the development process and the perceptions that may have affected the outcomes of the Bill.

5.5.1 Comparison of Cybersecurity Bill and the Stakeholders' Perception

SADC created a model law on cybersecurity, which formed the basis for the Bill. This section compares the Bill to the SADC Model Law and the stakeholders' perceptions about cybersecurity, as shown in Table 5.10. The objective is to determine the extent to which the stakeholders' perceptions have been incorporated into the Bill.

Table 5.10: Comparison of Cybersecurity Bill and the Stakeholders' Perception

Components of cybersecurity	**Stakeholders Perceptions**	**Computer Crime and Cybersecurity Bill**	**SADC Model Law on Computer Crime and Cybercrime**
Cybersecurity Council The council has not been defined in the Model Law	*"The main objective is establishing cybersecurity management by establishing a cybersecurity advisory council and establishing CSIRT" (Respondent 7).*	*"Responsible for coordinating cyber security matters among relevant parties and advising the Government on cyber security matters"* (Lesotho Senate, 2022).	This structure is not indicated in the Model Law
Incident Response Team(CSIRT) The cybersecurity Incident Response team has not been referenced in the SADC Model Law.	*"It would be good to have such a response team also for information sharing of incidents" (Respondent 16).*	*"CSIRT provides Lesotho with cyber security intelligence, alerts, warnings, technical assistance, eradication of threats and recovery from cyberattacks"* (Lesotho Senate, 2022)	This structure is not indicated in the Model Law
Critical Infrastructure Protection	*"That's why we are talking about critical*	*" Any person who wilfully hinders or interferes with a*	*"A person who intentionally,*

The Model law, however, does not only provide a definition without any details of the roles and functions and roles.	*infrastructure to be protected; if it affected, it would affect national security" (Respondent 6).*	*computer system used in critical infrastructure operations, whether exclusively or generally, with the intention of affecting or impacting its lawful use commits an offence*" (Lesotho Senate, 2022).	*without lawful excuse or justification or in excess of a lawful excuse or justification hinders or interferes with a computer system that is exclusively for the use of critical infrastructure operations, the punishment shall be imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both"* (ITU, 2013b).
Cyber Offenses Only 13 out of 35 cybercrimes that are in the Bill and Model Law are listed by participants.	*"The other issues have to do with bad mouthing on social media, because this conflicts with human rights, so there is a lot of cyberbullying" (Respondent 10).*	*"A person who intentionally, without lawful excuse, initiates any electronic communication with the intent to coerce, intimidate, harass, abuse, or cause emotional distress to a person"*(Lesotho Senate, 2022).	*"A person who initiates any electronic communication with the intent to coerce, intimidate, harass, or cause substantial emotional distress to a person"* (ITU, 2013b).

Some aspects of the Bill seem to have been derived from the stakeholders' perceptions, such as CSIRT, Cybersecurity Advisory Council, and Critical Infrastructure Protection. However, the descriptions of the cybercrimes and the related penalties in the Bill seem to have been influenced by other factors.

a) Cybersecurity Advisory Council

Participants believed the country requires a Cybersecurity Advisory Council. The participants have also defined the Council as a team that would be responsible for the coordination of cybersecurity in the country. This function has been established in the Bill to provide advice to the government on cybersecurity issues and coordinate national cybersecurity stakeholders *(*Lesotho Senate, 2022). Some respondents suggested that this team would be critical in implementing national cybersecurity (Respondent 16).

The Computer Crime and Cybersecurity Bill clearly defines the advisory council structure, as shown in Table 5.10. Since this structure is defined in the Bill and not specified in the SADC Model Law, participants are likely to have introduced it in the Bill due to their perception of its role in national Cybersecurity.

b) Cybersecurity Incident Response Team

The CSIRT is essential for the country in providing intelligence and disseminating cybersecurity information and awareness to all stakeholders (Lesotho Senate, 2022). The team would also protect the country proactively and reactively against cybercrimes by providing threat intelligence (Respondent 3, Respondent 7, and Respondent 8). The Computer Crime and Cybersecurity Bill defines the functions of this structure and its composition (Lesotho Senate, 2022). The SADC Model Law has not provided any guidance on the formation and functions of such a structure. The presence of this structure in the Bill could have been introduced by stakeholders due to their perception of CSIRT during the Bill's formulation.

c) Critical Infrastructure Protection

As perceived by the participants, Lesotho must have the capability to protect the infrastructure that sustains essential services (Respondent 2, Respondent 17, and Respondent 4). This infrastructure includes water systems, electricity, health facilities, and communications infrastructure. The Bill defined this capability and provided details on the approach to

identifying and protecting these essential national assets from cybercrimes. Any destruction or harm to this infrastructure has also been said to be a punishable offence (Lesotho Senate, 2022).

The SADC Model Law has defined Critical Infrastructure Protection and criminalised the destruction and illegal interference of its operations. This function has also been defined in the Bill. It enables the identification, protection, and recovery of critical assets from cyber threats *(*Lesotho Senate, 2022). From the findings, critical infrastructure protection seems to have been influenced by stakeholder's perceptions. Even though this structure is described in the SADC Model Law, the description in the Model Law is limited since it does not include details of the function of critical infrastructure protection or guidance on its formation.

d) Cyber Offences in the Bill

Many cybercrimes have occurred in Lesotho, as described by participants; some of these are shown in Table 5.8. The crimes range from illegal access to information, phishing, cyberbullying, Cyber Fraud, and many others. *"Issues of phishing, a lot of phishing happens on social media, and people are not even aware of it*" (Respondent 15).

The participants indicated that these crimes needed to be identified by the law and criminalised. The Computer Crime Cybersecurity Bill has identified at least 35 cyber offences and corresponding penalties (Lesotho Senate, 2022). Similarly, the SADC Model Law also identifies all these crimes in the same fashion; the model law also states that these crimes are punishable (ITU, 2013b). The corresponding penalties are not defined in the model law; they are left for the SADC member countries to domesticate.

The crimes and penalties set in the Bill seem not to have been influenced by participants' perceptions about cybersecurity. Even though the participants defined some of these crimes, only thirteen crimes have been identified by participants. It may be assumed that the lack of cybersecurity reporting mechanisms, such as CSIRT, could have caused a lack of knowledge of cybercrime in the country. The cybercrimes defined in the Bill have likely been derived from the Model Law due to the identical nature of the two documents as far as the cybercrime definitions are concerned.

The fines were also said to be draconian, too high, and not in alignment with the local economic context (Responded 3). The misalignment of the fines in the Bill and the stakeholders'

perception of the fines may indicate that the fines were also not influenced by participants' perceptions of cybersecurity.

5.5.2 Participation in the formulation of the Bill

The study shows that the participation of stakeholders in the formulation of the Bill was inadequate; some participants noted that their views were not incorporated into the Bill (Respondent 12). This may be a cause for concern because some of the inputs of some stakeholders may have been left out. Cybersecurity controls are a way for governments to manage cyber risks, and this is achieved through collaboration with stakeholders (Lebogang et al., 2022). Inadequate participation and engagement of stakeholders may bias the Bill's outcomes and reduce its alignment with the cybersecurity challenges as viewed by participants.

Some of the crucial stakeholders were not engaged in the entire process; this led to the rejection of the Bill by the Parliament (National Assembly, 2021). This may have led to the Bill not being passed into law by the government. Some of the stakeholders who were left out of the consultations include media houses, telecommunications agencies, and security agencies (National Assembly, 2021). Research shows that collaboration between government, academia, research, and innovation facilities is also lacking in many African countries; this collaboration is critical to building informed cybersecurity initiatives (Ikuero, 2022; Malatji et al., 2021).

The ability to ensure that various interests of society are represented in the development of a Bill may most likely ensure buy-in and ownership. Some Civil organisations have also claimed that the Bill lacks human rights and privacy protection. They also stated that the Bill violates some basic human rights, such as the right to privacy ("Media Statement on Computer Crime and Cyber Security Bill," 2021). This deficiency could have also led to the Bill being regarded by some participants as undemocratic in nature**.**

5.5.3 Contextualisation

There is evidence from the study that indicates that the Bill was not customised to fit Lesotho's context. Participants stated that the Bill was derived from the SADC Model Law, and it was developed without adequate contextualisation (Respondent 11). Some stakeholders believed that there was no need to customise the Bill to fit Lesotho's context because cybersecurity is not country-specific. However, research shows that without a deliberate effort to customise

the Bill to fit the local context, the resulting document may become narrow in scope and may lack the ability to address challenges faced by local stakeholders (Orji, 2018; Kunyenje & Chigona, n.d.).

5.5.4 Consultants Involvement

The development of the Bill was externally led; the consultant who led the formulation process was engaged by the International Telecommunication Union (ITU). Some of the participants claimed that the consultant assisted with expertise in drafting the Bill (Participant 6).

When consultants and international organisations take the lead on developing a policy or law instead of local experts, the resulting instruments may not cover all the necessary aspects. The result may also be that some local stakeholders may withdraw from the development process due to a lack of ownership (Kunyenje & Chigona, n.d.). The leadership of the external consultants might have had a detrimental effect on the local participants' sense of ownership of the Bill. The consultant may also not have been familiar with the local context where the proposed law was intended to operate.

5.6 Summary

The objective of the study was to determine the effects of stakeholders' perceptions on the outcomes of the Computer Crime and the Cybersecurity Bill. The study determined stakeholders' perceptions of cybersecurity. The study has found that it is essential to assess stakeholders' comprehension of cybersecurity, as well as their attitudes and beliefs about cybersecurity, before implementing any cybersecurity measures (Haney & Lutters, 2018).

The perceptions that participants have about cybersecurity seem to have had a partial effect on the outcomes of the Bill. The Bill is identical to the SADC Model Law on cybersecurity. The majority of the Bill's content was not contextualised to Lesotho's environment, which could be because the development process was also externally led by consultants. The consultant may not have been fully aware of the context of the country. There was also limited participation and engagement on the part of some of the stakeholders. Some of the stakeholders who were engaged did not sufficiently participate because of their limited understanding of cybersecurity. Some of the challenges that were identified in the process included limited political will, inadequate skills and expertise in cybersecurity, and a lack of financial resources for cybersecurity issues.

Chapter 6: Conclusion

This chapter summarises key findings related to the research objectives. It also describes the study's potential contribution and implications from a practical and theoretical standpoint. This section also presents the study's limitations and suggestions for future research.

6.1 Summary of Findings

The study's objective was to determine the effects of stakeholders' perceptions on the outcomes of the Computer Crime and Cybersecurity Bill. To achieve this objective, stakeholders' perceptions about Cybersecurity were investigated, and the sources of these perceptions were determined. The outcomes contained in the Computer Crime and Cybersecurity Bill were investigated.

6.1.1 Stakeholders' perceptions about cybersecurity

The study determined the stakeholders' perceptions about cybersecurity from the participants in the formulation of the Computer Crime and Cybersecurity Bill. Some of these perceptions were that cybersecurity is borderless and that it is about the protection of information and citizens in cyberspace. The participants perceived cybersecurity as a component of national security since cyberspace is a new battleground for warfare in the 21st century. Participants also perceived that cybersecurity is about Critical Infrastructure protection, the establishment of CSIRT, and the Cybersecurity Advisory Council. It has also been perceived that there are cybercrimes in Lesotho; however, some participants perceived that Lesotho may not be attractive for cybercriminals due to its limited economic activity compared to other nations.

6.1.2 Sources of Perceptions

The sources of stakeholders' perceptions about cybersecurity were determined from the study. Some participants believed that cybersecurity capacity building in the form of education and training has assisted them in understanding cybersecurity. Perceptions also seem to have originated from exposure to cybersecurity, such as news, social media, and technology usage. Basotho culture has also been found to contribute to how stakeholders perceived cybersecurity, while some of the perceptions seem to have originated from political influences. Awareness and skills of cybersecurity has also been found to be very low in the country. Implementing

awareness campaigns has been said to have the potential to improve the understanding of cybersecurity.

6.1.3 Outcomes of the Computer Crime and Cybersecurity Bill

The outcomes of the Computer Crime and Cybersecurity Bill, as found in the Bill, are described in this section; they are grouped into three major components. The first deals with cybersecurity management, which includes setting up structures to manage cybersecurity. These structures include the Cybersecurity Advisory Council, the Cybersecurity Incident Response Team, and Critical Infrastructure Protection. The Bill also described cybersecurity functions within the country's context, including assisting in investigating and protecting citizens. Lastly, the Bill identifies the various cybercrimes and their corresponding penalties. The respondents also described challenges in the formulation of the Bill. They include limited participation and consultation of various stakeholders and a lack of contextualisation of the Bill.

6.1.4 Effects of stakeholders' perceptions on the outcomes of the Bill

Stakeholders' perceptions about cybersecurity seem to have influenced the outcomes of the Bill to a limited extent. Management structures such as CSIRT, Advisory Council, and Critical Infrastructure Protection seem to have been considered necessary by the participants to implement cybersecurity. These components are also not provided for in the SADC Model Law on Cybersecurity, which is the source document for the Bill. Critical Infrastructure Protection is mentioned in the SADC Model Law. However, it has only been described without details of its operation and functions. It may be assumed that this structure has been included in the Bill as an outcome of the stakeholders' interaction in its formulation. Cybercrimes defined in the Bill are identical in their descriptions and definitions to those in the SADC Model Law; this may suggest that they were not influenced by stakeholders' perceptions but by the SADC Model Law. The participants also criticised the penalties set in the Bill as being too heavy for the context of Lesotho; this may also imply that they have not been directly influenced by the stakeholders' perceptions. The perceptions of the stakeholders influenced some of the outcomes of the Bill. other outcomes seem to have been influenced by other factors such as external consultants assisting in the formulation of the Bill and the SADC Model Law on Computer Crime and Cybersecurity, among others.

6.2 Limitations of the Study

The study was limited by the time participants had available to contribute to the study; thus, getting time to conduct the interviews was a challenge. Some of the potential respondents declined to participate, while other interviews were cancelled. The interviews were organised at a convenient time for participants, including outside of regular business hours and on weekends. Some meetings were conducted virtually using Microsoft Teams. There was limited documentation and published information on the formulation process of the Computer Crime and Cybersecurity Bill. Only two documents were used in the data gathering process: the Computer Crime and Cybersecurity Bill document and the SADC Model Law on Cybersecurity document.

Some participants were hesitant to provide information regarding their involvement in the formulation of the Bill. The challenge was addressed by assuring participants that their anonymity would be maintained throughout the study. The data obtained from interviews was supplemented with document analysis data to address the limitation of information. Generalisability of the study's findings was difficult since the research was a case study; the results may only be inferred by countries with similar contexts. The researcher also acknowledges that this qualitative study is prone to data collection and interpretation bias.

6.3 Contribution of the Study

The study makes both theoretical and practical contributions to the field of cybersecurity legislation formulation.

6.3.1 Practical contributions

The study may add to the understanding of the implementation of cybersecurity legislation in the African context. Even though the study was conducted in Lesotho, its results may be inferred by other countries with similar contexts. The challenges that some of the countries face, which may have been outlined in the study, may act as lessons learned. These details may also be helpful as a guide for any country embarking on the process of transposing and domesticating the SADC Model Law into cybersecurity legislation.

Understanding stakeholders' perceptions of cybersecurity may lead to proactive and informed engagements during the formulation and agenda-setting of cybersecurity legislation. If stakeholders' perceptions of cybersecurity are not aligned with the government agenda, the

expected legislation outcomes may not be consistent with the expected objectives. International organisations such as SADC, Commonwealth, ITU, and African Union that have agreements on cybersecurity may learn to effectively engage stakeholders in consideration of their perceptions to create more informed and context-driven legislation.

6.3.2 Theoretical contributions

Human aspects such as beliefs, experience, and expectations are important in understanding cybersecurity, especially when developing controls to mitigate cybercrime. This area of cybersecurity has received minimal attention from researchers. This study has described the understanding of stakeholder perceptions and the process of their formulation. It has defined sources of cybersecurity perceptions. Various perceptions about cybersecurity have also been outlined, which may have contributed to the overall understanding of cybersecurity.

While many studies in the field of cybersecurity legislation focus on technical aspects of cybersecurity controls, this study's focal point is on the humanistic aspects of cybersecurity. Most studies conducted on cybersecurity perceptions were based on the context of developed nations; this study is based on the context of a least developed country in the African continent. The study also utilises interviews as primary data-gathering techniques; this is also unique because most studies in the context of cybersecurity legislation utilise document review as the primary source of data.

6.3.3 Recommendations for Practice

It was the perception of the stakeholders that the engagement process in the formulation of the Bill was not inclusive enough and did not incorporate some of the participants' views. This view pertains to the heavy penalties in the Bill and the perception that the Bill violates some basic constitutional rights of the citizens, such as the right to privacy. There is a need to engage further on the penalties set in the Bill to align them with the expectations and the context of the country. These issues require further consultations with stakeholders to improve ownership of the bill and its alignment with the country's local context.

It has also been noted that the country's education curricula on cybersecurity does not address the needs of the community and the industry. Therefore, there is a need to review this curriculum in consultation with organisations and companies to create an alignment of requirements. Cybersecurity education should also reach a broader range of technology users,

such as the elderly, primary school pupils, and high school students. This proposed broader scope of coverage may promote cybersecurity and contribute to the government's efforts to mitigate cyber risk. This change in the education and training approach could also address the skill shortage prevalent in the country in terms of cybersecurity.

There is also a need for the government and other entities, such as educational institutions and non-governmental organisations, to create awareness of cybersecurity. This should be led by credible experts in the field of cybersecurity using all forms of media, such as news, social media, and radio, to distribute the information. The approach will ensure that all parts of society have access to verified cybersecurity awareness content. The language used in this awareness initiative should also be understandable to the broader Basotho population; the recommendation is that the two official languages used in the country, namely Sesotho and English, should be used to publish this content.

There is also a need for the government to become more involved and interested in cybersecurity mitigation initiatives in the country. The study revealed a lack of political will on the part of the government to implement cybersecurity. The recommendation is that the Computer Crime and Cybersecurity Bill should be finalised and implemented as the main tool for combating cybercrime at a national level. Cybersecurity management structures such as CSIRT, Cybersecurity Advisory Council, and Critical Infrastructure Protection should be established. These structures will enable the government to achieve its goals of implementing cybersecurity. The necessary budget should also be provided to enable the implementation of the government's cybersecurity objectives.

There is also a need for the county to demonstrate compliance with international agreements on cybersecurity. This compliance includes the implementation of the SADC Model Law on Cybersecurity. The country should also comply with other agreements, such as the African Union Convention on Cybersecurity, the ITU Global Cybersecurity Agenda (GCA) of 2007, and the Commonwealth Cyber Declaration 91 of 2018. On the one hand, failure to comply could result in sanctions being imposed on Lesotho and reputational loss. On the other hand, if the country were to comply, there could be an increase in foreign direct investment in Lesotho because compliance has been shown to boost investor confidence.

6.4 Suggestion for future research

It was determined from the study that the impact of culture on cybersecurity is one of the least researched areas of cybersecurity. It is worth noting that culture is at the core of human-centric cybersecurity (Rahman, Rohan, Pal, & Kanthamanon, 2021). This is one of the areas that may require more research focus. The findings also indicated that there was inadequate stakeholder engagement in the formulation of the Bill. This was one of the reasons that led to the parliament's repudiation of the Computer Crime and Cybersecurity Bill in 2021. The significance and impact of stakeholder engagement on cybersecurity initiatives and controls may require more research to gain further insight.

6.5 Summary

The study determined the perception of cybersecurity amongst stakeholders. Some of these perceptions were that cybersecurity is borderless and about protecting information and citizens while using technology. Participants defined cybersecurity as a component of national security since cyberspace is a new platform for war in the 21st century. The study determined that stakeholders' perceptions about cybersecurity originated from training and education activities. They also originated from exposure to cybersecurity, from news and media, and from technology usage. Basotho culture has also been found to contribute to how stakeholders perceive cybersecurity. Awareness of cybersecurity has also been found to be very low. This could be because Lesotho has been described as being at a startup status of cybersecurity capacity in a study by C3SA (C3SA, 2023).

It has been determined that the Computer Crime and Cybersecurity Bill has three major components. The first deals with the management of Cybersecurity, which includes setting clear structures to manage cybersecurity. This includes establishing the Cybersecurity Advisory Council and the Cybersecurity Incident Response Team. The Bill also describes cybersecurity functions within the country's context, including assisting in the investigation and protection of citizens. Lastly, the Bill describes various cybercrimes and their corresponding penalties.

The findings from the study are that the perceptions of stakeholders influenced some of the outcomes of the Bill. These outcomes are the formation of a CSIRT, Cybersecurity Advisory Council, and Critical Infrastructure Protection in the Bill. Other outcomes were influenced by other factors, such as the SADC Model Law of Cybersecurity and external consultants'

involvement in the formulation of the Bill. These outcomes include the description of cybercrimes in the Bill and the penalties set for each crime. The Bill was drafted from the SADC model law on cybersecurity; as a result, some of the outcomes of the Bill seem to have been primarily shaped by the model law.

References

Adomako, K., Mohamed, N., Garba, A., & Saint, M. (2018). *Assessing Cybersecurity Policy Effectiveness in Africa via a Cybersecurity Liability Index* (SSRN Scholarly Paper No. ID 3142296). Rochester, NY: Social Science Research Network. https://doi.org/10.2139/ssrn.3142296

African Union. (2015). African Union Convention on Cyber Security and Personal Data Protection | African Union. Retrieved December 9, 2023, from https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection

Alshaikh, M., & Adamson, B. (2021). From awareness to influence: Toward a model for improving employees' security behaviour. *Personal and Ubiquitous Computing*, *25*(5), 829–841. https://doi.org/10.1007/s00779-021-01551-2

Altuna, J., & Lareki, A. (2015). Analysis of the Use of Digital Technologies in Schools That Implement Different Learning Theories. *Journal of Educational Computing Research*, *53*(2), 205–227. https://doi.org/10.1177/0735633115597869

Ani, U. D., He, H., & Tiwari, A. (2019). Human factor security: Evaluating the cybersecurity capacity of the industrial workforce. *Journal of Systems and Information Technology*, *21*(1), 2–35. http://dx.doi.org/10.1108/JSIT-02-2018-0028

Bada, M., Von Solms, B., & Agrafiotis, I. (2019). *Reviewing National Cybersecurity Awareness in Africa: An Empirical Study*. Apollo - University of Cambridge Repository. https://doi.org/10.17863/CAM.40856

Baumann, I. (2016). *The Plight of Older Workers: Labor Market Experience after Plant Closure in the Swiss Manufacturing Sector*. Cham: Springer International Publishing. https://doi.org/10.1007/978-3-319-39754-2

Bernard, H. R. (2011). *Research methods in anthropology: Qualitative and quantitative approaches* (5th ed). Lanham, Md: AltaMira Press.

Bhattacherjee, A. (2012). *Social Science Research: Principles, Methods, and Practices* (2nd ed.). Florida, USA: Global Text Project.

Biernacki, P., & Waldorf, D. (1981). Snowball Sampling: Problems and Techniques of Chain Referral Sampling. *Sociological Methods & Research*, *10*(2), 141–163. https://doi.org/10.1177/004912418101000205

Bowen, G. (2009). Document Analysis as a Qualitative Research Method. *Qualitative Research Journal*, *9*, 27–40. https://doi.org/10.3316/QRJ0902027

BrainGymmer. (2020). How perception works. Retrieved December 28, 2023, from BrainGymmer website: https://www.braingymmer.com/en/blog/perception/

Braun, C., & Busuioc, M. (2020). Stakeholder engagement as a conduit for regulatory legitimacy? *Journal of European Public Policy*, *27*(11), 1599–1611. https://doi.org/10.1080/13501763.2020.1817133

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, *3*(2), 77–101. https://doi.org/10.1191/1478088706qp063oa

Brewer, R., de Vel-Palumbo, M., Hutchings, A., Holt, T., Goldsmith, A., & Maimon, D. (2019). *Cybercrime Prevention: Theory and Applications*. Cham: Springer International Publishing. https://doi.org/10.1007/978-3-030-31069-1

Bryant, L. C., Vincent, R., Shaqlaih, A., & Moss, G. (2013). Behaviorism and behavioral learning theory. In *The handbook of educational theories.* (pp. 91–103). Charlotte, NC, US: IAP Information Age Publishing.

C3SA. (2022). *Southern African Development Community Cybersecurity Maturity Report 2021*. Cybersecurity Capacity Centre for Southern Africa (C3SA). Retrieved from https://open.uct.ac.za/items/593e24ab-251c-451e-b7be-187345d8abb7

C3SA. (2023). Lesotho-CMM-Report-2022-vFinal_31032023.pdf. Retrieved August 10, 2024, from https://cybilportal.org/wp-content/uploads/2023/05/Lesotho-CMM-Report-2022-vFinal_31032023.pdf

Chang, L. Y. C., & Coppel, N. (2020). Building cyber security awareness in a developing country: Lessons from Myanmar. *Computers & Security*, *97*, 101959. https://doi.org/10.1016/j.cose.2020.101959

Cheimbi, S. (2023, September 18). The Cybersecurity Talent Gap in Africa. Retrieved January 14, 2024, from GOMYCODE: Learn digital skills! website: https://gomycode.com/the-cybersecurity-talent-gap-in-africa/

Chib, A., May, J., & Barrantes, R. (Eds.). (2015). *Impact of Information Society Research in the Global South*. Singapore: Springer Singapore. https://doi.org/10.1007/978-981-287-381-1

Commonwealth, C. (2018). Commonwealth Cyber Declaration, 2018. Retrieved December 9, 2023, from Commonwealth website: https://thecommonwealth.org/commonwealth-cyber-declaration-2018

Corallo, A., Lazoi, M., Lezzi, M., & Luperto, A. (2022). Cybersecurity awareness in the context of the Industrial Internet of Things: A systematic literature review. *Computers in Industry*, *137*, 103614. https://doi.org/10.1016/j.compind.2022.103614

Creese, S., Dutton, W. H., & Esteve-González, P. (2021). The social and cultural shaping of cybersecurity capacity building: A comparative study of nations and regions. *Personal and Ubiquitous Computing*, *25*(5), 941–955. https://doi.org/10.1007/s00779-021-01569-6

Creswell, J. W., & Clark, V. L. P. (2007). Designing and Conducting Mixed Methods Research. *Library & Information Science Research*, *29*(3). https://doi.org/10.1016/j.lisr.2007.02.003

Crouch, M., & McKenzie, H. (2006). The logic of small samples in interview-based qualitative research. *Social Science Information*, *45*(4), 483–499. https://doi.org/10.1177/0539018406069584

de Barros, M. J. Z., & Lazarek, H. (2018). Comparative Study of Cybersecurity Policy Among South Africa and Mozambique. *International Conference on Cyber Warfare and Security*, 521-529,XI. Reading, United Kingdom: Academic Conferences International Limited. Retrieved from http://www.proquest.com/advancedtechaerospace/docview/2018926085/abstract/1583A5FBE8F0436DPQ/22

DeCarlo, M. (2018). *7.3 Unit of analysis and unit of observation*. Retrieved from https://pressbooks.pub/scientificinquiryinsocialwork/chapter/7-3-unit-of-analysis-and-unit-of-observation/

Denzin, N. k., & Lincon, Y. S. (2011). Discipline and Practice C.R Qualitative Research | Positivism. Retrieved August 11, 2024, from Scribd website: https://www.scribd.com/document/369907335/1-Denzin-Lincoln-2011-Discipline-and-Practice-C-R-1

Du Toit, R., Hadebe, P. N., & Mphatheni, M. (2018). Public perceptions of cybersecurity: A South African context. *Acta Criminologica: African Journal of Criminology & Victimology*, *31*(3), 111–131.

Dubé & Paré. (2003). Rigor in Information Systems Positivist Case Research: Current Practices, Trends, and Recommendations. *MIS Quarterly*, *27*(4), 597. https://doi.org/10.2307/30036550

Dutton, W. H., Creese, S., Shillair, R., & Bada, M. (2019). Cybersecurity Capacity: Does It Matter? *Journal of Information Policy*, *9*, 280–306. https://doi.org/10.5325/jinfopoli.9.2019.0280

Etikan, I. (2016). Comparison of Convenience Sampling and Purposive Sampling. *American Journal of Theoretical and Applied Statistics*, *5*(1), 1. https://doi.org/10.11648/j.ajtas.20160501.11

Ezumah, B., & Adekunle, S. O. (2012). A Review of Privacy, Internet Security Threat, and Legislation in Africa: A Case Study of Nigeria, South Africa, Egypt, and Kenya. *Internet and Distributed Computing Advancements: Theoretical Frameworks and Practical Applications*, 115–136.

Farquhar, J. (2012). *Case Study Research for Business*. 1 Oliver's Yard, 55 City Road, London EC1Y 1SP United Kingdom: SAGE Publications Ltd. https://doi.org/10.4135/9781446287910

Feroz, H. M. B., Zulfiqar, S., Noor, S., & Huo, C. (2022). Examining multiple engagements and their impact on students' knowledge acquisition: The moderating role of information overload. *Journal of Applied Research in Higher Education*, *14*(1), 366–393. Scopus. https://doi.org/10.1108/JARHE-11-2020-0422

Fonseca, R. S., & van Wyk, J.-A. (2021). Cybersecurity in South Africa: Status, governance, and prospects. In *Routledge Companion to Global Cyber-Security Strategy* (pp. 591–607). Routledge.

Freeman, R. E., Phillips, R., & Sisodia, R. (2020). Tensions in Stakeholder Theory. *Business & Society*, *59*(2), 213–231. https://doi.org/10.1177/0007650318773750

Gaillard, A. (2021). Cybersecurity Challenges and Governance Issues in the Cyberspace'When Stronger Passwords Are not Enough: Governing Cyberspace in Contemporary African Nations' Case Study: Can South Africa and Nigeria Secure Cyberspace without a Lock? *Available at SSRN 3877526*.

Gerring, J. (2017). Qualitative Methods. *Annual Review of Political Science*, *20*(1), 15–36. https://doi.org/10.1146/annurev-polisci-092415-024158

Gill, P., Stewart, K., Treasure, E., & Chadwick, B. (2008). Methods of data collection in qualitative research: Interviews and focus groups. *British Dental Journal*, *204*(6), 291–295. https://doi.org/10.1038/bdj.2008.192

global partners digital. (2020). Involving Stakeholders in National Cybersecurity Strategies: A Guide for Policymakers. Retrieved April 11, 2024, from https://www.gp-digital.org/wp-content/uploads/2020/08/NCSS-guidance-doc_gpd.pdf

Government of South Africa. (2013). Minister inaugurates National Cyber Security Advisory Council | South African Government. Retrieved February 4, 2024, from https://www.gov.za/news/media-statements/minister-inaugurates-national-cyber-security-advisory-council-15-oct-2013

Grünbaum, N. N. (2007). Identification of ambiguity in the case study research typology: What is a unit of analysis? *Qualitative Market Research: An International Journal*, *10*(1), 78–97. https://doi.org/10.1108/13522750710720413

Guzman, A. T. (2005). The Design of International Agreements. *European Journal of International Law*, *16*(4), 579–612. https://doi.org/10.1093/ejil/chi134

Haney, J. M., & Lutters, W. G. (2018). "It's scary...it's confusing...it's dull": How cybersecurity advocates overcome negative perceptions of security. *Proceedings of the Fourteenth USENIX Conference on Usable Privacy and Security*, 411–425.

Hennink, M. M., Kaiser, B. N., & Marconi, V. C. (2017). Code Saturation Versus Meaning Saturation: How Many Interviews Are Enough? *Qualitative Health Research*, *27*(4), 591–608. https://doi.org/10.1177/1049732316665344

Ikuero, F. E. (2022). Preliminary review of cybersecurity coordination in Nigeria. *Nigerian Journal of Technology*, *41*(3), 521–526. https://doi.org/10.4314/njt.v41i3.11

ITU. (2007). *ITU Global Cybersecurity Agenda (GCA): Framework for International Cooperation in Cybersecurity*. Retrieved from https://ifap.ru/library/book169.pdf

ITU. (2013a). Lesotho in-Country transposition of the SADC Cybersecurity Model laws. Retrieved December 9, 2023, from ITU website: https://www.itu.int:443/en/ITU-D/Projects/ITU-EC-ACP/HIPSSA/Pages/in-country-assistance/Lesotho.aspx

ITU. (2013b). SADC Model Law on Computer Crime and Cybercrime. Retrieved August 13, 2024, from https://www.itu.int/en/ITU-D/Cybersecurity/Documents/SADC%20Model%20Law%20Cybercrime.pdf

ITU. (2024). ITU Project 9MLW19002. Retrieved June 20, 2024, from https://www.itu.int/net4/ITU-D/CDS/projects/display.asp?ProjectNo=9MLW19002

ITU, I. (2021). Connectivity in the least developed countries: Status report 2021. Retrieved April 19, 2022, from ITU Hub website: https://www.itu.int/hub/publication/d-ldc-ictldc-2021-2021/

Jadhav, K., Haggag, S., & Haggag, H. (2022). *Diving deep into human centric issues within cyber security*. 60–68. Retrieved from https://urn.kb.se/resolve?urn=urn:nbn:se:umu:diva-206039

Jaquire, V., & Von Solms, B. (2015). A best practice strategy framework for developing countries to secure cyberspace. In Zaaiman J. & Leenen L. (Eds.), *Proc. Int. Conf. Cyber Warf. Secur., ICCWS* (pp. 472–480). Academic Conferences Limited. Scopus. Retrieved from https://www.scopus.com/inward/record.uri?eid=2-s2.0-84969134545&partnerID=40&md5=ec9aeaff8e70d24a67b7319247bf8675

Karim, R., Bonhi, T. C., & Afroze, R. (2019). Governance Of Cyberspace: Personal Liberty VS. National Security. *INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH VOLUME 8*, *8*(11). https://www.ijstr.org/final-print/nov2019/Governance-Of-Cyberspace-Personal-Liberty-Vs-National-Security.pdf

Kasper, A. (2020). *EU cybersecurity governance – stakeholders and normative intentions towards integration*. https://www.um.edu.mt/library/oar/bitstream/123456789/52308/1/EU_cybersecurity_governance%E2%80%93stakeholders_and_normative_intentions_towards_integration_2020.pdf

Klein, H. K., & Myers, M. D. (1999). A Set of Principles for Conducting and Evaluating Interpretive Field Studies in Information Systems. *MIS Quarterly*, *23*(1), 67. https://doi.org/10.2307/249410

Klimburg, A., & Almeida, V. A. F. (2019). Cyber Peace and Cyber Stability: Taking the Norm Road to Stability. *IEEE Internet Computing*, *23*(4), 61–66. https://doi.org/10.1109/MIC.2019.2926847

Kostyuk, N., & Wayne, C. (2021). The Microfoundations of State Cybersecurity: Cyber Risk Perceptions and the Mass Public. *Journal of Global Security Studies*, *6*(2), ogz077. https://doi.org/10.1093/jogss/ogz077

Kshetri, N. (2019). Cybercrime and Cybersecurity in Africa. *Journal of Global Information Technology Management*, *22*(2), 77–81. https://doi.org/10.1080/1097198X.2019.1603527

Chigona, W. (n.d.). External Actors in Forming National ICT Policy in Malawi: A Cause for Concern in Low-Income Countries?. *The African Journal of Information Systems*, *11*(1), 2..

Lebogang, V., Tabona, O., & Maupong, T. (2022). Evaluating Cybersecurity Strategies in Africa. In *Cybersecurity Capabilities in Developing Nations and Its Impact on Global Security* (pp. 1–19). IGI Global. Retrieved from https://www.igi-global.com/book/cybersecurity-capabilities-developing-nations-its/272594

Leech, N. L., & Onwuegbuzie, A. J. (2007). An array of qualitative data analysis tools: A call for data analysis triangulation. *School Psychology Quarterly*, *22*(4), 557–584. (2007-19518-005). https://doi.org/10.1037/1045-3830.22.4.557

Lesotho Senate, L. S. (2022). Computer Crime and Cyber Security Bill, 2022 – Lesotho Senate. Retrieved December 6, 2023, from https://senate.parliament.ls/2022/05/19/computer-crime-and-cyber-security-bill-2022/

Machepha, M. (2010). Parliamentary role and its relationship with its relevant institutions in effectively addressing climate change issues-Lesotho. Retrieved December 31, 2023, from https://www.iied.org/sites/default/files/pdfs/migrate/G03024.pdf

Maisikeli, S. (2020). UAE Cybersecurity Perception and Risk Assessments Compared to Other Developed Nations. *2020 3rd International Conference on Information and*

Computer Technologies (ICICT), 432–439. https://doi.org/10.1109/ICICT50521.2020.00075

Maksimov, V., Wang, S. L., & Luo, Y. (2017). Reducing poverty in the least developed countries: The role of small and medium enterprises. *Journal of World Business*, *52*(2), 244–257. https://doi.org/10.1016/j.jwb.2016.12.007

Makulilo, A. B., & Mophethe, K. (2016). Privacy and Data Protection in Lesotho. In A. B. Makulilo (Ed.), *African Data Privacy Laws* (pp. 337–347). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-319-47317-8_16

Malatji, M., Marnewick, A. L., & von Solms, S. (2021). Cybersecurity policy and the legislative context of the water and wastewater sector in South Africa. *Sustainability (Switzerland)*, *13*(1), 1–33. Scopus. https://doi.org/10.3390/su13010291

Marshall, M. N. (1996). Sampling for qualitative research. *Family Practice*, *13*(6), 522–526. https://doi.org/10.1093/fampra/13.6.522

Maxwell, J. A. (2018). Collecting Qualitative Data: A Realist Approach. In U. Flick, *The SAGE Handbook of Qualitative Data Collection* (pp. 19–31). 1 Oliver's Yard, 55 City Road, London EC1Y 1SP: SAGE Publications Ltd. https://doi.org/10.4135/9781526416070.n2

McNabb, D. E. (2002). *Research methods in public administration and nonprofit management: Quantitative and qualitative approaches*. Armonk, N.Y: M.E. Sharpe.

Media Institute of Southern Africa. (2021). Report on Cybersecurity in SADC and its implications on human rights now available! Retrieved December 9, 2023, from MISA Regional website: https://misa.org/blog/report-on-cybersecurity-in-sadc-and-its-implications-on-human-rights-now-available/

Media Statement on Computer Crime and Cyber Security Bill. (2021, July 8). Retrieved October 18, 2023, from MISA Lesotho website: https://lesotho.misa.org/2021/07/08/media-statement-on-computer-crime-and-cyber-security-bill/

Mitchell, A. (2018). A Review of Mixed Methods, Pragmatism and Abduction Techniques. *Electronic Journal of Business Research Methods*, *16*(3), pp103-116-pp103-116.

Mogoane, S. N., & Kabanda, S. (2019). Challenges in information and Cybersecurity program offering at higher education institutions. *Proceedings of 4th International Conference on The*, *12*, 202–212.

Mohammed, A. K. (2020). Does the policy cycle reflect the policymaking approach in Ghana? *Journal of Public Affairs*, *20*(3), e2078. https://doi.org/10.1002/pa.2078

Morse J., Barrett M., Mayan M., Olson K. & Spiers J. (2002). Verification strategies for establishing reliability and validity in qualitative research. *International Journal of Qualitative Methods*, 1(2), 1–19.

Mosola, N. N., Moeketsi, K. F., Sehobai, R., & Pule, N. (2019). Cybersecurity Protection Structures: The Case of Lesotho. *International Journal of Computer and Information Engineering*, *13*(3), 158–163.

Mpaki, B. (2022). Lesotho: National Assembly Approves Cyber-Crime Bill. *Lesotho Times*. Retrieved from https://allafrica.com/stories/202205170646.html

Mukherjee, J., Lindeborg, M. M., Wijayaratne, S., Mitnick, C., Farmer, P. E., & Satti, H. (2020). Global Cash Flows for Sustainable Development: A Case Study of Accountability and Health Systems Strengthening in Lesotho. *Journal of Health Care for the Poor and Underserved*, *31*(1), 56–74.

Myers, M. D. (2013). *Qualitative research in business & management* (2nd ed). London: SAGE.

National Assembly. (2021). Computer-crime-and-cybersecurity-Bill-2021-Report.pdf. Retrieved December 9, 2023, from Lesotho National Assembly website: https://nationalassembly.parliament.ls/wp-content/uploads/2021/09/Computer-crime-and-cybersecurity-Bill-2021-Report.pdf

Navajas-Adán, J., Badia-Gelabert, E., Jiménez-Saurina, L., Marijuán-Martín, M. J., & Mayo-García, R. (2024). Perceptions and dilemmas around cyber-security in a Spanish research center after a cyber-attack. *International Journal of Information Security*. https://doi.org/10.1007/s10207-024-00847-7

Ndebele, L. (2023). Lesotho government challenged to clear outstanding human rights cases from previous regime. Retrieved December 9, 2023, from News24 website: https://www.news24.com/news24/africa/news/lesotho-government-challenged-to-clear-outstanding-human-rights-cases-from-previous-regime-20230508

Ngo, F. T., Deryol, R., Turnbull, B., & Drobisz, J. (2024). The Need for a Cybersecurity Education Program for Internet Users with Limited English Proficiency: Results from a Pilot Study. *International Journal of Cybersecurity Intelligence & Cybercrime*, *7*(1). https://doi.org/10.52306/2578-3289.1160

Niosi, A. (2021). *The Perceptual Process*. Retrieved from https://opentextbc.ca/introconsumerbehaviour/chapter/the-perceptual-process/

Nwankwo, W., & Chiwuike Ukaoha, K. (2019). (PDF) Socio-Technical Perspectives On Cybersecurity: Nigeria's Cybercrime Legislation In Review. *International Journal of Scientific & Technology Research 8(10)*. https://www.researchgate.net/publication/337033615_Socio-

Technical_Perspectives_On_Cybersecurity_Nigeria's_Cybercrime_Legislation_In_Review

'Nyane, H. (2022). Lesotho elections: Newcomers score impressive win, but politics will still be unstable. Retrieved December 10, 2023, from The Conversation website: http://theconversation.com/lesotho-elections-newcomers-score-impressive-win-but-politics-will-still-be-unstable-192466

Oates, B. J., McLean, R., & Griffiths, M. (2022). Researching Information Systems and Computing. 1–100.

Onyango, G. (Ed.). (2021). *Routledge Handbook of Public Policy in Africa*. London: Routledge. https://doi.org/10.4324/9781003143840

Orji, U. (2018). The African Union Convention on Cybersecurity: A Regional Response Towards Cyber Stability? *Masaryk University Journal of Law and Technology*, *12*, 91. https://doi.org/10.5817/MUJLT2018-2-1

Osho, O., & Onoja, A. D. (2015). National Cyber Security Policy and Strategy of Nigeria: A Qualitative Analysis. *International Journal of Cyber Criminology*, *9*(1), 120–143. https://doi.org/10.5281/zenodo.22390

Patton, M.Q. (2002). Qualitative research and evaluation methods. Sage Publications: London.

Pedrini, M., & Ferri, L. M. (2018). Stakeholder management: A systematic literature review. *Corporate Governance: The International Journal of Business in Society*, *19*(1), 44–59. https://doi.org/10.1108/CG-08-2017-0172

Pickens, J. (2005). Attitudes and perceptions. *Organizational Behavior in Health Care*, *4*(7), 43–76.

Poshai, L., Chilunjika, A., & Intauno, K. (2023). Examining the institutional and legislative frameworks for enforcing cybersecurity in Zimbabwe. *International Cybersecurity Law Review*, *4*(4), 431–449. https://doi.org/10.1365/s43439-023-00093-y

PricewaterhouseCoopers. (n.d.). Investors put cybersecurity top of the business threat list. Retrieved June 20, 2024, from PwC website: https://www.pwc.com/kz/en/pwc-news/what-new/investors-put-cybersecurity.html

Rahman, T., Rohan, R., Pal, D., & Kanthamanon, P. (2021). Human Factors in Cybersecurity: A Scoping Review. *The 12th International Conference on Advances in Information Technology*, 1–11. Bangkok Thailand: ACM. https://doi.org/10.1145/3468784.3468789

Reegård, K., Blackett, C., & Katta, V. (2019). *The Concept of Cybersecurity Culture*. https://doi.org/10.3850/978-981-11-2724-3_0761-cd

Reveron, D. S., & Savage, J. E. (2020). Cybersecurity Convergence: Digital Human and National Security. *Orbis*, *64*(4), 555–570. https://doi.org/10.1016/j.orbis.2020.08.005

Rohan, R., Funilkul, S., Pal, D., & Chutimaskul, W. (2021). Understanding of Human Factors in Cybersecurity: A Systematic Literature Review. *2021 International Conference on Computational Performance Evaluation (ComPE)*, 133–140. https://doi.org/10.1109/ComPE53109.2021.9752358

Ron, M., Fuertes, W., Bonilla, M., Toulkeridis, T., & Díaz, J. (2018). Cybercrime in Ecuador, an Exploration, which allows to define National Cybersecurity Policies. *CISTI (Iberian Conference on Information Systems & Technologies / Conferência Ibérica de Sistemas e Tecnologias de Informação) Proceedings*, 1–7.

Rubin, E. L. (1989). Law and Legislation in the Administrative State. *Columbia Law Review*, *89*(3), 369–426.

Saunders, M., Lewis, P., Thornhill, A., & Bristow, A. (2019). *"Research Methods for Business Students" Chapter 4: Understanding research philosophy and approaches to theory development*.

Sekaran, U., & Bougie, R. (2013). *Research methods for business: A skill-building approach* (6. ed). Chichester: Wiley.

Sharma, G. (2017). *Pros and cons of different sampling techniques*. 1–5.

Sherif, M., & Cantril, H. (1945). The psychology of "attitudes": Part I. *Psychological Review*, *52*(6), 295–319. https://doi.org/10.1037/h0062252

Sheth, M., Bhosale, S., & Kurupkar, M. (2021). *Research Paper on Cyber Security*. 2021.

Snail Ka Mtuze, S., & Musoni, M. (2023). An overview of cybercrime law in South Africa. *International Cybersecurity Law Review*, *4*(3), 299–323. https://doi.org/10.1365/s43439-023-00089-8

Snider, K. L. G., Shandler, R., Zandani, S., & Canetti, D. (2021). Cyberattacks, cyber threats, and attitudes toward cybersecurity policies. *Journal of Cybersecurity*, *7*(1), tyab019. https://doi.org/10.1093/cybsec/tyab019

Sunkpho, J., Ramjan, S., & Ootthamakorn, C. (2018). *Cybersecurity Policy in ASEAN Countries*.

Tanner, M., & Du Toit, A. (2015). The Influence of Higher Education Institutions on the Sustainability of ICT4D Initiatives in Underserved Communities. *THE ELECTRONIC JOURNAL OF INFORMATION SYSTEMS IN DEVELOPING COUNTRIES*, *71*(1), 1–16. https://doi.org/10.1002/j.1681-4835.2015.tb00516.x

Thetsane, R. M., Meyer, D., & Chambwe, M. (2024). An application of Hofstede's cultural dimensions and golden circle in entrepreneurship education. *The Southern African*

Journal of Entrepreneurship and Small Business Management, 16(1). http://dx.doi.org.ezproxy.uct.ac.za/10.4102/sajesbm.v16i1.934

Thomas, D. R. (2006). A General Inductive Approach for Analyzing Qualitative Evaluation Data. *American Journal of Evaluation*, *27*(2), 237–246. https://doi.org/10.1177/1098214005283748

Thuraisingham, D. M. V. (2023, May 24). *Cybersecurity in Lesotho: Current Challenges and Future Opportunities* [SSRN Scholarly Paper]. Rochester, NY. https://doi.org/10.2139/ssrn.4459493

Tomšů, M. (2021). Cybersecurity as a New Type of Security and Its New Perception. *2021 International Conference on Military Technologies (ICMT)*, 1–7. https://doi.org/10.1109/ICMT52455.2021.9502751

UN. (2021). LDCs at a Glance | Department of Economic and Social Affairs. Retrieved April 19, 2022, from https://www.un.org/development/desa/dpad/least-developed-country-category/ldcs-at-a-glance.html

Vakulyk, O., Petrenko, P., Kuzmenko, I., Pochtovyi, M., & Orlovskyi, R. (2020). CYBERSECURITY AS A COMPONENT OF THE NATIONAL SECURITY OF THE STATE. *Journal of Security and Sustainability Issues*, *9*(3), 775–784. https://doi.org/10.9770/jssi.2020.9.3(4)

van der Spuy, A., & Oolun, K. (2018). Promoting cybersecurity through stronger collaboration in Africa. *Available at SSRN 3275125*. http://dx.doi.org/10.2139/ssrn.3275125

van Vuuren, J. C. J., & van Vuuren, A. J. (2022). Preparing for the Fourth Industrial Revolution: Recommendations to Adapt Cyber Security Governance and Skills in South Africa. *Journal of Information Warfare*, *21*(1), 71–90.

Vasileiou, K., Barnett, J., Thorpe, S., & Young, T. (2018). Characterising and justifying sample size sufficiency in interview-based studies: Systematic analysis of qualitative health research over a 15-year period. *BMC Medical Research Methodology*, *18*(1), 148. https://doi.org/10.1186/s12874-018-0594-7

Walsham, G. (2006). Doing interpretive research. *European Journal of Information Systems*, *15*(3), 320–330. https://doi.org/10.1057/palgrave.ejis.3000589

World Bank, W. B. (2022). World Bank [Text/HTML]. Retrieved April 16, 2024, from World Bank website: https://www.worldbank.org/en/country/lesotho

World Population Review. (2024). Lesotho Population 2024 (Live). Retrieved April 16, 2024, from https://worldpopulationreview.com/countries/lesotho-population

Yalin, B. E. (2018). *CYBERSECURITY PERCEPTIONS OF UNIVERSITY STUDENTS IN TURKEY12*. *5*(16).

Yan, Z. (2022). The Dual Foundation of Cybersecurity Legislation. *Social Sciences in China*, *43*(3), 4–20. https://doi.org/10.1080/02529203.2022.2093065

Yin, R. k. (2015). Case Study Research Design and Methods (5th ed.). *Canadian Journal of Program Evaluation*, *30*(1), 108–110. https://doi.org/10.3138/cjpe.30.1.108

7. **Appendices**

7.1 Appendix: Ethics Approval

Faculty of Commerce

Private Bag X3, Rondebosch, 7701

2.26 Leslie Commerce Building, Upper Campus

Tel: +27 (0) 21 650 4375/ 5748 Fax: +27 (0) 21 650 4369

E-mail: jacques.rousseau@uct.ac.zaInternet: www.uct.ac.za

@Commerce UCT **UCT Commerce Faculty Office**

Khotso Mohale 13 02 2023

Department of Information Systems

University of Cape Town

REF: REC 2023/02/002

The Effects of stakeholder perceptions on cybersecurity Policy development outcomes:A case of Lesotho

We are pleased to inform you that your ethics application has been approved. Unless otherwise

specified this ethical clearance is valid until 29-Feb-2024 .

Your clearance may be renewed upon application.

Please be aware that you need to notify the Ethics Committee immediately should any aspect of your study regarding the engagement with participants as approved in this application, change. This may include aspects such as changes to the research design, questionnaires, or choice of participants.

The ongoing ethical conduct throughout the duration of the study remains the responsibility ofthe principal investigator.

We wish you well for your research.

2023.02.13 Signed by candidate

15:48:12 +02'00'

Jacques Rousseau

Commerce Research Ethics ChairUniversity of Cape Town Commerce Faculty Office

Room 2.26 | Leslie Commerce Building

Office Telephone: +27 (0)21 650 2695 / 4375

Office Fax: +27 (0)21 650 4369

E-mail: jacques.rousseau@uct.ac.za

Website: http://www.commerce.uct.ac.za/com/Ethics-in-Research

7.2 Appendix B: Research Interview Guide

cybersecurity Perception

a) Tell me about your experience while participating in Lesotho's Computer Crime and Cybersecurity Bill formulation process.
b) What were the main objectives and priority agenda items for Lesotho's Computer Crime and Cybersecurity Bill formulation initiative?
c) Which events or activities occurred within the past 10 years that could have necessitated the formulation of the Computer Crime and Cybersecurity Bill for Lesotho?
d) With justification, can you indicate whether the Computer Crime and Cybersecurity Bill is relevant in Lesotho's economic, technological, or social context?
e) Based on your understanding of cybersecurity, what benefit does a Computer Crime and Cybersecurity Bill play in the country?

Factors Influencing Perceptions

a) What factors contributed to your perception/understanding of cybersecurity?
b) Have you had exposure/experience or education to the subject of cybersecurity before you participated in the Computer Crime and Cybersecurity Bill development?
c) Do you believe there is a good understanding of cybersecurity among those participants formulating the Computer Crime and Cybersecurity Bill of Lesotho?
d) Please explain.
e) What factors do you believe influenced the extent of the understanding of cybersecurity among Bill formulation participants?
f) What actions do you think can positively improve the understanding of cybersecurity among Bill formulation participants?
g) What challenges if any, emerged in the Bill formulation process?

Association of Perceptions and Bill Outcomes

a) How do the effects of culture and values affect the country's posture to cybersecurity risk controls?
b) In what way does exposure, training, and subject knowledge contribute to the Computer Crime and cybersecurity Bill outcomes?
c) In what way did consideration of the sociocultural environment contribute to the Bill outcomes?
d) Do you believe that the Bill formulation process of Lesotho has sufficient representation from all relevant stakeholders? Please elaborate with examples.
e) What do you believe was your contribution to the Bill formulation process?
f) In your understanding, what are the main outcomes in the country's Computer Crime and cybersecurity Bill?

What other comments do you have about Lesotho's cybersecurity Bill formulation process?

Thank you for your participation in the study

7.3 Appendix C: Interview Consent Form

Department of Information Systems

Leslie Commerce Building Engineering Mall, Upper Campus

OR

Private Bag X3 - Rondebosch - 7701 Tel: +27 (0) 21 650 2261 Fax: +27 (0) 21650 2280 Internet: http://www.commerce.uct.ac.za/informationsystems

10/02/2023

Request to conduct research and interview participation consent form

Sir/Madam,

In terms of the requirements for completing a Master's Degree in Information Systems at the University of Cape Town, a research study is required.

The researcher, in this case, Khotso Mohale, has chosen to conduct a case study entitled; The Effects of Stakeholder Perceptions on Outcomes of the Computer Crime and Cybersecurity Bill: A Case of Lesotho. The objective of the research is to determine stakeholder's perceptions and how they affect the outcomes of the cybersecurity Bill .

Your participation in this research is voluntary, original data gathered from this study will be made available to others purely for academic purposes. No individual names will be recorded or published. You will not be requested to supply any identifiable information, ensuring anonymity of your responses. You can choose to withdraw from the research at any time for whatever reason, in accordance with ethical research requirements.

The data collection method will be one-on-one interviews with stakeholders who participated in development of cybersecurity policy for Lesotho. The interviews will be conducted virtually or at Ministry of work location of the participants and will last for 30 minutes to 1hour. If you are willing to participate in this study, kindly sign the attached form and return to me at your earliest convenience.

Should you have any questions regarding this research, please feel free to contact me on +266 58886390 or mhlkho035@myuct.ac.za.

Your participation in this study would be greatly appreciated but is entirely voluntary.

Sincerely,

Khotso Mohale

Researcher I am running a few minutes late; my previous meeting is running over. M.Com Student, (UCT)

Department of Information Systems

University of Cape Town

Email: mhlkho035@myuct.ac.za.

Ayanda Pekane

Research Supervisor

Department of Information Systems

University of Cape Town

Email: wallace.chigona@uct.ac.za

Research Participant Consent Form

I,_____, consent to participate in the research on the effects of stakeholder perceptions on the outcomes of cybersecurity Bill: A case of Lesotho. I am aware that participation is voluntary and that I may choose to withdraw from this study at any time, should I choose to do so.

_____ _____

Signature Date

7.4 Appendix D: Management Consent Form

Department of Information Systems

Leslie Commerce Building

Engineering Mall, Upper Campus

OR

Private Bag X3 - Rondebosch - 7701

Tel: +27 (0) 21 650 2261 Fax: +27 (0) 21650 2280

Internet: http://www.commerce.uct.ac.za/informationsystems

15 February 2023

Request for permission to carry out research using a sample of participants from the Ministry of Communications Science and Technology

Dear Sir/Madam,

As part of requirements for completing a master's degree in Information Systems at the University of Cape Town, I am required to conduct empirical research. The title of my study is: The Effects of Stakeholder's Perceptions on the Outcomes of the Computer Crime and Cybersecurity Bill: A Case of Lesotho. The objective of the research is to determine stakeholders' perceptions and how they affected cybersecurity Bill's outcomes.

This is to request your permission to use participants from your organization as part of the sample for respondents in the study. The ethical aspect of the research ensures the preservation of the identity of the participants. Data gathered in this study will be used for academic purposes only, these data will not include details that can identify participants. All personal details will be treated with the highest form of confidentiality. Participation in this research is voluntary and participants can opt out of the study at any time.

Data for the study will be collected using semi-structured interview with a small group of the staff who participated in cybersecurity policy formulation. The interviews will be conducted virtually or physical at the Ministry of Communication's Science and Technology premise and will last for 30 to 60 minutes. If you authorise this study to be undertaken at your organisation, please kindly sign the attached form and return to me at your earliest convenience.

Should you have any questions regarding this research, please feel free to contact me on +266 58886390 or mhlkho035@myuct.ac.za

Your organisation's participation in this study would be greatly appreciated. Sincerely,

Khotso Mohale

Signed by candidate

Researcher Thank you for reaching out. M.Com Student, (UCT) Department of Information Systems University of Cape Town

Email: mhlkho035@myuct.ac.za

Professor Wallace Chigona

Signed by candidate

Research Supervisor

Department of Information Systems

Ayanda Pekane

Signed by candidate

Research Supervisor

Department of Information Systems University of Cape Town Email:ayanda.pekane @uct.ac.za

Management Consent

I, ____, give the researcher of this study consent to conduct their study in the following organisation:

_____

_____

I am aware that participation is voluntary and that respondents may choose to withdraw from this study at any time, should they choose to do so.

_____ _____

Signature Date

"Our Mission is to be an outstanding teaching and research university, educating for life and addressing the challenges facing our society."

7.5Appendix E: Research Schedule

Research Deliverables	**Duration**	**Deliverable Date**
Research Proposal	4 months	June 2022
Full Literature Review	3 months	18th July 2022
Research Design	2 months	12 September 2022
Ethics Approval	2 months	13th February 2023
Data Collection	4 months	30th June 2023
Data Analysis	3 Months	30th Jully 2023
Write up	5 months	30th November 2023
Review of Dissertation	2 months	30th January 2024
Draft Submission and Review	1 month	13th February 2024
Dissertation Report & submission	3 Months	30th June 2024

7.6 Appendix F: List of Cyber Crimes in the Computer Crime and Cybersecurity Bill

1. Illegal access
2. Illegal remaining
3. Illegal interception
4. Illegal data interference
5. Illegal system interference
6. Data espionage
7. Cyber terrorism
8. Cyber extortion
9. Misuse of devices
10. Computer related forgery
11. Computer related fraud
12. Child pornography
13. Distribution of data message of intimate image without consent
14. Identity related crimes
15. Racist and xenophobic material
16. Racist and xenophobic motivated insult
17. Genocide and crimes against humanity
18. Unsolicited messages
19. Disclosure of details of an investigation
20. Cyber-bullying and harassment
21. Violation of intellectual property rights
22. Attempt, abetment and conspiracy
23. Publication of false information
24. Cyber squatting
25. Social engineering attacks
26. Interception of electronic messages or money transfers
27. Willful misdirection of electronic messages
28. Inducement to deliver electronic messages
29. Intentionally withholding messages delivered erroneously
30. Unlawful destruction of electronic message
31. Issuance of false electronic instructions