A Cybersafety Educational Framework for Primary School Learners in South Africa

by

Lean Kucherera

December 2020

A Cybersafety Educational Framework for Primary School Learners in South Africa

by

Lean Kucherera

213229706

Submitted in fulfilment of the requirements for the degree
Master of Information Technology

Faculty of Engineering, the Built Environment and Technology
Nelson Mandela University

Supervisor: Prof Lynn Futcher

December 2020

DECLARATION

NAME: Lean Kucherera

STUDENT NUMBER: 213229706

QUALIFICATION: Master of Information Technology

TITLE OF PROJECT: A Cybersafety Educational Framework for Primary School Learners in South Africa

I, Lean Kucherera (213229706), hereby declare that this dissertation in Master's in Information Technology is my own work and has not been previously submitted for assessment to any other institution or for any other qualification.

SIGNATURE: ……LKucherera……

DATE: November 2020

Official use:

In accordance with Rule G5.11.4, I hereby declare that the above-mentioned treatise/ dissertation/ thesis is my own work and that it has not previously been submitted for assessment to another University or for another qualification. However, material from publications by the student may be embodied in a treatise/dissertation/ thesis.

ABSTRACT

Information and communication technologies (ICTs) have made life much easier for many people but have also brought many dangers to the world. School learners are amongst the users of ICT who are becoming cyber citizens. This age is good at exploring new things, with a growing number of school learners having access to ICT devices, such as mobile phones, tablets and desktop computers. This is due to the affordability of mobile phones, which they normally receive as gifts from their parents. Due to easy access of ICT, school learners can now access cyberspace which offers them many advantages and benefits. Such advantages and benefits include having a platform to socialise, improved and ease of access to information as well as improving their learning. Despite these benefits, school learners (primary school learners in particular) are prone to falling victim to a range of cyber risks and attacks since cyberspace is an unregulated platform that poses many potential dangers

Common cybersafety threats associated with school learners include cyberbullying, sexting/“sextortion”, engaging with strangers, accessing inappropriate content and being exposed to a breach of privacy. Because the cybersafety of children, especially primary school learners, is often compromised, there is a need to protect them from the threats associated with ICT. However, protecting children from the aforementioned cybersafety threats is complicated because access to cyberspace is no longer confined to the home computer, but has extended to mobile phones, which are even more pervasive. Therefore, it is essential for school learners to be educated on how to protect themselves and their information in the virtual computer world.

A number of developed countries like Australia, New Zealand, Canada, United States of America (USA) and United Kingdom (UK) have included cybersafety education in their school curricula. Similarly, the rapid growth of the Internet around the world, allowed some countries in Africa to take the initiative to start implementing cybersafety education in schools including Mauritius, Tunisia, Kenya, Ghana, Mozambique, Cameroon, Egypt and Rwanda. Countries like Uganda, Sudan, Morocco and South Africa are still facing challenges in this aspect. This study is focused on the cybersafety of primary school learners in the South African context.

Cybercrime is very high in South Africa and the country has the third highest number of cybercrime victims in the world, contributing significantly to these cybercrime statistics. To circumvent cybercrime, a cybersafe culture is needed. However, cultivating a cybersafe culture in South Africa, may be challenging due to the huge diversity of the population in terms of religion, culture, language, economic dispensation; diversity of knowledge access and technology; as well as the absence of centralised e-learning policies and resources. Yet, ICT use in schools is becoming the norm and an increasing number of learners are exposed to ICT devices at school, ranging from mobile phones and tablets to computers.

Currently, South Africa has no formalised curriculum in place to teach learners about cybersafety and there is less involvement from the government's side to implement cybersafety education in South Africa. Nevertheless, some effort has been made to address cybersafety education in South Africa. The Department of Basic Education (DBE) has come forward with guidelines to assist schools in implementing cybersafety education. More so, researchers from various institutions like the Nelson Mandela University, the University of Johannesburg and the University of South Africa (Unisa) are still trying to assist in this regard. However, according to this study, when addressing cybersafety education in South Africa one has to look closely at the context which is being addressed. This might help in improving cybersafety education in South Africa. Therefore, this study proposes a framework on how to address cybersafety education, particularly for primary school learners in South Africa.

To address cybersafety education in South Africa, this study started with a literature review to identify the problem area, **many primary school teachers in South Africa are ill-equipped to implement cybersafety initiatives, thus leading to learners being vulnerable to cyber-related threats**. Thus, leading to the following identified research objectives together with research methods, to address the problem area.

To identify the key cybersafety threats and related risks to primary school learners.

To address this research objective, more investigations were conducted through literature review. This was in line to identify cybersafety threats and related risks for primary school learners. These threats and related risks were used towards developing the solution

To investigate current cybersafety initiatives both globally and in South Africa.

Having to identify the cybersafety threats and related risks to primary school learners. The next step was to investigate the current cybersafety initiatives in South Africa and globally. Therefore, a qualitative content analysis and another literature review were conducted, to identify what efforts are there in South Africa and globally.

To identify the main challenges relating to cybersafety education in the South African context.

The purpose of this research objective was to highlight main challenges relating to cybersafety education in South Africa. Therefore, to identify these challenges a comparative analysis, literature and argumentation were conducted**.**

To determine the key components required to overcome the challenges identified in addressing the cybersafety education of primary school learners in South Africa.

Finally, comparative analysis, literature review and argumentation were research methods used to identify key components required to overcome the challenges identified in addressing the cybersafety education for primary school learners in South Africa. Through argumentation, modelling and critical reasoning, these components were used to develop a framework for cybersafety education of primary school learners in South Africa.

ACKNOWLEDGEMENTS

Firstly, I would like to thank the God almighty for providing me with strength, knowledge, understanding and aligning me with the right people to support me to complete this dissertation. I would like to extend my gratitude to the following people:

- My supervisor, **Prof Lynn Ann Futcher,** for being patient with me as I struggled along the way facing difficult challenges in life. I acknowledge her for the support, guidance, and knowledge in shaping my area of study.
- **My siblings**, for the support, love and encouragement they gave me to keep me going when it was not easy, and when I felt like quitting.
- **Mr Gratitude Kudyachete**, for helping me to understand some of the processes in my research. I appreciate the time he gave me in his busy schedule.
- **Lisa Yokwe**, for proofreading my research.
- **Jeanne and Ronel,** for language editing and technical editing my research.
- **Friends**, for their prayers, support and encouragement.
- The financial assistance from **National Research Foundation (NRF)** and the NMU **Research Capacity Development (RCD)** towards this research is hereby acknowledged.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ACRONYMS AND ABBREVIATIONS

AUP	Acceptable Use Policy
CAPS	Curriculum Assessment Policy Statements
CIA	Confidentiality, Integrity, and Availability
CIE	Cambridge International Examinations
CJCP	Centre for Justice and Crime Prevention
DBE	Department of Basic Education
ICT	Information and Communication Technology
IEEE	Institute of Electrical and Electronics Engineers
ISO/IEC	International Organisation for Standardisation/International Electrotechnical Commission
NRF	National Research Foundation
NZ	New Zealand
OSTWG	Online Safety and Technology Working Group
RCD	Research Capacity Development
SACSAA	South African Cyber Security Academic Alliance
SONA	State of the Nation Address
SWGfL	South West Grid for Learning Trust
UK	United Kingdom
UNICEF	United Nations Children's Fund
USA	United States of America
WEF	World Economic Forum

CHAPTER 1
INTRODUCTION

1.1. BACKGROUND

Information and communication technology (ICT), which includes computers, mobile telephones and the Internet (Kritzinger, 2014a), plays a vital role in today's society. Examples of where these devices and technology are used include business, education, games, and social media. Boren (2014) noted that in 2014, the world had more mobile phones than people and 40 percent of the global population has access to ICT (Boren, 2014).

Media today makes use of the Internet which is convenient as it helps people to connect and communicate in business, social life and for many more reasons. Whilst it may be true that ICTs have made life much easier for many people, it has also increased the risk of exposure to danger to millions of people worldwide. When ICT is used in a positive way, it typically yields positive results; however, when used negatively, it can create macro-level disasters (Halder, 2015). ICT is associated with information security risks like identity theft and computer viruses (Kritzinger & Padayachee, 2007).

According to the World Economic Forum (WEF) school learners around the world, including South Africa are one group of ICT users who are becoming cyber citizens (Khanyile, 2019). These school learners are vulnerable online and 62 percent of them are exposed to at least one cyber risk (Khanyile, 2019). It is therefore important to create a culture of awareness with regards to the potential dangers of cyberspace and the actions that can be implemented to reduce the risk of being exposed to them. This culture can be achieved through cybersafety initiatives which primarily focus on the protection of the physical and emotional well-being of those using ICT. According to the Story Park website (2018) the safe and responsible use of ICT “is not just about keeping information safe and secure, but also involves being responsible with that information, being respectful of other people online, and using good ‘netiquette’ (internet etiquette)”.

Common cybersafety threats like cyberbullying, sexting/“sextortion”, talking or meeting with strangers (particularly through social media platforms), accessing inappropriate

content and exposure to a breach of privacy can also be found through the use of ICT devices (UNICEF, 2012). According to Smith, Mahdavi, Carvalho, and Tippett (2006) cyberbullying involves using electronic devices or technology to bully and harass someone while sexting involves sending a text of a sexual nature or nude images and sexually explicit photos (D'Antona, Kevorkian, Russom & Lauderdale, 2010).

Novice users of all ages (including school learners) are likely to face a range of ICT threats simply because of they are not familiar with the technology, making it difficult for them to recognise the potential threats and to understand the protection required (Atkinson, Furnell, & Phippen, 2009). Since the cybersafety of children, especially primary school learners, is often compromised, there is a real need to protect them from the threats associated with ICT. However, the task of protecting school learners is difficult because access to cyberspace is no longer confined to the home computer, but has extended to mobile phones, which are easily available for everyone. (Kritzinger & Padayachee ,2013).

In an investigation conducted by Kritzinger (2017a) focus was on learners who are 8 years or younger and the study noted that most primary school learners engaged in the survey (72 percent) own mobile devices. Livingstone and Smith (2015) also emphasised that more school learners than before now have access to ICT devices, such as mobile phones, tablets and desktop computers. Factors such as the increased affordability of mobile phones, the peer pressure to own one from a younger age and the increasing need to be connected to the Internet for school projects are further contributing to the complication. Ramaphosa's pledge in the 2019 State of the Nation Address (SONA) stated that every school age child will have access to a tablet device by 2025 (Presidency Republic of South Africa, 2019). This clearly indicates that more and more school learners will from now onwards have access to ICT devices.

According to Longe, Ngwa, Wada and Mbarika (2009) the Internet and mobile phones are platforms and tools that can be exploited for identity theft, email scams, trafficking, sexual exploitation and prostitution. Paedophiles disguising themselves as responsible citizens prey on children on cyber platforms like social networks, forums and chat rooms (Kritzinger & Padayachee, 2013). Kritzinger (2017a) is of the view that the age of learning about and experimenting with technology, cyberspace and social media starts as early as primary school. School learners that have access to

cyberspace benefit from socialising, having access to information and it helps with their learning. However, cyberspace is an unregulated platform, due to few rules governing cyberspace As a result, the platform is potentially dangerous for school learners, particularly learners in primary school who could easily fall victim to a range of cyber risks and attacks (Furnell, 2010). It should be noted that school learners now spend more time online than ever before (Park, Na & Kim, 2014). This shows that a growing number of school learners are being exposed to technology earlier on in life (Chandrashekhar, Muktha & Anjana, 2016; Srivastava, 2017; Rigby, 2017). Therefore, it is essential for school learners to be educated to protect themselves (and their information) in the cyber environment (Cross, Shaw, Hadwen, Cardoso, Slee, Roberts, Barnes, b2016; Kritzinger, 2014b)

Many cyber risks and threats associated with cyberspace may have a short- and/or long-term impact on the socio-physical and emotional well-being of school learners (Byron, 2008). Stone (2013) points out that cyber risks for school learners fall into three main categories:

- **Individuals' intentions to harm the learner** – Cyberbullying, trolling, flaming, excluding, masquerading, mobbing, denigrating, outing, harassing, cyber grooming, impersonation, blackmail, cyber snooping, identity theft, social engineering and online predators.
- **Learners' exposure to harmful online interactions** – Inappropriate content or material, digital reputation ruin, social platforms and chat rooms, viruses, malware and cookies.
- **Learners place themselves in harmful situations** – Illegal file sharing, plagiarism, inappropriate online posting, free downloads, copyright infringements, non-ethical postings of others' material and sexting.

Bada (2017) further elaborated on cyber risks and issues to be dealt with in primary schools, which include: passwords protection, managing privacy settings, observing cyber etiquette, meeting in person people initially met online, age-appropriateness and digital footprint. As these threats are so wide ranging in nature it is important that primary school learners are made aware of them and educated on how to best minimise them in order to protect their personal safety.

1.2. CYBERSAFETY GLOBALLY

Cybersafety education has been included in the school curricula of numerous developed countries across the world, e.g. the United Kingdom (UK), Australia, the United States of America (USA), New Zealand (NZ) and Canada. The government of the UK has successfully integrated the cybersafety curriculum at primary level (De Barros & Lazarek, 2018). Australia has incorporated several measures into the education of cybersafety in a bid to protect school learners (Department of Communications and the Arts, Australia, 2014). USA, NZ and Canada are also educating school learners about cybersafety (Kortjan & Von Solms, 2014).

However, in many African countries, cybersafety education is an issue that is often poorly advised and regularly overlooked. Most African countries have been regarded as lacking the skill of cybersafety (Kritzinger, 2017b). Moreover, Africa has high computer illiteracy and legislation that is not effective (Kritzinger, 2017b). However, due to the fast growth of the Internet around the world, some countries in Africa have taken the initiative to start implementing cybersafety education in schools including Mauritius, Tunisia, Kenya, Ghana, Cameroon, Egypt and Rwanda (De Barros & Lazarek, 2018). Also Mozambique has started to address the gap for cybersafety education among primary and secondary shool learners (Zucule de Barros & Lazarek, 2018). Whereas countries like Uganda, Sudan, Egypt, Morocco, Kenya and South Africa are still facing challenges in this respect (Von Solms & Von Solms, 2014).

1.3. CYBERSAFETY IN THE SOUTH AFRICAN CONTEXT

The availability of faster and cheaper access to the internet has increased the vulnerability of African countries to cyber threats (Wolfpack, 2013). In South Africa, service providers have even provided statistics to prove this effect. Cell C service provider stated that the effective price per megabyte has decreased by 20 percent in 2016, 36 percent in 2017 and 28 percent in the first half of 2018 (Pretorius, 2019). According to the 2013 Norton Report, South Africa scored 73 percent in terms of cybercrime and was listed as a country with the third highest number of cybercrime victims in the world (Symantec, 2013). The country with the highest cybercrime is Russia with 85 percent, seconded by China with 77 percent (Symantec, 2013).

South Africa lost more than R3.7 billion to cybercrime in 2012 (Mochiko, 2012). According to Mochiko (2012) cybercrime is dominant in internet banking, ecommerce

and social media sites. These statistics also include cybersafety. With around 1.5 million cybercrime victims each year, cybercrime has been largely ignored by the South African government (Magumane, 2012). In a recent survey conducted by the World Economic Forum, it has also been indicated that South Africa is among the top ten countries that are facing an increase in cyber risk (Khanyile, 2019).

Cultivating a cybersafe culture in South Africa, may be challenging due to the huge diversity of the population in terms of religion, culture, language, economic dispensation; diversity of knowledge access and technology; as well as the absence of centralised e-learning policies and resources (Czerniewicz, 2010). Yet, ICT use in schools is becoming the norm and an increasing number of learners are exposed to ICT devices at school, which include mobile phones, tablets and computers (DBE, 2010; De Lange, 2012). This is confirmed by the figures from the National Education Infrastructure Management System which show that as of March 2018, 9 313 primary schools around South Africa have internet connectivity (Writer, 2018).

Threats such as cyberbullying are a major concern, as many parents and teachers lack the capacity or self-confidence to address cyber risks (De Lange & Von Solms, 2012). In addition, teachers are not well trained on cybersafety, they have limited ICT capacity, and are ill-equipped to assist the learners (Kritzinger, 2014b) or handle ICT and cyber-related incidents. This is due to the generation gap, speed of internet growth, and lack of substantiated training. South Africa having 11 official languages could also be a factor, i.e. a language barrier that is affecting cybersafety awareness.

A substantial amount of available information and guidance about cybersafety is produced in the English language, as it is generally acknowledged as being the language of business in SA. It has been noted that South African legislation has made provision for foundation phase learners (from grade R up to grade 3) to be taught in their individual official language, this in turn contributes towards the digital divide. More so, the lack of budget within schools has been identified as a constraint to teachers in educating primary school learners about cybersafety, while access to technical infrastructure and geographical location are further barriers to cybersafety in South Africa (Kritzinger, 2015).

According to the statistics from the National Education Infrastructure Management System, as of March 2018, Gauteng has 280 primary schools with internet access

whereas the Northern Cape schools have no internet connectivity pipeline (Writer, 2018). Since technology is continually advancing, teachers may experience difficulties in keeping abreast with the rapidly changing online landscape, the associated cybersafety threats, as well as the various methods of protection from cybercrimes (Miles, 2011). According to South Africa's State of Nation Address, it is important that school educators receive annual training in ICT use, so that they are in a position to assist school learners (Presidency Republic of South Africa, 2019).

Kritzinger (2015) summarised the current situation in South Africa regarding school learner's awareness of cybersafety as follows:

- Limited commitment shown by the South African government to improve cybersafety awareness amongst school learners, nor are there any policies in place that protect learners in the event of a cyber incident. The government is not committed to the implementation of cybersafety education in the school curriculum.
- Teachers and schools are ill-equipped to implement cybersafety initiatives without backstopping support; they lack knowledge about ICT and are also hampered by limited resources (time and money).
- Schools are ill-equipped and have limited infrastructure to resolve problems with ICT devices and argue that there are economic, language and educational barriers within schools that contribute to the lack of a cybersafety culture in South Africa.
- Limited cyber-related initiatives are being implemented by the South African government.

The above list clearly indicates challenges that South Africa is currently facing regarding cybersafety education. Nevertheless, this study suggests that to a certain extent South Africa has made some efforts in trying to address cybersafety education. In 2010 the Department of Basic Education (DBE) provided guidelines to implement cybersafety education in schools. This contradicts the findings above and pre-dates it by seven years. These guidelines (DBE, 2010) include topics like plagiarism and copyright infringements, obsessive use of the Internet, exposure to unsuitable content, physical danger and sexual abuse, inappropriate or illegal online behaviours and

online harassment and cyberbullying. According to (DBE, 2010) the following role players were identified to be important when implementing cybersafety education in schools: teachers, learners, and their parents/guardians. However, the document was not clear when it comes to the role of principals and governing bodies.

Currently, South Africa has no formalised curriculum in place to teach learners about cybersafety (Von Solms & Fischer, 2017). The University of South Africa, the University of Johannesburg and the Nelson Mandela University have collaborated to form the South African Cyber Security Academic Alliance (SACSAA, 2011). The main responsibility of SACSAA is to provide free cybersafety education in the form of posters, flyers and school curricula (Von Solms & Von Solms, 2015). All this material for cybersafety education is available in English and very little material has been translated into other South African languages.

Most of the material that has been developed to educate school learners about cybersafety education by universities, research institutions, private and public organisations, in the attempt to keep school learners safe, is available online (Google, 2017; Unisa, 2017; University of Pretoria, 2017). Many children struggle to find the material online (Kritzinger, 2016; Von Solms & Von Solms, 2014) due to limited internet access in school and due to the language barrier as much of this material is available in English. To make information more accessible, the University of Pretoria has created teachers' manuals and activity books for school learners relating to cybersafety, while private sectors have secured partnerships with the government in trying to provide necessary ICT infrastructure in schools. This is being done through programmes like SA Connect which has already started to connect some of the schools, health centres, government facilities, post offices and Thusong service centres in rural areas. However, this is a relatively slow process as the programme started in 2013 and hopes to be completed only by 2030 (Mzekandaba, 2019).

1.4. PROBLEM STATEMENT

Based on the reviewed literature, the specific problem addressed by this research was the following:

Many primary school teachers in South Africa are ill-equipped to implement cybersafety initiatives, thus leading learners to be vulnerable to cyber-related threats.

1.5. RESEARCH OBJECTIVES

1.5.1. Primary Objective

To address the problem identified, the primary research objective of this study was:

> *To develop a framework for the cybersafety education of primary school learners in South Africa, in order to overcome the cybersafety threats and related risks that these learners are exposed to.*

1.5.2. Secondary Objectives

To achieve the primary research objective, the following secondary objectives were identified:

- **Secondary objective 1 (SO1):** To identify the key cybersafety threats and related risks to primary school learners.
- **Secondary objective 2 (SO2):** To investigate current cybersafety initiatives globally and in South Africa.
- **Secondary objective 3 (SO3):** To identify the main challenges relating to cybersafety education in the South African context.
- **Secondary objective 4 (SO4):** To determine the key components required to overcome challenges identified in addressing the cybersafety education of primary school learners in South Africa.

1.6. DELINEATION

This research focuses on supporting teachers in the cybersafety education of primary school learners in the intermediate phase (Grades 4 to 6) in South Africa.

1.7. RESEARCH PROCESS

This study commenced with a literature review to identify the problem areas with regards to cybersafety in primary schools in South Africa. It was evidenced that many primary school teachers in South Africa are ill-equipped to implement cybersafety initiatives, thus leading to learners being vulnerable to cyber-related threats. To address this problem area the following research objectives were identified (and also indicated in Table 1.1 below):

- **To identify the key cybersafety threats and related risks to primary school learners**

  In order to address this research objective, a further literature review was conducted. This aimed to identify what the cybersafety threats and related risks for primary school learners are (refer to Chapter 3.) These threats and related risks were subsequently utilised towards developing the solution (refer to Chapter 5).

- **To investigate current cybersafety initiatives both globally and in South Africa**

  The next step in this research was to investigate current cybersafety initiatives both globally and in South Africa. A qualitative content analysis and a literature review were used to identify what efforts, both globally and in South Africa, have been made with regards to cybersafety education (refer to Chapter 4).

- **To identify the main challenges relating to cybersafety education in the South African context**

  The main challenges relating to cybersafety education in the South African context are highlighted in Chapter 4. To identify these challenges a comparative analysis, a literature review and argumentation were undertaken.

- **To determine the key components required to overcome the challenges identified in addressing the cybersafety education of primary school learners in South Africa**

  Finally, in order to determine the key components required to overcome the challenges identified in addressing the cybersafety education of primary school learners in South Africa, a comparative analysis, a literature review and argumentation were conducted. Through argumentation, modelling and critical reasoning, these key components were used to develop a framework for cybersafety education of primary school learners in South Africa (refer to Chapter 5).

Table 1.1: Research Methods Related to Research Objectives

Objectives		Research method used
PO	• To develop a framework for cybersafety education of primary school learners in South Africa, , in order to overcome the cybersafety threats and related risks that these learners are exposed to.	Argumentation/Critical reasoning/ Modelling.
SO1	• To identify the key cybersafety threats and related risks to primary school learners.	Literature review
SO2	• To investigate current cybersafety initiatives both globally and in South Africa.	Literature review/ Qualitative content analysis.
S03	• To identify the main challenges relating to cybersafety education in the South African context.	Literature review/ Comparative analysis/Argumentation.
S04	• To determine the key components required to overcome the challenges identified in addressing the cybersafety education of primary school learners in South Africa.	Literature review/ Comparative analysis/ Argumentation.

1.8. ETHICAL CONSIDERATIONS

No ethical clearance was required in this study as all secondary data was obtained through review of the literature and content analyses.

1.9. STUDY OVERVIEW – LIST OF CHAPTERS

Chapter 1: Introduction – This chapter focuses on the background of this research study. The problem area is identified, together with the research objectives and the research methods that were used.

Chapter 2: Research Process and Design – The purpose of this chapter is to introduce the research process and design used in this study which is qualitative approach. This research approach involved undertaking a literature review, various content analyses, comparative analyses, critical reasoning, modelling and argumentation.

Chapter 3: Cybersafety – The aim of this chapter was to identify the key cybersafety threats and related risks to primary school learners (SO1). To attain this research objective an investigation around cyberspace was conducted. The chapter also discusses the advantages of cyberspace, the risks associated with using cyberspace, and explores safety measures around cyberspace.

Chapter 4: Cybersafety Education in Primary Schools – Chapter 4 focuses on investigating cybersafety education globally (SO2). Secondly, it presents the main challenges identified that relate to cybersafety education in the South African context (SO3). Next, it presents the key components necessary to overcome challenges identified in addressing the cybersafety education of primary school learners in South Africa (S04). It also discusses the commonalities, gaps and findings that were identified for developing key components of a cybersafety educational framework for primary school learners in South Africa.

Chapter 5: The Proposed Framework – The purpose of this chapter is to propose an appropriate framework to address cybersafety education for primary school learners in South Africa.

Chapter 6: Conclusion – This chapter summarises the research findings and argues how this study has met each research objective. This chapter also discusses the limitations of this study and notes considerations for possible future studies in the same research area.

1.10. CONCLUSION

This study primarily focused on primary school learners who have been identified as being highly vulnerable in cyberspace. It has been evidenced that they do not have the necessary skills and knowledge on how to protect themselves from cybersafety threats and related risks. Moreover, for the exact same reason, many teachers are not able to assist them. However, according to Kritzinger, Bada and Nurse (2017) cybersafety education must start as early as primary school since it is the entry point of education and the age to explore technology. Therefore, this study proposes a framework on how to address cybersafety education, particularly for primary school learners. To develop the proposed framework, this study followed the research process discussed in Section 1.6. Chapter 2 discusses in detail the research process followed by this study.

CHAPTER 2
RESEARCH PROCESS AND DESIGN

2.1. INTRODUCTION

Chapter 1 Section 1.1 provided a brief background on the challenges relating to cybersafety education in South Africa. These challenges include: a lack of commitment from the South African government regarding cybersafety education, ill-equipped teachers, a lack of infrastructure and limited cyber-related initiatives. Furthermore, the problem area of this study was also identified in Chapter 1 Section 1.4, followed by the research objectives of this study.

Chapter 2 discusses the research methodology in Section 2.2, describes the research setting in Section 2.3 and the research process in Section 2.4. The research process includes the following research objectives that were formulated to address this area of study: to identify cybersafety threats and related risks to primary school learners; to investigate cybersafety initiatives both globally and in South Africa; to identify the main challenges relating to cybersafety education in the South African context; determining the key components required to overcome the challenges identified in addressing the cybersafety education of primary school learners in South Africa; and developing a framework for cybersafety education of primary school learners in South Africa.

2.2. RESEARCH METHODOLOGY

The purpose of this section is to discuss the research methodology utilised by this study. In lay terms, research methodology is a way to conduct a research study (Williams, 2007). To conduct a research study, there are three common approaches that are followed, namely qualitative, quantitative and mixed methods (Matthews & Ross, 2010). A qualitative research approach aims to gain an understanding of primary reasons, motivations and people's perceptions towards their experiences around the world (Creswell, 2003). In a qualitative research process, texted data is analysed to bring up arguments, draw up conclusions or highlight any finding (Krippendorff, 1980). Normally in a qualitative research approach the researcher has a general idea of what he is looking for. A qualitative research approach involves methods such as semi-structured/unstructured interviews, gathering related documents and focus groups (Matthews & Ross, 2010).

A quantitative research approach is normally presented as numerical data (Walliman, 2010). Text data is grouped into certain categories and described as statistics to draw up conclusions or highlight any finding (Matthews & Ross, 2010). In a quantitative research approach, the researcher normally knows what he is looking for (Matthews & Ross, 2010). The quantitative approach includes closed-ended information such as content analyses, surveys and questionnaires and case studies (Creswell, 2003; Matthews & Ross, 2010).

The mixed methods research approach combines qualitative and quantitative research methods in a way that is suitable for a specific research project (Matthews & Ross, 2010). The researcher collects and analyses both numeric and narrative data and both result in qualitative and quantitative research process. This method benefits a study by overcoming the weaknesses of both the qualitative and quantitative research approaches (Williams, 2007).

For the purpose of this study, a qualitative research approach was followed.

2.3. RESEARCH SETTING

This research was conducted focusing on supporting teachers in the cybersafety education of intermediate phase primary school learners (Grades 4 to 6) in South Africa.

2.4. RESEARCH PROCESS

A research process is an overview of the objectives for a research project, specifying sources for data collection, and discussing how the researcher plans on conducting the research (Saunders, Lewis, & Thornhill, 2009; Mafuwane, 2011). Figure 2.1 provides an outline on how the research process was conducted to lead to the solutions for this study.

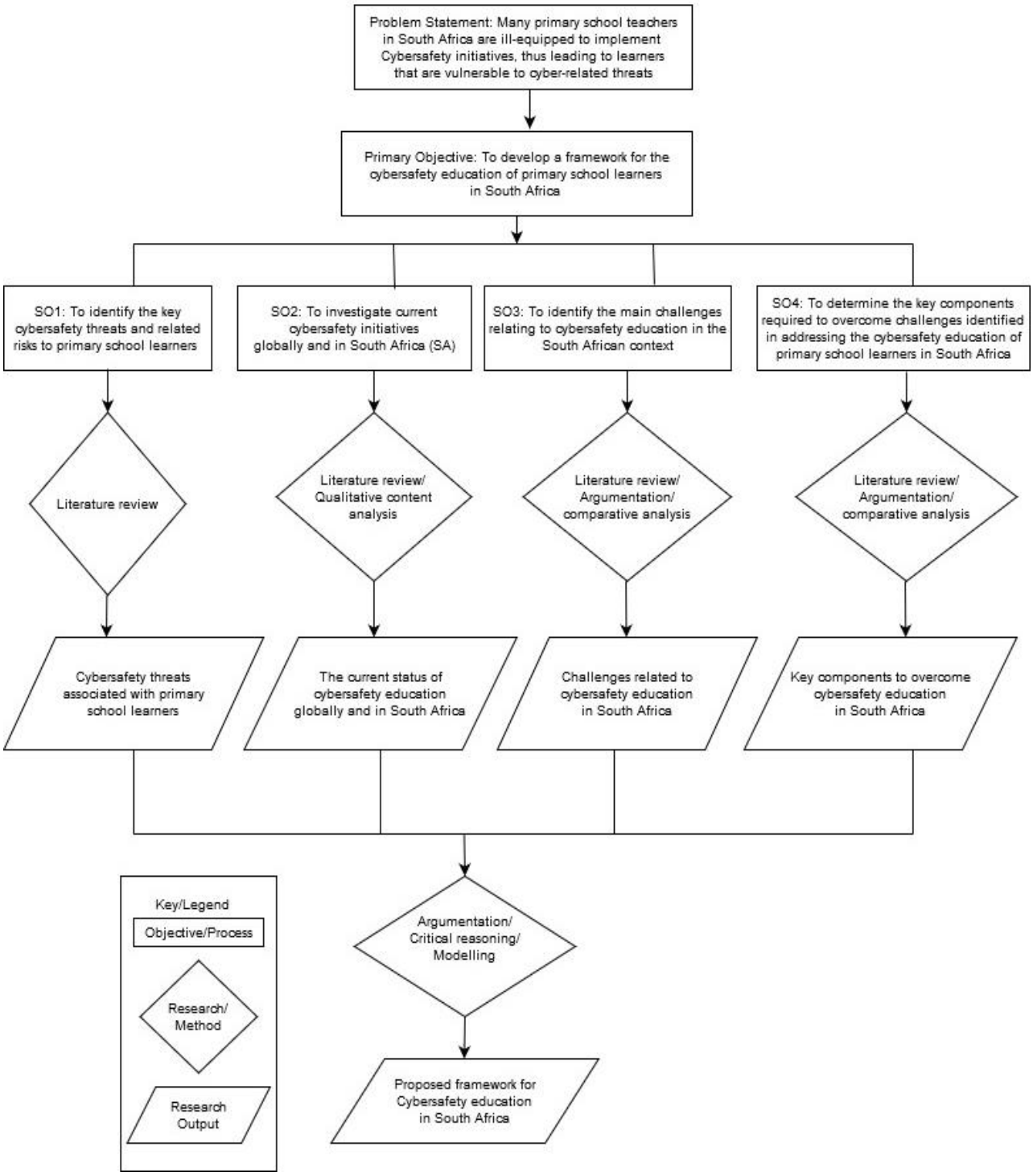


Figure 2.1: Research Process Diagram

To begin this study, a literature review was conducted. This involved reviewing a variety of articles, books, journals and other sources that were relevant to this study being undertaken. A literature review is a process of studying relevant information that

has been published previously (Boote & Beile, 2005). According to Matthews and Ross (2010), one will be able to discover what is already known about your research area; compare and contrast different sources and the opinions of experts; put your research into a context and find the important issues or variables in your topic. Through the information gathered in the literature review, a problem statement was identified, i.e. many primary school teachers in South Africa are ill-equipped to implement cybersafety initiatives, thus leading to learners that are vulnerable to cyber-related threats.

In order to address the identified problem area, research objectives were formulated in Chapter 1 (Section 1.4) and further literature reviews were undertaken to subsequently explore these objectives and to identify the key cybersafety threats and related risks to primary school learners. The identified cybersafety threats and related risks were further utilised in developing a framework for cybersafety education for primary school learners in South Africa – which is discussed and dealt with in Chapter 5.

During this study, related documents were gathered to collect data for further analysis. This was done using qualitative content analysis, literature review, and comparative analysis. According to Krippendorff (1980), content analysis is a research method for making replicable and valid inferences from data to their context, with the purpose of providing knowledge, new insights, a representation of facts and a practical guide to action. It is an empirical method in which data, text, images and expressions are analysed in the context of their use (Krippendorff, 1980).

When completing a content analysis, a researcher starts with a question in mind and reads the content of previous studies in order to ascertain if the findings within them are applicable to their own area of research study. A content analysis can either be qualitative or quantitative. In quantitative content analysis, text data is grouped into certain categories and described as statistics whereas in qualitative content analysis, texted data is analysed to bring up arguments, draw conclusions or highlight any finding (Krippendorff, 1980). This study conducted a qualitative content analysis to investigate current cybersafety initiatives globally and in South Africa.

To conduct the content analysis, firstly, the research objectives to be answered need to be selected and secondly, the sample to be analysed must be selected. Each

literature source is evaluated and, if the resource is found to be both trustworthy and relevant, it is analysed according to the thematic questions that have been chosen.

The thematic questions for this study were chosen from the following studies: Guidelines to Establish an e-Safety Awareness in South Africa (De Lange, 2012) and a Cybersecurity Awareness and Education Framework for South Africa (Kortjan, 2013). These thematic questions had to be dealt with prior to the development of the cybersafety education framework. Therefore, the following thematic questions were used to conduct a content analyses, which is presented in Chapter 4:

- What are the goals of the initiatives?
- Who are the overseers of the initiatives?
- What is the target audience?
- What are the topics to be covered?
- What resources are to be used?
- What is the context of the initiatives?
- Who are the role players?

2.4.1 Scope of the analysis

The objective of the literature review for this study was to examine cybersafety educational initiatives both globally and in South Africa to provide a clear overview of current cybersafety efforts. A search was conducted from a wide variety of sources, such as the Institute of Electrical and Electronics Engineers (IEEE), Science Direct, Springer, Research Gate, Google engine and Google Scholar. These sources were deemed as relevant to this research study by the researcher. To conduct a content analysis, the search term ‘cybersafety education’ was initially used as the key searching term and only studies from 2007 to 2018 were included. However, a further screening was conducted which solely identified cybersafety education for primary school learners and 24 articles were selected to investigate cybersafety education globally, in Africa and in South Africa.

To investigate cybersafety education globally and in South Africa, as discussed in Chapter 1 Section 1.1 and 1.2, the countries selected were Canada, UK, USA, Australia, NZ, Mauritius, Tunisia, Kenya, Ghana, Cameroon, Egypt and Rwanda. Some of these countries have already implemented cybersafety education at primary

school level, such as Canada, UK, USA, Australia and NZ. However, Mauritius, Tunisia, Kenya, Ghana, Cameroon, Egypt and Rwanda are still in their initial stages. South Africa is also still lagging in this aspect. Therefore, a content analysis focused on cybersafety initiatives of these countries as well as on nationally initiated and driven cybersafety educational initiatives. From the analysis, the efforts already made relating to cybersafety education globally and in South Africa were identified.

A comparative analysis was used to identify the main challenges relating to cybersafety education in primary schools in South Africa and to identify the key components required to overcome these challenges (SO3). According to Mills, Van de Bunt, and De Bruijn (2006) a comparative analysis is defined as a method to search for similarity and variance from different data sources. A comparative analysis is used to study two or more countries or cultures; it is commonly used in policy studies (Matthews & Ross, 2010). Normally a comparative analysis includes a detailed examination of an aspect, policy or issue. The researcher is not only interested in similarities and variances of countries, but also variances in the contexts (Matthews & Ross, 2010). These contexts may include the history, customs, institutions, ideologies, values and lifestyles of the country, culture, organisation or community (Matthews & Ross, 2010). Therefore, this aspect was quite relevant for this study as the focus was on the South African context, with unique values, customs, culture, community, history, lifestyle and institutions.

Through argumentation, the main challenges relating to cybersafety education in South Africa and the key components used to address them were argued (SO4). With argumentation, conclusions are reached through logical thinking (Van Eemeren & Grootendorst, 2004). In simple terms, argumentation forms the core principle of developing a solution (Tekeni, Botha & Thomson, 2015). Therefore, through argumentation a framework for cybersafety education of primary school learners in South Africa was subsequently developed.

Through critical reasoning and argumentation, key components to develop a framework for cybersafety education of primary school learners in South Africa were identified (SO4). Critical reasoning includes the element skills of analysing arguments, making suggestions, using inductive or deductive reasoning, judging or evaluating, and making decisions or solving problems (Lai, 2011). It involves both cognitive skills

and dispositions. These dispositions can be seen as attitudes or habits of mind and they include open- and fair-mindedness, interest, flexibility, a tendency to seek reason, a desire to be well-informed, and a respect for and willingness to entertain diverse viewpoints (Lai, 2011). A model can be defined as a “theoretical construct that represents physical, biological or social processes, with a set of variables and a set of logical and quantitative relationships between them” (Tomhave, 2005). It can be an abstract or a conceptual model and is not necessarily detailed in implementation. This means that it is a high-level construct representing processes, variables and relationships (Tomhave, 2005). Therefore, through modelling, a high-level framework was developed in this research, linking all the relationships between the identified key components.

2.5. CONCLUSION

Chapter 2 focused on the overview of the research methodology, the research process and the research setting of this study. It was highlighted (in Section 2.2) that all the research processes involved in this study utilised qualitative methods. The study was conducted through a literature review, modelling, critical reasoning, arguments, a comparative analysis and a content analysis. Therefore, the chapters to follow expand on these processes of the study, providing detailed information regarding the investigation conducted for this study, the solution and future recommendations.

CHAPTER 3
CYBERSAFETY

3.1. INTRODUCTION

Chapter 1 provided a brief background on the challenges regarding cybersafety education. These challenges include, but are not limited to, a lack of commitment from the South African government, ill-equipped teachers, lack of infrastructure and limited cyber-related initiatives.

Chapter 2 provided the research process that was followed in this study which included: a qualitative content analysis; a literature review; a comparative analysis; argumentation; modelling and critical reasoning.

Chapter 3 provides an overview of key cybersafety threats and related risks to primary school learners. The chapter also discusses the advantages of cyberspace, the risks associated with using cyberspace, and explores safety measures around cyberspace.

3.2. CYBERSPACE

The use of cyberspace in society has become undebatable (Kritzinger, Bada, & Nurse, 2017). According to Sawyer (2017) ICT and the Internet provide the backbone of cyberspace. De Wet, Koekemoer, and Nel (2016) defined ICT as the use of electronic gadgets such as computers, telephones, internet and satellite systems that store, retrieve and distribute information in the form of data, text and images. Cyberspace is described as an intricate context which results from the interaction of people, software and services on the Internet through technological devices and networks connected to it, which do not exist in any physical form (ISO/IEC 27032, 2012).

Cyberspace comprises digital storage, the exchanging and improving of data through networked systems and is supported by crucial information infrastructure. Hence, it can be viewed as a global community where 1.7 billion people are connected to exchange ideas, services and friendship (Kosseff, 2018). Figure 3.1 indicates the current number of users online around the world. It is identifying Asia, Europe and Africa as having the highest number of online users. Asia has 2197 million users, seconded by Europe with 719 million online users, followed by Africa with 492 million users.

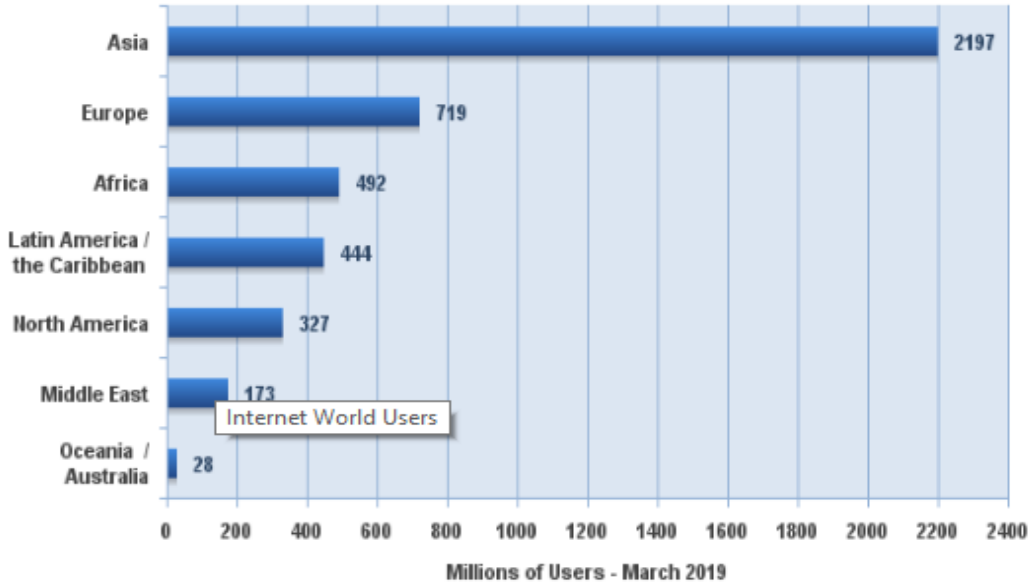


Figure 3.1: Internet Users in the World (Miniwatts Marketing Group, 2019)

Cyberspace has redefined the lives of many people, including those of school learners. The more school learners access cyberspace, the deeper and more diverse are their online activities (Livingstone et al., 2012a). It has been indicated in Figure 3.2 that school learners visit cyberspace for a variety of purposes such as education, socialising, gaming and information gathering, playing music, watching videos and uploading photos. In addition, Figure 3.2 presents some of the cyberspace activities that are undertaken amongst school learners of different age groups. However, this study focused on the target audience of 10 to 12-year olds, which typically comprises intermediate phase primary school learners in South Africa. Thus, information was gathered from age groups listed in Figure 3.2.

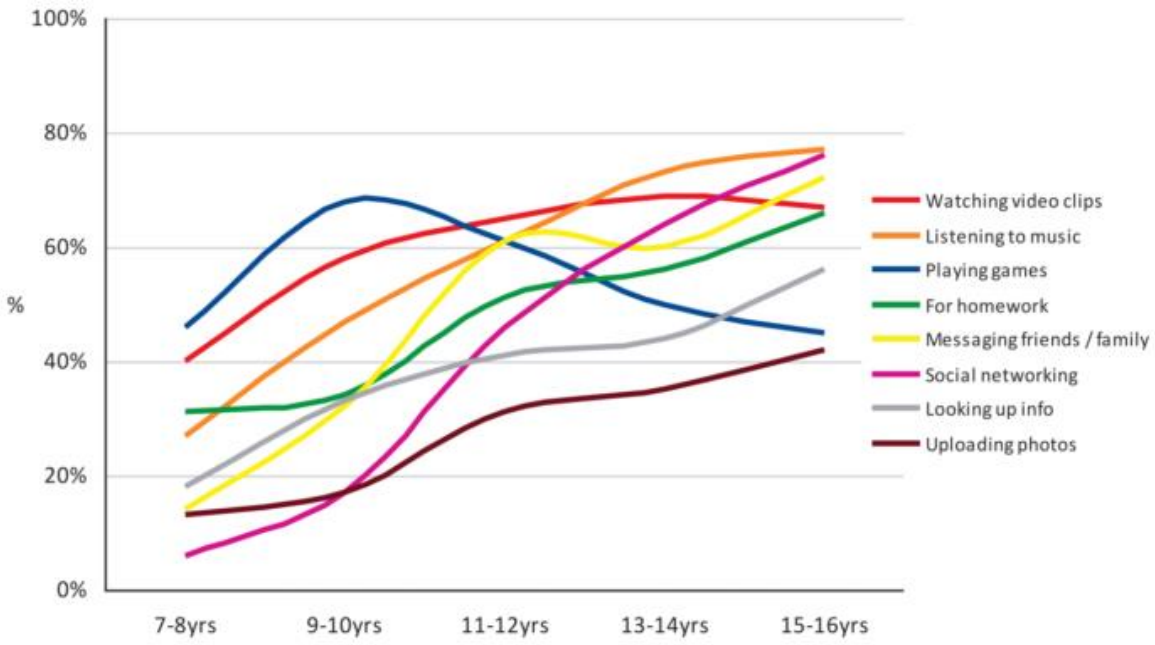


Figure 3.2: Reasons for Going Online, by Age (Livingstone, Davidson, Bryce, & Batool, 2017)

As illustrated in Figure 3.2, school learners aged between 10 and 12 years of age access most of the cyberspace activities. Due to their age, they make moderate use of social media platforms, education, information gathering and uploading photos. Conversely, they mainly access cyberspace for messaging friends/family, online gaming, listening to music, watching videos and education. With these activities comes various cyber-related risks and thus the need for the development and knowledge of cybersecurity, cybersafety and cyberethics.

3.3. DEFINING CYBERSECURITY

The global adoption of cyberspace has made its security a primary concern. Singer and Friedman (2014) emphasised that cybersecurity is a matter of global urgency that warrants clarity and understanding. Cybersecurity is used to secure cyberspace (Klaper & Hovy, 2014). It attempts to ensure the completion and maintenance of security properties of organisations' and users' assets against relevant security risks in the cyber-environment. The general security objectives include confidentiality, integrity and availability. These objectives are commonly referred to as the CIA triangle (Von Solms & Van Niekerk, 2013). Confidentiality ensures that any information being developed, accessed or processed is only available to authorised individuals (ISO/IEC 27002, 2005) whilst the focus of integrity is to guarantee that information remains

uncompromised, i.e. meaning that the information remains in its original state (Van Niekerk & Thomson, 2010). According to Klaper and Hovy (2014) cybersecurity is a technical discipline that defends digital systems against abuse and intrusion. Kritzinger (2011) defined cybersecurity as the physical safeguarding (both hardware and software) of personal data and technological resources from unauthorised access gained through technological means. Boyes' (2015) definition of cybersecurity is similarly holistic and includes people, processes, physical, and technological aspects. Cybersecurity has been defined as "the protection of cyberspace itself, the electronic information, the ICTs that support cyberspace, and the users of cyberspace in their personal, societal and national capacity, including any of their interests, either tangible or intangible, that are vulnerable to attacks originating in cyberspace" (Von Solms & Van Niekerk, 2013). The definition of cybersecurity by Von Solms and Van Niekerk (2013) includes the support of ICTs and the users of cyberspace, and thus these users need to be educated in cybersafety.

3.4. DEFINING CYBERSAFETY

According to Radoll (2014) cybersafety is a general term used to describe one's personal safety in the digital world. It is associated with all types of computers, mobile devices and all types of digital information from text messages, to social media, emails and website content. Cybersafety also focuses on the negative uses of cyberspace such as cyberbullying. Cybersafety can be described as the state of being shielded against any harm, any damage or failure in cyberspace which can be either physical, social, financial, political, emotional or occupational, and so on (ISO/IEC 27073, 2012). According to this definition, there is a clear indication that cybersafety focuses on the human aspect of harm and harm prevention when engaging with cyberspace. This definition of cybersafety was used for the purpose of this study.

Cybersafety can also be referred to as e-safety, internet safety, online safety or digital safety (Radoll, 2014). It can be used to educate children about the positives and negatives of using ICTs and aims to help safeguard children from internet predators, who often attempt to contact children online and arrange unmonitored meetings (Grey, 2019). However, cybersafety education is a complex matter; it can be particularly difficult for school learners to grasp as they do not fully comprehend the social and technical complexities of the Internet. Therefore, Berson and Berson (2004) are of the

view that cybersafety education should provide guidance and direction on cyberethics, in order to assist users to develop appropriate attitudes towards their safety in their use of ICT.

3.5. DEFINING CYBERETHICS

Cyberethics are the moral and ethical decisions that people make when they are using Internet-capable technologies and digital data (Pusey & Sadera, 2011). It refers to the code of responsible behaviour on the Internet. As with everyday life, people are taught to act responsibly whilst upholding moral values such as; *do not take what does not belong to you* and *do no harm to others*. These lessons are equally applicable in cyberspace. Therefore, it can be said that safe, responsible conduct on the Internet, should mirror that of good behaviour in everyday life. Cyberethics establishes boundaries for users to prevent self-harm and it also assists in identifying online risks in order to subsequently counteract them (Pruitt-Mentle, 2001). According to Kritzinger (2011) cyberethics deals with several different aspects including plagiarism, hacking, piracy and the uploading of inaccurate or incorrect data.

After briefly discussing cybersecurity, cybersafety and cyberethics, it is apparent that they are intricately linked. The following section serves to further discuss this relationship.

3.6. RELATIONSHIP BETWEEN CYBERSECURITY, CYBERSAFETY AND CYBERETHICS

Klaper and Hovy (2014) elaborated on the fact that while cybersecurity remains a very technical practice, it is people that make decisions and who have the ability to domineer cyberspace. Klaper and Hovy (2014) went on to suggest that it is important that users of cyberspace, that hold sensitive data, know the importance and application of safety principles and mechanisms. As previously mentioned, (in Section 3.3), good cybersecurity is holistic and based on a comprehensive approach that includes people, processes, physical and technological aspects. Cybersafety, as cited in Section 3.4, relates to individuals' personal safety within the digital domain. As with everyday society, it requires people to act with good moral intentions and values, which concurrently form the basic principles of cyberethics. Therefore, it is important

that users of cyberspace are aware of the threats and risks related to their behaviour when engaging in cyberspace.

The next section looks into the most common current cybersafety threats as they relate to primary school learners.

3.7. CYBERSAFETY THREATS

School learners are becoming cyber citizens. Access to cyberspace has provided them with a multitude of benefits, from increased access to resources and knowledge, to improved and expanded methods of communication. However, this leaves them vulnerable to becoming victims of cybersafety risks. The increase in the use of technology worldwide has caused an increase in the occurrence of cyber threats as a form of aggression amongst learners (Smit, 2015). To help build awareness of potential issues that can happen while using these technologies, it is vital that school learners appreciate and understand the cybersafety threats associated with cyberspace. The most common cybersafety threats amongst primary school learners include: cyberbullying, immoral or illegal online behaviours, physical danger, sexual abuse, invasion of privacy, plagiarism and copyright violation, inappropriate content, online gaming, identity theft and talking to and meeting strangers (DBE, 2010; Grey, 2019; Kritzinger, 2015; De Lange, 2012; Von Solms & Von Solms, 2014; UNICEF, 2012; Third, Forrest-Lawrence, & Collier, 2019).

3.7.1. Online Harassment and Cyberbullying

Cyberbullying can take various forms and includes using ICT devices for sending unwanted messages; “cyber stalking” and the posting of hurtful or insulting statements about others that can make them feel uneasy, upset, depressed, or afraid. School learners often form groups and friendship circles in cyberspace where activities that start out as harmless and innocent fun, such as expressing a different opinion to another school learner, can quickly turn into something much more serious. In South Africa, cyberbullying has remained a concern as recently a teenager committed suicide due to repeated, unwanted online communication (Gous, 2019). School learners need to be informed that online bullying carries serious consequences (DBE, 2010). It is therefore crucial that learners understand that the same rules apply to

bullying in both the physical and cyber worlds. School learners must likewise be taught how to appropriately respond to cyberbullying.

3.7.2. Inappropriate or Illegal Online Behaviours

School learners may become involved in other inappropriate, anti-social or illegal behaviour while using ICT. Such behaviours include, but not limited to the following (DBE, 2010):

- Identity theft
- Participating in hate or cult websites
- Buying and selling stolen goods
- Divulging or sharing personal information online
- Posting endangering information which may taint a person's reputation.

The teaching of appropriate behaviour and critical thinking skills is essential as it will enable school learners to be safe and lawful when in cyberspace (DBE, 2010). School learners involved in risky or illegal behaviours in cyberspace may benefit from professional support or counselling to readdress the balance of their cyberspace and real-world life (DBE, 2010). Some school learners may become participants or victims of major cyber risks. It is important that school learners become aware of how dangerous it is to leave online tracks, also known as a CyberCV. A CyberCV can contain personal information which includes remarks that individuals have made or that have been made about them online, and future employment opportunities may be negatively affected along with an increased exposure to identity theft (DBE, 2010).

3.7.3. Physical Danger and Sexual Abuse

Some criminals use cyberspace services such as "chat-rooms" to interact with school learners (DBE, 2010). Their aim is to create and develop relationships with school learners in an attempt to persuade them into sexual activity and exploitation (DBE, 2010). Paedophiles often target specific individuals, to develop an online friendship by pretending to be a school learner with similar interests and hobbies until they gain the trust of the learner to such an extent that they create other forms of communicating like text messaging and eventually meeting in person. They could possibly persuade the learner to participate in creating or distributing inappropriate material such as explicit photographic images. Such acts are examples of criminal conduct and any

adult persons who commit such acts can be convicted of the “sexual grooming” of children.

Cyberstalking is whereby individuals keep track of the activities of their victims through their participation on social networking sites (DBE, 2010). This can result in physical stalking if the location of the targeted individuals are revealed in cyberspace. Therefore, school learners need to understand that giving personal information, sharing pictures of an explicit nature or arranging to meet their online contacts, could pose a direct risk to their safety, and/or that of their loved ones (DBE, 2010).

3.7.4. Inappropriate Content

Exposure to inappropriate material poses risks when in cyberspace. School learners can be exposed to unsuitable content (De Lange, 2012), such as pornographic material, content that is hateful or violent in nature, activities that are dangerous or illegal, and/or material that is inappropriate for their age or biased (DBE, 2010). Cyberspace is open to all, but sadly this also means that everyone can share their ideas without restraint or considering the effects those views may have on others. Therefore, one can access inappropriate content unknowingly either by clicking unknown links or pop ups or by searching using the wrong terms (Paraiso, 2016). Cyberspace is host to an enormous amount of pornographic material. Through the use of ICT devices such as mobile phones, school learners may become involved in the creation and circulation of inappropriate content and indecent images. Thus, they may consciously or otherwise be adding to the available online pornography content (DBE, 2010). It is important to raise awareness amongst school learners that inappropriate content poses a direct risk to them.

3.7.5. Obsessive Use of the Internet

De Lange (2012) identified that addictive behaviours and obsessions can be developed by school learners who are regularly engaged in cyberspace. This is concurrent with the DBE’s (2010) report which found that typical addictive behaviour in cyberspace creates the potential for school learners to become obsessed with the online world. As a result, this has a negative impact on their lives. Spending a great deal of time in cyberspace causes a drop in the quality of schoolwork being produced, results in learners having less sleep, and may have negative impacts on their family

relationships (DBE, 2010). All of these are indications that cyberspace has the potential to take too high a priority in a school learner's life and, if not managed appropriately, can have serious effects on their academic performance (DBE, 2010). According to De Lange (2012) such obsessive use or addictive behaviours may lead the school learner to feel lonely and depressed.

3.7.6. Sharing of Information

We live in a world where information is vital to our everyday lives. Most information is now available online and a number of websites have made it easy to share information (De Lange & Von Solms, 2012). Children connect to one another through cyberspace, using mobile phones, emails, social media and many more (Von Solms & Von Solms, 2014). Common platforms include Facebook, Twitter and My Space for communicating between individuals (De Lange, 2012). It has become inexpensive to upload and publish information due to these technologies. However, criminals are targeting these media platforms to commit cybercrime. School learners are uploading information on social media without contemplating the consequences, and thus they serve to be easy targets for those who aim to groom or predate them (De Lange, 2012).

More so, misusing ICT devices in the school environment includes spreading anything not related to school such as large file attachments. This does not only affect the connectivity speed but also becomes time consuming to manage the inappropriate and personal activities carried out during school hours which can end up being costly to the performance of the teacher and the learner (DBE, 2010).

Hence, it is important that school learners be educated on how to protect their own privacy online, including the sharing of passwords, personal details and spreading information that is not school related.

3.7.7. Game Addiction

School learners are becoming increasingly addicted to the Internet and mobile phone chats, spending more time online. Many learners neglect their schoolwork, have limited sleeping time and neglect family time and relationships because of their internet obsession (DBE, 2010). According to the DBE (2010) game addiction is another risk

factor which school learners may be exposed to. Many learners would prefer to play online games rather than go out with their friends or play a sport. The addiction of games can lead to poor health, poor eating habits and bad social reputation (Von Solms & Von Solms, 2014). Games may require money to purchase them online, which can be very expensive or expose school learners to identity theft (as they are not aware if it is a trusted website) as they upload their personal information online (Von Solms & Von Solms, 2014). Games are often designed to keep people returning to play them through the use of daily rewards or special features that can only be obtained once a set number of playing hours have been reached. It is therefore crucial that school learners be monitored and educated about the negative effects associated with prolonged hours spent online.

3.7.8. Copyright

School learners have been indicated to regularly download music files and copy and paste homework assignments. They often do this with little or no awareness that copyright laws apply on the Internet. School learners need to be taught that it is illegal to download information, music, images, videos and software without the owner's consent. They also need to be taught that it is unethical to use someone's work as their work or their own idea (Kritzinger, 2011). Topics such as referencing, and citations must be taught to learners when they are writing their assignments. Social media is regarded as one of the platforms that has allowed the sharing of information without acknowledging the source (DBE, 2010). It is important that learners are made aware that copyright laws also apply in cyberspace.

3.7.9. Sexting

Sexting can be defined as the act of sending and receiving sexually suggestive text messages, photos or videos (Burton & Mutongwizo, 2009). It also refers to the participation of school learners in sending and receiving sex content, which can be termed child pornography or paedophilia (Online Safety and Technology Working Group, 2010). School learners need to be educated on how unethical it is to circulate sex content and that they may be breaking the law in doing so.

3.7.10. Talking or Meeting with Strangers

Cyberspace gives school learners the ability to converse as well as freely and remotely share ideas and knowledge (UNICEF, 2012). However, sharing information and online chatting often prompts individuals to then meet up face-to-face (UNICEF, 2012). Unfortunately, sharing of information and chatting offers a wide platform for predators as well (Paraiso, 2019). According to Canadian statistics, between 2014 and 2016, cyber-related criminal activity increased from 15,000 cases to 24,000 cases and 22 percent of these cases targeted school learners in the form of making and distributing of child pornography, exploitation and child luring (Eagle, 2018). In South Africa, news reports and research studies have highlighted that many school learners are meeting an increasing number of strangers online and subsequently meeting them in person (UNICEF, 2012).

3.8. CONCLUSION

This chapter identified cybersafety threats in cyberspace as they relate to primary school learners. Cyberspace has proven to be beneficial to many; however, primary school learners should be made aware that it also has a dark side. Hence, it is important that primary school learners recognise the benefits and risks associated with cyberspace. Many primary school learners are being affected by these risks and they do not know how to adequately respond. It is important that these primary school learners are taught how to identify these cybersafety threats. To cultivate this culture among primary school learners, cybersafety education is essential. As such, cybersafety educational initiatives in developed and developing countries were investigated and are presented in the next chapter. This investigation was undertaken by the researcher in order to identify the key components that could guide the proposed framework for cybersafety education for primary school learners in South Africa.

CHAPTER 4
CYBERSAFETY EDUCATION IN PRIMARY SCHOOLS

4.1. INTRODUCTION

Chapter 3 described and discussed what is meant by some of the key terms utilised when referring to cyberspace. It explored the concepts of cybersecurity, cybersafety, cyberethics and how they inter-link.

Chapter 4, Section 4.2, discusses global cybersafety educational initiatives, while Section 4.3 discusses cybersafety educational initiatives in Africa (excluding South Africa). Section 4.4 discusses cybersafety educational initiatives in South Africa. Section 4.5 comprises a discussion of all these findings. How to address cybersafety education in South Africa is explored in Section 4.6.

To investigate current cybersafety initiatives globally, in Africa (excluding South Africa) and in South Africa (SO2), this chapter presents the literature that was reviewed for this purpose, as well as a qualitative content analysis (in order to address this research objective). The chapter points out the main challenges identified relating to cybersafety education in the South African context (SO3) and the key components identified that are required to overcome these identified challenges; in addressing the cybersafety education of primary school learners in South Africa (SO4). To address these research objectives a literature review, comparative analysis and argumentation were used.

These research methods are discussed, in detail, in Chapter 2 Section 2.4 including the process followed to conduct a qualitative content analysis and a comparative analysis.

Section 4.2 presents global cybersafety educational initiatives that the researcher investigated. A literature review and a qualitative content analysis were both conducted to investigate the efforts that have been made to date.

4.2. GLOBAL CYBERSAFETY EDUCATIONAL INITIATIVES

School learners are being exposed to technologies at a very early stage (De Lange & Von Solms, 2012). Hence, they must be taught how to make wise decisions online as they would in real life, for instance not to talk to strangers, not to give away personal information and not to go to unsafe places (Von Solms & Von Solms, 2014). “The

pedagogy for educating school children about cybersafety threats should be the same as traditional education of children on ethics and the grounded principle of ‘do no harm’” (Kritzinger, 2015). Therefore, it is wise to properly educate children on rules that govern cyberspace at an early stage when they are adopting the use of technology (Kritzinger, 2017a). Developed countries have included cybersafety education in their school curricula and amongst these countries is the United Kingdom (UK), where all school learners from the age of 11 to 14 years are educated on cybersafety (Farrell, 2014). Australia has implemented several cybersafety measures to better protect their learners (Australian Government, 2014). Countries such as Canada, USA and NZ are also educating school learners about cybersafety (Kortjan & Von Solms, 2014). The remainder of this section focuses on these developed countries and their respective cybersafety positions, specifically amongst primary school learners.

Table 4.1: Summary of Findings for Cybersafety Educational Initiatives Globally

Initiative	Goal	Overseers	Target audience	Role players	Delivery method		Resources	Access method	Context
ThinkUknow https://www.thinkuknow.co.uk/8_10/grown-ups/	Protect children both online and offline.	NCA-CEOP	8 to 10year olds and 11 to 13-year olds	Teachers and learners	Education curriculum		Videos and stories	Bandwidth	English UK
Safer Internet centre https://www.netsafe.org.nz/the-kit/resource/the-primary-zone-resources-for-3-11s-safer-internet-centre-uk/	Helps children to stay safe online.	Childnet International, InternetWatch Foundation and SWGfL	Primary school learners (3 to 11-year olds)	Teachers and learners	Education curriculum		Films, eBooks, games, and quizzes	Bandwidth	English UK
UKCCIS https://www.thinkuknow.co.uk/professionals/guidance/ukccis-framework-education-for-a-connected-world/	Protect children and young people to navigate in the digital world.	UK Government	7 to 14-year olds	Teachers and learners	Education curriculum		Framework curriculum	Offline	English UK
Cyber Safety for K-12 https://rems.ed.gov/docs/Cyber_Safety_K-12_Fact_Sheet_508C.PDF	Aims to protect children from obscene or harmful content on the Internet.	Readiness and Emergency Management for schools	Primary school learners (K-12)	Teachers and learners	Education curriculum		Power point slides, videos, presentations, classroom activities and tip sheets.	Offline/ Bandwidth	English USA

Internet safety https://www.cybertip.ca/app/en/internet_safety-for_children	To help educate Canadians about how to keep children safe while online.	Canadian centre Child protection	Primary school learners (5 to 11 years)	Teachers and learners	Education curriculum		Books, power point presentations, and videos	Offline/ Bandwidth	English Canada
e-Safety https://esafety.gov.au/education-resources/classroom-resources	Helping all Australians have safe, positive experiences online.	Australian Government	Middle primary school learners	Teachers, learners and parents	Education curriculum		Videos, games and blogs	Bandwidth	English Australia
Netsafe https://www.netsafe.org.nz/advice/young-people/page/3/	To educate the community on the risks of cybercrime.	Industry Government	Primary school learners (3 to 11 years)	Teachers and learners	Education curriculum		Videos	Bandwidth	English New Zealand
Stop.Think.Connect https://www.cisa.gov/sites/default/files/publications/Kids%20Cybersecurity%20Presentation.pdf	Campaign to help Americans understand the dangers that come with being online	Industry Government	School learners (8-18 years)	Teachers, Learners, Parents	Education curriculum		Games, books, presentations, work sheets	Bandwidth/ Offline	English USA

Table 4.1 is a presentation of the cybersafety educational initiatives like ThinkUknow, e-safety, Netsafe, UKCCIS, Internet safety, cybersafety for K-12, Safer Internet Centre and Stop.Think.Connect are applicable and available to primary school learners in the developed countries studied. As previously stated, these countries have implemented cybersafety education for primary school learners. In every one of these initiatives the following were identified: the goal of the initiative, the overseers (the individuals that are responsible for the initiative), target audience (who the initiative is aimed at), role players (the individuals that are involved in the initiative), delivery method (where the material is delivered), the resources to be used in the initiative, access methods (whether it be on line or off line learning) and context (i.e. the geographical location, the language utilised and the age appropriateness).

Many of these initiatives have created their own resources to educate primary school learners, with the exceptions of Netsafe initiative and K-12 initiative, which make use of resources from other initiatives, for example, ThinkUknow initiative. These countries have all utilised the English language in order to deliver and implement an educational curriculum inclusive of cybersafety. Furthermore, there is clear evidence of more than one delivery method being used to communicate cybersafety education. Access to most of these educational curricula requires bandwidth; as very few of them are supported offline.

4.2.1. Cybersafety Threats for Primary School Learners Globally

Figure 4.1 below is a graphical representation of cybersafety threats as they relate to primary school learners for each of the initiatives studied during this research. For a complete list of each of the cybersafety threat topics identified from global educational initiatives refer to Appendix A.

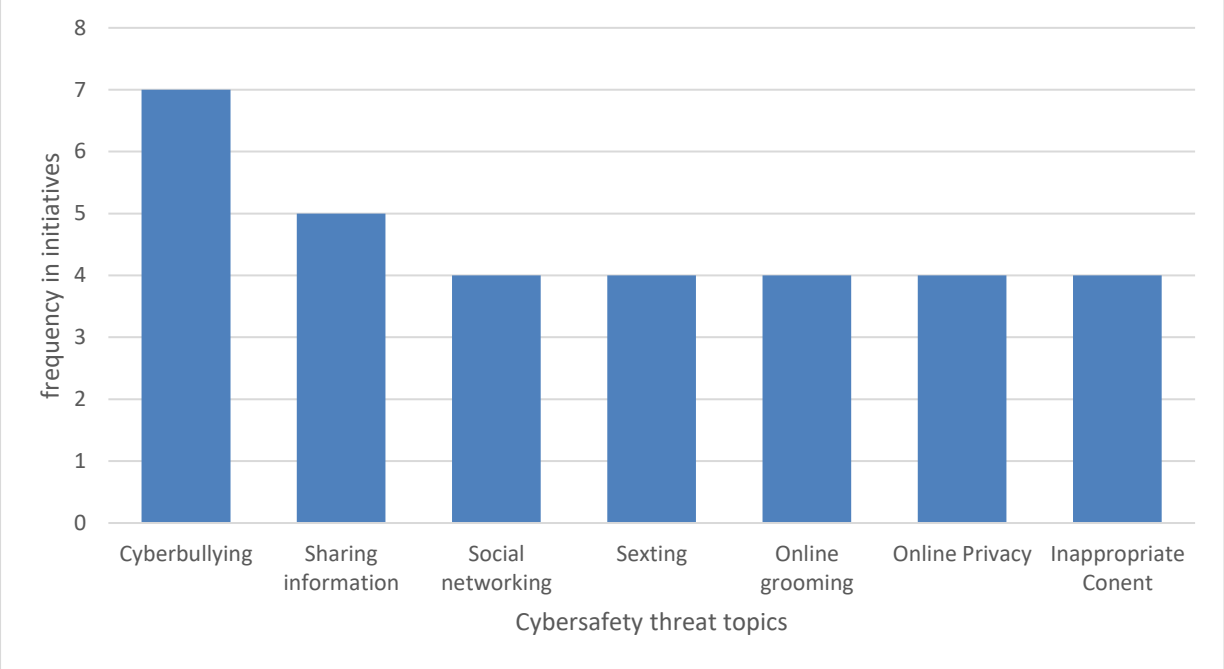


Figure 4.1: Global Cybersafety Threat Topics

Figure 4.1 illustrates the seven common cybersafety threat topics that were included in global initiatives aimed at educating primary school learners about cybersafety. As indicated, all of the initiatives studied covered the topic of cyberbullying, which infers that it is perceived as a principal threat to primary school learners. Followed by sharing information which was covered by almost initiatives. Four initiatives covered topics of a sexual nature, i.e. grooming and sexting, online privacy and inappropriate content. Whilst no reasons are provided for such, one could surmise that such topics may be deemed age inappropriate, particularly with those in the younger primary school grades. Social networking was also only covered four initiatives, which may be since most social networking sites (Facebook, Twitter, Instagram, Snapchat and Skype) require users to be 13 years or older; therefore, they are not primary school aged learners.

4.3. CYBERSAFETY EDUCATIONAL INITIATIVES IN AFRICA (EXCLUDING SOUTH AFRICA)

Section 4.2 investigated cybersafety educational initiatives for developed countries. The same content analysis process followed in Section 4.2 was applied in order to investigate cybersafety education in African countries; with the exclusion of South Africa.

The issue of cybersafety education has been a challenge in developing countries, especially within Africa. Many school learners are being exposed to cybersafety threats and related risks (Dlamini & Modise, 2012). This is due to a lack of the requisite knowledge and skills in cybersafety (Dlamini, Taute, & Radebe, 2011). According to Von Solms and Von Solms (2015) Rwanda, Tunisia, Kenya, Ghana, Cameroon, Egypt and Maurituis have begun to address cybersafety education. Rwanda and Mauritus has started on addressing cybersafety education among children, where as Ghana the focus to address cybersafety education is in high schools at the moment (Kingson, 2019).

In Tunisia the department of education and DCAF has already started to promote the need of cybersafety education in schools (DCAF, 2018). Through research departments, Mozambique has started to address the gap for cybersafety education among primary and secondary shool learners (Zucule de Barros & Lazarek, 2018). In Cameron, Kenya, Egypt and Tunisia there is still a lack of published studies with regards to cybersafety education. Uganda, Sudan and Morocco do not have measures yet in place for national cybersafety initiatives (Von Solms & Von Solms, 2014). Table 4.2 refers to cybersafety educational initiatives in Africa (excluding South Africa). This table was derived using the thematic questions identified in Chapter 2 Section 2.4. The headings/sections of Table 4.2 are as discussed in Section 4.2 of this chapter.

Table 4.2: Summary of Findings for Cybersafety Educational Initiatives in Africa (excluding South Africa)

Initiative	Goal	Overseers	Target audience	Role players	Delivery method	Resources	Access method	Context
Cyberteq http://rwandainspirer.com/2018/01/28/why-children-should-be-aware-of-cyber-crimes/	Children should be aware of cybercrime.	Industry	Primary school learners (11 years old)	Industry and learners	Classroom	Power point slides	Offline	English Rwanda
National Computer Board http://cybersecurity.ncb.mu/English/Pages/Kids.aspx	To educate the community on the risks of cybercrime.	Industry and Government	Kids (age not specified)	Children, industry, government and parents	Website	Blog	Online	English Mauritius
A Cyber Safety Model for Schools in Mozambique Zucule de Barros & Lazarek, 2018	Promoting a cyber safety culture among children and young people.	Researchers (Technical University of Dresden, Germany)	Primary and secondary school learners	Teachers Learners Private sector Parents Government International cooperation	Model	Posters Leaflets Books Newspaper article Workshop Videos	Offline/ Online	Portuguese and other languages

Table 4.2 presents cybersafety educational initiatives in Rwanda, Mozambique and Mauritius. There is a clear indication that cybersafety education in these countries is still in its early stages. Some of these initiatives have goals which are to address cybersafety among primary school learners for Rwanda and Mozambique, whilst Mauritius focuses on the community. It is illustrated in Table 4.2 that these initiatives have overseers, namely the government, research departments and industry. Furthermore, these initiatives target a specific audience which in this case includes primary school learners.

As indicated in Table 4.2, the delivery method used in Rwanda for teaching cybersafety is through classroom learning (offline), in Mozambique materials will be accessed offline medium such as newspapers, books, leaflets, posters and workshops and through online methods such as videos. Mauritius the material can accessed via a website (online). In Mozambique cybersafety education has tried to focus in addressing their context whereas Rwanda and Mauritius initiatives are delivered in English, which highlights some of the challenges we are currently facing in South Africa, as a nation with 11 official languages, regarding cybersafety education. Having investigated these initiatives, there is a clear indication that Africa is still in its early stages regarding the development and delivery of cybersafety education. As indicated in Table 4.2, Africa as a whole is under resourced, and the context, specifically the language of delivery (i.e. English) of cybersafety education, remains a concern and as found with Mauritius, the goal is primarily aimed at the wider community and there is little or no focus on primary school age learners.

The following were concluded to be the common topics covered in cybersafety educational initiatives in Africa (excluding South Africa): cyberbullying, online etiquette, social networking, identity theft and inappropriate language. For a comprehensive list of these cybersafety threats please refer to Appendix B.

Cybersafety educational initiatives identified in South Africa are discussed in the next section.

4.4. CYBERSAFETY EDUCATIONAL INITIATIVES IN SOUTH AFRICA

The previous section (4.3) investigated cybersafety initiatives in Africa (excluding South Africa). There was a clear indication that Africa is still in the process of identifying a need for and subsequently developing and delivering cybersafety

education. This section investigates cybersafety educational endeavours in South Africa.

The same content analysis and data collection process that was utilised and presented in Section 4.2 and 4.3, also applies in this section.

It has been identified that South Africa does not have any formal cybersafety education in place and that cybersafety is not currently incorporated into their school curriculum (Von Solms & Fischer, 2017). As a result, many primary school learners lack the skills and knowledge needed in cybersafety. Kritzinger (2017a) noted that the lack of cybersafety education in school has left doors open for many cyber-attacks on school learners. In addition to this, it was documented that teachers in schools are not trained about cybersafety and some of them do not know how to use ICT devices correctly. As a result, they are ill-equipped to assist school learners in this regard. Several other factors that have been associated in negatively affecting cybersafety education in South Africa include: access to technical infrastructure, geographical location and a language barrier (Kritzinger, 2015).The language barrier is one of the main aspects that hinders and exacerbates the gap concerning cybersafety in most developing countries. South Africa has 11 official languages and it has presented an opportunity to its foundation phase learners (7 to 9 years) to be educated in their own languages (Kritzinger, 2017a). However, as indicated with global studies, the majority of cybersafety education is presented and delivered to learners in the English language.

Table 4.3 highlights cybersafety educational initiatives in South Africa. This table was again derived by using the same thematic questions from Section 3.2.1 and the table headings are the same as those utilised in Sections 4.2 and 4.3.

Table 4.3: Summary of Findings for Cybersafety Educational Initiatives in South Africa

Initiative	Goal	Overseers	Target audience	Role players	Delivery method	Resources	Access method	Context
Kritzinger & Padayachee, 2007	To survey how life skills learning outcomes can be extended to the safe use of ICT.	Researchers (University of South Africa)	Applicable to everyone	School learners, government, parents, guardians, internet service providers and teachers	Educational framework (in Life Orientation)	Framework	Offline	English SA
Kritzinger & Padayachee, 2013	To provide an overview of a possible framework to engender an e-safety culture among all relevant role players and the application thereof.	Researchers (University of South Africa)	Primary school learners (age group not specified)	Primary school learners, teachers, parents, guardians and government	Educational curriculum Life Orientation	Framework	Offline	English SA
Kritzinger, 2011	To deliver cybersafety awareness throughout South Africa to all groupings of the population.	Researchers (University of South Africa)	Primary school learners (age group not specified)	Schools, learners, parents and teachers	Educational curriculum	Class activity and Homework activity	Offline	English SA

Kritzinger, 2015	To propose a framework that can be used to design offline cyber safety games to grow a cybersafety culture among school children in South Africa.	Researchers (University of South Africa)	Pre-primary, primary, or secondary school category (5 to 19 years old)	Government, learners, parents and teachers	Framework for offline cyber safety game development	Offline cyber safety game	Offline	Translated into many Languages SA
Kritzinger, 2017a	To identify children (school learners); readiness in becoming ICT users; and the gaps regarding cybersafety awareness and education.	Researchers (University of South Africa)	Children (school learners) (age not specified)	School learners, parents/guardians; teachers/caregivers, government; including the Department of Education; industry and educational systems (schools)	Educational curriculum (Life Orientation)	Cyber-culture approach	Offline	English SA
Kritzinger, 2017b	To identify children (school learners); their readiness to become ICT users; and the gaps regarding cybersafety awareness and education.	Researchers (University of South Africa	School learners (7 to 13 years old)	Teachers, learners, parents, external role players, and school governing bodies	Educational curriculum	Board games and online games.	Offline/ Bandwidth	Translated into different languages SA
Von Solms and Von Solms, 2014	To empower primary school teachers,	Researchers (Nelson Mandela	Primary school learners (7 to 13 years old)	Government, law enforcement, parents/guardians,	Educational curriculum	Online videos	Bandwidth	English SA

	specifically in Africa, to impart the basic principles of cyber safety to their learners.	University and University of Johannesburg)		schools, teachers and peers				
Von Solms and Von Solms, 2015	To introduce a curriculum for teaching cybersafety in junior or primary school.	Researchers (Nelson Mandela University and University of Johannesburg)	Primary school learners (7 to 13 years old)	Teachers and primary school learners	Education curriculum	Online videos	Bandwidth	English SA
Reid and Van Niekerk, 2014	To introduce a novel approach for educating the youth about information security.	Researchers (Nelson Mandela University)	Ages (7 years old and above)	School learners	Board Game	Game (Snakes and Ladders)	Offline	English SA
Reid and Van Niekerk, 2013	To create a case study of a cybersafety awareness campaign conducted amongst school children in the Nelson Mandela Metropolis.	Researchers (Nelson Mandela University)	Primary school and secondary school (7 to 19 years old)	Primary School learners, secondary School learners and teachers	Educational Poster	Posters and Videos	Offline	English SA
De Lange and Von Solms, 2012	To propose a framework that might contribute	Researchers (Nelson	Primary and secondary schools (7 to 19 years old)	Schools, teachers, parents and learners	Educational curriculum	Framework	Offline	English SA

	towards the development of an e-Safety culture.	Mandela University)						
DBE, 2010	To equip role players with guidelines around the ability to recognise potential dangers and be discerning enough to avoid them.	Government	Teachers, learners and parents/guardians	Teachers, learners and parents/guardians	Guidelines	Guidelines	Offline	English SA
Von Solms & Fischer, 2017	Promoting Digital awareness Among children	Researchers (Nelson Mandela University)	Children (no age stipulated)	DBE, Learners and Teachers	Book	Short messages, Poems	Offline	English SA

As presented in Table 4.3, South Africa has set goals for numerous cybersafety initiatives. However, there is a clear indication that the South African government and the private sector have had minimal involvement in these cybersafety educational initiatives. Research departments from various universities like Unisa, the University of Johannesburg and the Nelson Mandela University in South Africa have taken the leading role in the development and implementation of cybersafety initiatives. As several of the initiatives had a wide target audience, i.e. the whole community or both primary and secondary school aged learners, it was not always possible to separate the data into the specific target audience that this research was concerned with, namely primary school children aged between 10 and 12 years of ages.

Table 4.3 shows that some of the initiatives did not include all necessary role players such as the government, the governing body and principals. Table 4.3 also serves to highlight that in every single initiative there is only one identified delivery method which can reduce their effectiveness, as we have seen from previous research that the best approach to learning is a holistic approach. This research has indicated that South Africa has failed to consider the issue of language as a barrier to learning and geographical location as having significance. This can be ascertained from the findings in that most of the initiatives use the English language and are delivered using online methods.

4.4.1. Cybersafety Threats for Primary School Learners in South Africa

This section provides a graphical representation of cybersafety threats and related risks (as topics) for primary school learners. A comprehensive list of these cybersafety threats are presented in Appendix C.

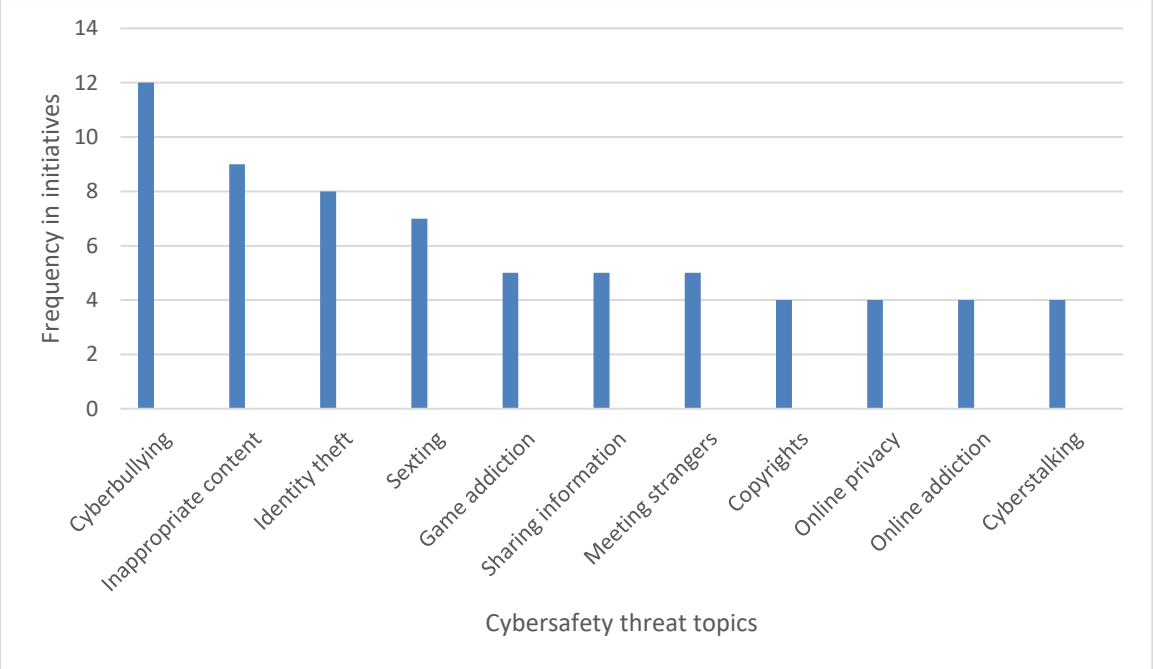


Figure 4.2: Cybersafety Threat Topics in South African Initiatives

Figure 4.2 shows the cybersafety threat topics which are common in South African cybersafety initiatives. As depicted, there is a clear indication that the most common cybersafety threat topics covered are as follows; cyberbullying, inappropriate content, identity theft, sexting, with game addiction, sharing information, meeting strangers, copyrights, online privacy, online addiction and cyberstalking are moderately covered topics. Again, it can be surmised that a key factor in determining the topics that are covered is the age of the children that the initiatives are aimed at, i.e. bullying is a long highlighted in primary schools and so it would be prudent to extend anti-bullying campaigns to cyberspace.

Sexting and information sharing are often seen by older primary school children to be a form of teasing/childish banter. Both topics were covered by many initiatives and it can be deduced that this is to ensure that children understand the implications that such actions have and the legalities surrounding what they may deem as innocent pranks. Whilst identity theft is usually associated with credit card/banking fraud (and considered an adult issue), its prevalence in modern society may provide an explanation as to why the topic is covered in so many initiatives for primary school children; *forewarned is forearmed*. This also includes topics like sexting and copyright,

which have not been covered in this study as they are not age appropriate for the target audience of this study.

4.5. DISCUSSION OF FINDINGS

The previous sections, Section 4.3 and Section 4.4, presented a qualitative content analysis of cybersafety educational initiatives for the UK, USA, Canada, Australia, New Zealand (NZ), Mozambique, Rwanda, Maurituis and South Africa. Based on the analysis, this section provides a discussion of the findings and conclusions through a comparative analysis. The layout of the discussion is according to the thematic questions that were posed in this analysis, as listed below:

- What are the goals of the initiatives?
- Who are the overseers of the initiatives?
- Who are the role players?
- What is the target audience?
- What is the context of the initiatives?
- What are the resources being used?
- What are the topics covered?
- What are the delivery methods?

4.5.1. Goals of Cybersafety Educational Initiatives

As presented in Table 4.1, in the UK the goal for cybersafety initiatives is to protect children so that they stay safe online and offline. In the USA, the goal is to protect children and young people. Canada's main goal is also to protect children whilst they are online, whereas in Australia the goal is to help Australia have safe, positive experiences online and in NZ the goal is to educate the community on the risks of cybercrime. Having investigated Australia and NZ, it is evident that they have different goals from the UK, USA and Canada. Whilst in the UK, USA and Canada cybersafety initiatives directly address children, Australia and NZ are more aligned to address the community at large.

As presented in Table 4.2, in Rwanda the goal of their cybersafety educational initiative was to educate primary school learners on exposing their information online and threats in cyberspace, whilst Mauritius also focused more on the community at

large. In Mozambique the gaol is to address both primary and secondary school learners.

As presented in Table 4.3, researchers in South Africa have set goals in their cybersafety educational initiatives. Some of these goals include: the delivery of cybersafety awareness throughout South Africa, empowering teachers to educate learners on cybersafety education, proposing frameworks that can assist design of in the offline cybersafety games, proposing a framework to contribute towards the development of an e-safety culture, and using open resources as a cybersafety curriculum. The common goal in these initiatives is to protect children, whether it be in directly educating them, or indirectly through educating the adults involved in their lives, for example, parent/guardians and teachers, for them to impart their knowledge to the children.

As with any concept, having a clear goal can be regarded as an important aspect in its success. Goals serve to identify what the initiative seeks to achieve and enable the measurement of the effectiveness of each initiative.

4.5.2. Overseers of Initiatives

As indicated in Table 4.1, developed countries' cybersafety educational initiatives have been delegated by governments, industry, non-governmental organisations, as shown in Table 4.4.

Table 4.4: Cybersafety Educational Initiatives and Overseers

Initiatives	**Overseers**
ThinkuKnow (UK)	NCA-CEOP
Safer internet centre (UK)	Childnet international
UKCCIS (UK)	UK government
Cybersafety K-12 (USA)	Government
Internet safety for kids (Canada)	Canadian centre Child protection
e-safety (Australia)	Australian government
Netsafe (New Zealand)	Industry and government
Stop.Think.Connect	Government/Industry

As presented in Table 4.4, there is clear evidence that the government for some developed countries, like UK, USA and NZ, work together with the private sector in designing and implementing cybersafety initiatives. On the other hand, Australia is led by the government and Canada by non-governmental organisations.

As indicated in Table 4.2, Africa (excluding South Africa) has followed the same principle. In Rwanda the private sectors are involved in delegating cybersafety education while nothing has been done by the government as plans are still progressing. In Mauritius, it is both the private and government sectors which are involved in cybersafety education. Whereas in Mozambique the research departments have taken the initiative to try and address cybersafety education.

However, in South Africa, as presented in Table 4.3, various research departments from different universities in South Africa have acquired most of the responsibility in designing and implementing cybersafety education of primary school learners in South Africa. There is clear evidence that there is less involvement from the government of South Africa and the private sector and little collaboration in promoting and executing cybersafety education. The UK, USA and NZ have shown that collaboration between government and private sectors is possible. Having more than one agency involved in an initiative can be beneficial as it not only combines experience and knowledge from more than one area, but it also assists in promoting accountability, as one partner will be held accountable for their actions etc. by the other/s involved. With many initiatives in Africa, including South Africa, being led by a single organisation, these benefits are not being realised.

4.5.3. The Role Players

According to Kortjan (2013) cybersafety education is a shared responsibility and everyone enjoying the cyberspace has a role to play. This means that role players such as the government, the researchers, school principals, governing bodies, the private sector, teachers, the parents and the learners all have a role to play in cybersafety education. In developed countries, the government has taken a leading role in resourcing cybersafety education. In addition, industries have partnered with the government in implementing cybersafety education, thus indicating a sense of shared responsibility. In Mauritius, government has partnered with the industries,

whilst Rwanda is industry led and thus it doesn't show any collaboration with the government. In Mozambique it is the research department leading the initiatives, also they are no evidence of the government being involved. The research data however reflects that in South Africa, both the government and industry have been involved to a lesser extent. It is the field of research that is leading the way in developing and implementing cybersafety in primary schools. More so, some of the initiatives suggested in South Africa are not clear in this matter of role players in cybersafety. Moreover, as highlighted in Chapter 1 (Section 1.3), the Department of Education is not yet clear with regards to their contribution as role players in this regard. Governing bodies and school principals were also demonstrated to be unclear in their position as key role players.

Therefore, when implementing cybersafety education, role players should be identified, and their relevant responsibilities should be defined. Additionally, partnerships with relevant stakeholders should be considered as beneficial as well.

4.5.4. The Target Audience

It is important that every initiative of cybersafety education focuses on specific groupings of the society. These groupings may include; businesses, school learners, teachers and parents. For this study, the target audiences were primary school learners and Tables 4.1, 4.2 and 4.3 presented cybersafety education in these groupings for the analysed countries. Developed countries have done well in grouping their target audiences. Mauritius just says 'children' and therefore it is also not specific in its target audience and Rwanda have tried the same in specifying target audience. Mozambique has combined both primary and secondary school learners, yet they are affected differently. Several South African initiatives (as per Table 4.3) have shown a clear indication that they are aimed at primary school learners and/or high school learners. It is important to focus on these groupings separately as they are targeted with different cybersafety threats and the best delivery methods also vary, mainly in accordance to the difference in age of the children involved.

4.5.5. Context for Cybersafety Educational Initiatives

When addressing cybersafety education, it is of paramount importance to consider the following: language, infrastructure, geographical location and age appropriateness.

The environment in which cyberspace is being utilised additionally impacts considerations for cybersafety education, and this may differ depending on the target audience. Using an example of school learners and businesses; school learners can be contacted at school whereas businesses can be contacted at their work premises and increasingly outside of the traditional business premises – with the introduction of intra-nets and employees being issued smart phones for business purposes. Consideration should be paid to the different types of school environment. For example, in South Africa there are Model C schools, public schools and private schools. The environment in which these schools are run and governed varies vastly from the way in which education that is taught to the physical infrastructure that is in place.

In Table 4.1, it can be seen that the majority of the initiatives have been communicated via bandwidth and are all in English; English being the main official language in each of the countries. This clearly shows that developed countries have taken into consideration the context in which they are addressing cybersafety. However, in Africa and South Africa, this has proven to be a problematic issue. Most initiatives have been designed, developed and communicated in English, yet South Africa has many languages (11 that are officially recognised). Therefore, understanding the language of the initiatives can be seen as a barrier to learning for school learners. Moreover, the issue of infrastructure has been of concern in South Africa, with many schools being under resourced when it comes to ICT infrastructure; as indicated in Chapter 1 (Section 1.3). However, in the attempt to tackle this, some initiatives have been borrowed from other developed countries. Therefore, context should be a serious consideration when developing cybersafety education as it should influence the method and/or tools to be utilised by the initiative.

4.5.6. Resources for Cybersafety Educational Initiatives

Most developed countries have created their own materials for use with cybersafety education. These materials come in a variety of forms and range from using games, poems, discussions, posters, books, videos, activity cards, frameworks and pledges. However, some of the materials that are available can be accessed on YouTube, for example Hectors' world. In Mauritius and Rwanda, material is being constructed by ways of PowerPoint presentations and a blog (respectively); however, these initiatives

are still in their early stages of development. In Mozambique research departments has suggested that media like posters, leaflets, books, newspaper articles, workshops and videos should be updated cover cybersafety topic. Also, the model indicates International Cooperation. In South Africa, researchers have developed their own materials to address cybersafety education, although some initiatives have been found to borrow material from developed countries, for example the school curriculum suggested by Von Solms and Von Solms (2015). It is important to consider where the material is coming from before making use of it, as this may affect the target audiences. A curriculum must be approved for the age group that it's directed at and the incorporated topics must be both age and culturally appropriate.

4.5.7. Topics to be Covered

Figure 4.1 presented the topics in cybersafety that are identified as relevant to primary school learners for developed countries. Figure 4.2 presented the same information with regards to South Africa. Examples of common cybersafety threats for primary school learners in developed countries and South Africa are cyberbullying, sharing information, and sexting. Whilst other topics such as password protection, online privacy, meeting strangers online, online grooming were categorised as different topics between developed countries and South Africa, they can be seen to have the same general theme.

It has been evidenced that some of the initiatives within South Africa have presented the same topics for different target audiences. For example, the DBE of South Africa developed guidelines to implement cybersafety education but did not specify the target audience for the suggested topics. An e-Safety Educational Framework in South Africa was suggested by De Lange (2012) for primary school learners and secondary school learners. However, research has identified that these two target audiences are affected by different cybersafety threats to one another. Thus, before implementing cybersafety, it is important to first identify who the target audience is and then utilise topics that are appropriate for that audience. It cannot be a '*one size fits all'* approach.

Several of the aforementioned topics were discussed in detail as cybersafety threats in Chapter 3 Section 3.7. Each of these topics is associated with learning outcomes that school learners are supposed to master at the end of each lesson. Some of the

following learning outcomes, listed in Table 4.5, were adopted from a private curriculum created by Von Solms and Von Solms (2015).

Table 4.5: Learning Outcomes for Cybersafety Topics

Cybersafety Topics	Learning Outcomes
Cyberbullying	• Learners will know how to respond appropriately to cyberbullying.
Inappropriate content	• Learners will know the risks associated with viewing and sharing inappropriate content.
Sharing information	• Learners will understand and be able to implement measures to protect their personal details online.
Meeting strangers online	• Learners will be able to identify and understand the potentially negative consequences/dangers of meeting strangers online and know how to react if someone requests them to do so.
Online privacy	• Learners will be aware of the importance of privacy settings and how to activate them.
Online grooming	• Learners will be able to identify online grooming techniques that are utilised by predators and be able to respond appropriately, e.g. stop conversing with the predator and inform a responsible adult.
Protecting of passwords	• Learners will understand and be able to utilise effective password protection techniques.
Game addiction	• Learners will be able to recognise the signs and symptoms of gaming addiction, be aware of how to avoid becoming addicted and know where to seek help if they are suffering from game addiction.

Table 4.5 depicts the learning outcomes that primary school learners are supposed to master at the end of each lesson.

4.5.8. Delivery Methods

Cybersafety education can be communicated using different media. However, one should take target audiences into consideration when dealing with this aspect. For example, to communicate cybersafety education to primary school learners is different from communicating it to high school learners. As presented in Table 4.1, there are

different forms of media that can be considered to communicate information to primary school learners, including games, videos, books, education curriculums and frameworks. It is also noted that more than one medium has been taken into consideration to implement cybersafety educational initiatives in developed countries.

With regards to research into cybersafety education delivery in Africa, Mauritius and Rwanda were both shown to be one dimensional in that they communicated cybersafety education using only one medium. Whereas in Mozambique the model has tried to adopt different delivery methods. The same applies in South Africa, and whilst there are a variety of mediums used, which include games, videos, posters, pledges, books, frameworks and guidelines, only four initiatives have used more than one medium; most were one dimensional in their delivery. In order to be most effective, it is recommended that initiatives incorporate more than one medium as means of delivery.

4.6. CHALLENGES RELATING TO CYBERSAFETY EDUCATION IN SOUTH AFRICA

South Africa has taken relevant action in trying to address cybersafety awareness and education, although there is no formalised cybersafety education curriculum in place (Von Solms & Fischer, 2017). The South African government has been involved with minimum effort in addressing the issue of cybersafety education. As stated in Chapter 1, the national cybersecurity strategy has not been clear in how to implement cybersafety awareness and education. However, universities around South Africa have developed multiple online cybersafety education and learning materials (Von Solms & Fischer, 2017). From Table 4.3 it is evident that frameworks, games, posters, books, and information sharing sessions have been suggested as solutions to try and address cybersafety education in South Africa. However, this study has identified the following as gaps that South Africa still needs to address and most of these gaps have been mentioned in Chapter 1 (Section 1.3) as reasons why cybersafety education is still a challenge in South Africa and these include:

- The South African government not being able to implement a formal cybersafety education curriculum.

- Most cybersafety material is accessed online and this has been a challenge to most schools as there is a need of finances to address infrastructure and delivery methods.
- The issue of language barrier and geographical location. Moreover, the issue of infrastructure has been of concern in South Africa, with many schools being under resourced when it comes to ICT infrastructure as indicated in Chapter 1 (Section 1.3).
- More so, some of the initiatives suggested in South Africa are not clear in this matter of role players in cybersafety. As highlighted in Chapter 1 (Section 1.3), the Department of Education is not yet clear with regards to their contribution as role players in this regard. Governing bodies and school principals were also highlighted as being unclear in their position as key role players.
- Several South African initiatives (as per Table 4.3) have shown a clear indication that they are aimed at primary school learners and/or high school learners. It is important to focus on these groupings separately, as they are targeted with different cybersafety threats and the best delivery methods also vary, mainly in accordance to the difference in age of the children involved.
- The Department of Basic Education of South Africa developed guidelines to implement cybersafety education but did not specify the target audience for the suggested topics

In conclusion, having identified these as challenges that South Africa is currently facing, this study suggests that important considerations have to be put in place when developing and delivering cybersafety initiatives within the primary school environment. These include: the target audience – their age and their cultural background; the environment in which their schooling takes place; collaboration of the key role players involved in the delivery of the initiative; and the language and methods utilised for the delivery.

4.7. ADDRESSING CYBERSAFETY EDUCATION IN SOUTH AFRICA

The previous section (4.5) presented a discussion of the findings from a comparative analysis. Based on these findings and subsequent conclusions, this section presents the key components required to overcome the challenges that have been identified in addressing the cybersafety education of primary school learners in South Africa. The

layout of these suggestions is in accordance with the thematic questions that were posed for this analysis in Chapter 2, Section 2.4.

4.7.1. Goals of Cybersafety Education in South Africa

Firstly, it is important that in every initiative a goal must be set in order to provide clear objectives and subsequently measure the effectiveness of the initiative. Therefore, specific goals must be clear and in place from the outset.

4.7.2. Overseers of Cybersafety Educational Initiatives in South Africa

Secondly, it has been identified that there is less support from the South African government and the private sector regarding cybersafety education. Therefore, at present, the research departments from various universities have been at the forefront with regards to this matter. These are the ones delegating the initiatives. It is important to have overseers in cybersafety initiatives, and it is most effective when the government partners with other departments, for example the private sector and industry in order to achieve their cybersafety goals. It is the overseers who are responsible of setting the goals.

4.7.3. The Role Players in South Africa

As mentioned in Chapter 1, teachers and schools have not been able to implement cybersafety education on their own. Table 4.3 clearly indicates that, in South Africa, it is researchers at universities who are mostly responsible for implementing cybersafety education. To address this challenge, this study strongly recommends that every initiative must be accompanied with appropriate training and supporting guidelines to help schools and teachers on how to deliver cybersafety education to primary school learners. Also, learners must be provided with supporting material, in their home language, that is both multi-dimensional and age appropriate, in order to assist in their understanding of cybersafety education. It is important to firstly identify who the role players in the initiative are and to address them accordingly. It therefore means that role players such as the government, the researchers, the principals, governing bodies, the private sector, the teachers, the parents and the learners all have different, but inter-connected roles to play in cybersafety education.

An example of this is as follows: the government can form partnerships with private sectors in implementing cybersafety education. The role of the private sector together

with the government is to provide funding to implement cybersafety initiatives. The governing body and the principals, according to De Lange and Von Solms (2012) are responsible for the implementation of school policies and rules. In addition, they provide the environment in which cybersafety education and the school curriculum are implemented. The government of South Africa, meaning the DBE, is responsible for the school curriculum and to a lesser extent also responsible for cybersafety education. The teachers and the parents' roles are to assist learners in acquiring the skill and knowledge on how to operate in cyberspace. Teachers, learners and parents can also be learners, advisors and educators. However, as mentioned in Chapter 1, parents and teachers in South Africa need to first acquire the relevant skills and knowledge concerning cyberspace.

4.7.4. Context of Cybersafety Educational Initiatives in South Africa

The issue of addressing context has been of concern in South Africa and therefore this study focused on language barrier, geographical location, lack of finances and infrastructure. It is clear in Table 4.3 that some of the initiatives in South Africa have not been considering this component as a matter of urgency. Most initiatives have been implemented in English, yet South Africa has many languages, and only a few of the initiatives can be translated. Moreover, the issue of infrastructure has been of concern in South Africa, mainly due to financial constraints. To address this challenge, this study strongly suggests that when implementing cybersafety education, it is important to consider the context in the initial planning stages. Translated initiatives and printed material must be considered when implementing cybersafety education.

Furthermore, addressing the context helps the target audience to receive the message for cybersafety education as effectively as possible. Some of the cybersafety initiatives in South Africa have incorporated materials from developed countries. However, the issue of deciphering foreign accents in these cases has been of concern amongst primary school learners in South Africa (Von Solms & Fischer, 2017). To address this concern, this study recommends that, as an example, games can be played offline by using skills and concepts implemented in real life (Fisch, 2005). Games can contain animals as characters that can be recognised by African children (Von Solms & Fischer, 2017). Moreover, themes like; *'do not talk to strangers'* or *'looking both ways when you cross the street'* can be used for cybersafety education. According to Miles

(2011) and Von Solms and Von Solms (2015) children are taught these concepts to stay safe in the real world, and so they must be applied online as well. Therefore, having these types of concepts will serve to help children to understand cybersafety education in an effective way as they are relating to concepts they already know in real life.

4.7.5. Resources for Cybersafety Educational Initiatives in South Africa

Due to the lack of a formalised school curriculum to educate school learners to stay safe online, multiple websites and learning material on cybersafety have been made available by universities, research institutions, private and public organisations to keep children safe online (Google, 2017; South African Cyber Security Academic Alliance, 2015; Unisa ,2017; University of Pretoria, 2017). Many of these activities are accessed online while a few can be accessed offline. This has been a barrier to most learners as many schools lack ICT infrastructure (Jossel, 2016; Kritzinger, 2016). According to the Centre for Justice and Crime Prevention (CJCP) and the United Nations Children's Fund (UNICEF) (2012) and Kritzinger (2016) studies have indicated that initial awareness-raising phased campaigns must involve more than a website presence to create awareness and knowledge. Therefore, different forms of resources apart from websites must be available when addressing cybersafety education. These can include games, books, poems, videos and posters. More so, resources can be adopted and adapted from other initiatives, as long they are appropriate for the context and target audience.

This study strongly recommends that Life skills, as a subject in Curriculum Assessment Policy Statements (CAPS) or with existing cybersafety curriculums, can be utilised to improve the current status regarding cybersafety education for primary school learners in South Africa. According to Kritzinger and Padayachee (2013) risks cannot be identified only as technological, but may have a physiological, psychological and sociological influence on school learners, and hence it would be wise to teach these learners cybersafety as part of a programme that includes, health, social, physical and personal development issues. Life Skills as a subject, deals with complete development of the learner throughout childhood (Kritzinger & Padayachee, 2013); thus it would serve to provide an appropriate platform in assisting school learners to have a better understanding of cybersafety education.

4.7.6. Topics to be Covered in South Africa

As highlighted in Section 4.7.4, some of the initiatives have not been isolating target audiences, resulting in topics being the same regardless of the target audience. Yet different target audiences are affected by different cybersafety threats online. It is important to identify the cybersafety threats and related risks that are applicable for each age group before implementing the initiative; as they can be affected differently. In this study, cybersafety threats and related risks were identified and presented in Chapter 3 (Section 3.7 and Section 4.5.7) together with their learning outcomes in Section 4.5.7 and these are used as topics in Chapter 5 towards the proposed framework.

4.7.7. Delivery Methods in South Africa

As was evidenced in Table 4.1, there is a clear indication that developed countries have made use of combined delivery methods in each initiative. These delivery methods include videos, stories, films, eBooks, frameworks, curriculums, PowerPoint slides, presentations and games. However, in South Africa, as per Table 4.3, most initiatives have focused on one delivery method in every initiative to try and address cybersafety education and these include: frameworks, books, games, poems, flyers, posters, guidelines and online videos. Therefore, this study recommends that, to improve cybersafety education in South Africa, initiatives must be multi-faceted and employ more than one delivery method. Mahlangu (2019) suggested that a combination of delivery methods can be used to form a strategy. The aim is to exploit the strengths of the delivery methods while attempting to minimise the effect of their weaknesses.

Games can be used as a short-term method to address cybersafety education, meanwhile allowing the government to implement a suitable long-term approach (i.e. inclusion in the curriculum). Reid and Van Niekerk (2014) supported the idea of games by indicating that school learners prefer games as a learning tool. In addition, Giannakas, Kambourakis, and Gritzalis (2015) indicated that games can be formal and informal and that they can support outdoor activities in addition to traditional classroom methods. A large variety of games can be printed offline and translated into many different languages (Kritzinger, 2015). Games can be played offline by using skills and concepts implemented in real life (Fisch, 2005). Games can contain animals as

characters that can be recognised by African children (Von Solms & Fischer , 2017). Thus, this study strongly recommends that cybersafety education for primary school learners in South Africa can be improved through gaming, in order to address the highlighted issues such as financial constraints, language barriers and infrastructure.

According to Miles (2011) and Von Solms and Von Solms (2015) school learners are taught concepts to stay safe in the real world, and so they must be taught how to apply them online as well. Acknowledging the connection between the cyber world and the real world will assist in the understanding of cybersafety amongst primary school learners.

Life Skills as a subject has been identified as a platform that can be developed to deliver cybersafety education. As discussed in Section 4.7.5, Life Skills is concerned with the complete development of the learner throughout their childhood. Therefore, learners are equipped with real Life Skills at an earlier stage. The same is needed with regards to cybersafety education in that learners need to be equipped with knowledge and skills on how to navigate safely in cyberspace from an early age.

Therefore, to address the challenges that South Africa is currently facing, all arguments formulated above were compiled and applied towards the solution to this study. They fell under the defined components, as identified from the thematic questions, to form the basis of the proposed framework for cybersafety education of primary school learners in South Africa (which was the primary objective of this study). These components were drawn from the conclusion and deductions. In light of the following constraints that were identified in Section 4.7.4 – lack of funding, infrastructure shortages, language barriers and geographical location and teacher/parent lack of based knowledge – this study considered a component constraint rather than context. Hence, the components of the framework were identified as follows:

- Role players
- Constraints
- Resources
- Life skills
- Topics
- Learning outcomes

- Delivery methods.

4.8. CONCLUSION

Since school is compulsory in most countries and primary school is an entry point, most developed countries have found it easier to educate school learners about cybersafety at this point (Bada, 2017). Therefore, it should be a priority for the South African government to provide resources to schools so that they can afford the necessary education to equip school learners on how to act safely whilst online. This can be achieved through cybersafety education being introduced in schools as early as primary school level. The purpose of this chapter was to investigate cybersafety education globally as well as to do a comparative analysis to identify challenges currently facing South Africa regarding cybersafety education and subsequently to suggest possible solutions to these identified challenges. An investigation was first conducted for both developed and developing countries and key components were deduced. The basis on which the proposed cybersafety educational framework could be developed was established. The following chapter (Chapter 5) presents the details of the framework.

CHAPTER 5
THE PROPOSED FRAMEWORK

5.1. INTRODUCTION

Chapter 1 focused on the background of this study, where the problem area was identified as “many primary school teachers in South Africa are ill-equipped to implement cybersafety initiatives, thus leading to learners that are vulnerable to cyber-related threats”.

Based on the literature reviewed, there is clear evidence that ICT plays a vital role in today’s world. Kortjan and Von Solms (2014) claimed that it has redefined the way in which school learners communicate, gain access to and share information and entertain themselves. Section 1.2, however, revealed that school learners are a subgroup of society who particularly need cybersafety education. Cyberspace is a complex environment, since it is extremely difficult to enforce rules of law within it. Thus, children must be taught how to protect themselves from the threats associated with cyberspace.

However, to date, cultivating a cybersafe culture in South Africa has shown to be problematic. Several factors have been identified as contributing towards this, namely diversity in religion, culture, language, economic dispensation, knowledge and access to technology, the absence of centralised e-learning policies and resources, as well as the lack of a formal cybersafety education curriculum in place. The South African government, through the DBE (2010) has created guidelines to implement cybersafety education in schools. However, according to De Lange (2012) these guidelines alone are not enough to implement cybersafety education in schools. Moreover, teachers are presently unable to assist as they lack the relevant skills and knowledge to do so.

The aim of this chapter is therefore to present a proposed framework that will assist teachers in addressing cybersafety education for primary school learners in South Africa.

According to Tomhave (2005), a framework is “a fundamental construct that defines assumptions, concepts, values, and practices and that includes guidance for implementing itself”. It is further linked to demonstrable work. To develop a framework

for cybersafety education for primary school learners in South Africa, a comparative analysis, a literature review, argumentation and modelling were conducted.

There are three main types of schools within the South African mainstream education. These include: Public schools (which are fully dependant on the government for materials and funding), Model C schools (which receive government funding but are administered and largely subsidised by the Governing body), and Private schools (which are independent from and not owned by the government) (Richmond Magazine, 2019). For the purpose of this study, the framework was aligned with the context of Model C and Public Schools. However, it can be adopted in any context.

Section 5.2 discusses the three main types of schools in the South African Education system to provide the context for the proposed framework presented in Section 5.4, while Section 5.3 highlights the key elements of the proposed framework.

5.2. THE SOUTH AFRICAN EDUCATION SYSTEM

The South African education system has three main types of schools, namely private schools, public or government schools, and Model C schools.

5.2.1. Public Schools in South Africa

These are also known as government schools. They are fully dependant on the government for resources. Every province has a responsibility to ensure that its schools are equipped and have budgets for running costs and teachers' salaries. The school standards differ depending on the environment in which they are located and how they are being managed. Since it is the government's responsibility to fund the education system in public schools and the province's discretion to assign individual schools' budgets, the funding at these schools can be very low. The infrastructure, particularly in rural areas, is grossly underdeveloped (with over 4500 government schools still using pit toilets; and over 20 schools in the Eastern Cape being identified as having no sanitation facilities at all). Teachers in these schools are appointed by the DBE. They regularly have to teach with insufficient materials and equipment. It can be concluded that whilst not all schools, many schools in this subgroup provide fewer educational opportunities than Model C and private schools.

However, despite this chronic shortage in essential infrastructure, at the recent SONA (Presidency Republic of South Africa, 2019) president Ramaphosa pledged to provide

all school pupils with a tablet within the next six years. This demonstrated a recognition by the government that learners must have access to current ICT; subsequently also meaning that cybersafety frameworks, such as the one proposed by this study, will become an increasingly essential part of the school curriculum and learners' lives.

5.2.2. Model C Schools in South Africa

Model C schools receive funding from the government, whilst also receiving additional funding from the parent body. These are fee paying schools, with the fees varying from school to school; the fees are set by the parent body and bursaries are available on a sliding scale for those families who can prove that they receive little or no income. The top South African schools fall into this category. Due to the additional, parent-based funding, these schools have larger budgets than government schools. As Model C schools are based on what parents can afford, they are often seen to be equipped with the latest technologies and have outstanding extramural programmes for the learners to participate in. Many of these schools are English speaking schools. They do, however, very often become oversubscribed with learners (particularly in suburban areas) as families strive to get better standards of education for their children without being subjected to private school fees.

5.2.3. Private Schools in South Africa

These schools are known as independent schools and the government does not own or run these schools. They are owned either by the church, community, a for-profit company or operated by a trust. Private schools are funded by school fees and the parents' body. They typically have small class sizes of 15 children to one teacher and one assistant, which is many parents' preference. Schools like CURRO and Spark are examples of private schools. These schools are supported by private investors and have innovative business models. Such schools have access to the latest technologies and require tablets and data as part of their stationery list as online learning is commonplace within them.

Many private schools in South Africa follow the IEB (Independent Examinations Board) curricula, with others following the Cambridge International Examinations (CIE) curricula. This means that government-led initiatives and mandates are not necessarily incorporated into their learning outcomes. In spite of this, the proposed

framework for cybersafety education is still applicable to these schools as it emphasises collaboration between relevant parties, including the private sector. Furthermore, with the increased availability of and regular exposure to ICT at these schools, these learners have a heightened need for cybersafety awareness initiatives.

The following section discusses the key elements of the proposed framework.

5.3. KEY ELEMENTS OF THE PROPOSED FRAMEWORK

The framework in this section is discussed under the following structure: Key role players (Section 5.3.1); Key constraints (Section 5.3.2); Key resources (Section 5.3.3). The following sections dealing with the key delivery methods which encompass key topics, learning outcomes and delivery methods within the Life Skills curriculum.

5.3.1. Key Role Players

This section provides details of how various key role players were considered as part of the proposed framework. Some role players were identified as overseers; these are individuals who are responsible for delegating the initiatives and setting the initiative goals.

As depicted in Table 5.1, each key role player has been discussed in sections in the previous chapters.

Table 5.1: Key Role Players

Key role player	Sections
Government (Department of education)	Sections 1.3; 4.4.1 and 4.6.4
Private sector	Sections 1.3; 4.4.1 and 4.6.4
Researchers	Sections 1.3; 4.4.1 and 4.6.4
Governing body	Sections 1.3; 4.4.1 and 4.6.4
Principals	Sections 1.3; 4.4.1 and 4.6.4
Teachers	Sections 1.3; 1.4; 4.4.1 and 4.6.4
Parents	Sections 1.3; 4.4.1 and 4.6.4
Learners	Sections 1.3; 1.4; 4.4.1 and 4.6.4

The key role players (as depicted in Table 5.1 and Figure 5.1) are discussed below.

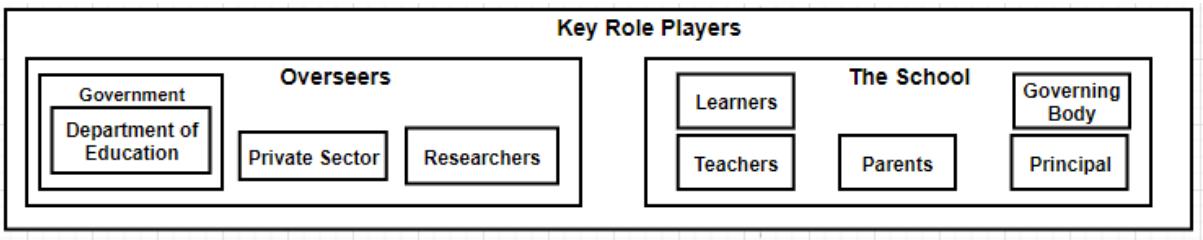


Figure 5.1: Key Role Players

To implement a cybersafety initiative, the roles of the key role players must be clearly defined. This study has identified the following key role players as vital in implementing a cybersafety initiative.

5.3.1.1. The Government

The South African government is considered to be one of the main overseers and role players to ensure that school learners are being educated about cybersafety and cyber use. According to Farrel (2014) it is the government who makes sure that school learners are protected against all possible cyber dangers, threats and exploitation. The DBE has attempted to address cybersafety education within South African schools and devised guidelines to implement cybersafety in the schools. The DBE is also responsible for devising, implementing and delivering public educational curricula.

Therefore, it is the DBE's duty to create cybersafety education material, policies and procedures to be utilised by schools (Badenhorst, 2011). As stated in Chapter 4 (Section 4.7.2), in this capacity the government (through the DBE) acts as overseers and their responsibility is to delegate tasks and oversee the whole implementation of cybersafety initiatives. Overseers are responsible for making sure that all constraints have been considered or catered for before the implementation of the cybersafety initiative. To promote cybersafety education in school, the government must consider the following (Kritzinger, 2017a):

- Include in national legislation cybersafety for school leaners.
- Include cybersafety awareness in the school curriculum, incorporating it into the current life skills programme.
- Provide access to dedicated teacher training programmes to improve cyber knowledge amongst teaching staff.
- Provide an action plan for the reporting and the handling of cybersafety incidents.
- Implement a monitoring process to ensure accountability and responsibility for actively pursuing a decrease in cyber incidents amongst school learners.
- Mandate schools to comply with and implement a national cybersafety policy.
- Ensure parents and SGBs and principals know what the government is mandated to do with regards to cybersafety education and know which channels to address for assistance with upholding these duties.

5.3.1.2. The Private Sector

The private sector (coupled with the government) is responsible for funding cybersafety initiatives. As previously revealed (in Chapter 1, Section 1.2), the private sector can have multi-faceted responsibilities. These may range from funding infrastructure within schools to helping drive cybersafety awareness campaigns to assist government with finances and resources. The private sector can form partnerships with the government to be overseers of initiatives. Below are some of the activities that the private sector can do to contribute towards cybersafety education

among school learners. It is working within these parameters that would assist in the proposed frameworks' success (Becta, 2009):

- Provide funding to create age and culturally specific cybersafety materials.
- Provide expertise to assist other role players with the necessary cyber knowledge and skills to grow a cyber-culture.
- Interact with schools to create and implement ICT/cyber policies and procedures.
- Assist with teacher and parent training to improve cybersafety knowledge, through materials, workshops and open days.

5.3.1.3. The Researchers

To date (as indicated in Chapter 4, Section 4.7.5), researchers have been found to have undertaken the majority of the groundwork in implementing cybersafety curriculum in South Africa. They have devised this curriculum after conducting extensive research studies into all aspects of cyber threats, cybersafety and cyber awareness amongst children. Chapter 1 (Section 1.2) revealed that currently no formal cybersafety education curriculum exists in South Africa. The framework in this study would encourage researchers to utilise their knowledge and expertise to work hand in hand with other role players, particularly the government, to act as overseers of cybersafety initiatives.

5.3.1.4. The School

The school includes the school principals and the school governing body. De Lange (2012) ascertained that it is the school that decides who the important role players are based on their own environment regarding cybersafety education. Role players such as governing bodies can collaborate with higher role players such as the DBE. Therefore, when implementing cybersafety education, schools must take legislation and regulations into consideration (De Lange, 2012). Moreover, schools are where cybersafety initiatives, as a part of the Life Skills curriculum, should be introduced (Kritzinger & Padayachee, 2013). Therefore, it is the governing body's duties to take the leadership in implementing cybersafety education. Below are some suggested duties that the governing body should undertake with regards to cybersafety (South West Grid for Learning Trust [SWGfL], 2010):

- Be responsible for the approval of the cybersafety school rules and policy;
- Regularly monitor cybersafety incident logs and filtering logs;
- Support the principal in developing cybersafety strategies;
- Ensure funds are available for the implementation of the various cybersafety initiatives;
- Promote cybersafety to parents; and
- Address policy breaches.

On the other hand, principals are responsible for taking care of the day-to-day activities of cybersafety activities within their schools. This means that all issues regarding cybersafety activities lie within the hands of the principals, though they work under the governing body wherever necessary. Below are some of the principals' responsibilities regarding cybersafety activities (SwGfL, 2010):

- Being responsible for the day-to-day cybersafety activities;
- Ensuring that the cybersafety school rules and policy are implemented;
- Taking full responsibility for cybersafety issues;
- Ensuring that the teachers receive the necessary support to carry out their cybersafety responsibilities;
- Supporting the teachers to cultivate a cybersafe culture amongst the children within the school;
- Ensuring that the governing body is informed and up to date with all cybersafety matters, especially the school rules and policy;
- Budgeting for cybersafety to be carried out;
- Promoting cybersafety across the curriculum;
- Addressing serious policy breaches.

The framework proposed in this study seeks to adopt the implementation of the aforementioned responsibilities in order to ensure that there is consistency across each of the three identified models of schools within South Africa.

5.3.1.5. The Teachers

Teachers can hold different roles and interchange between them as and when needed. These roles include: an advisor, a learner, an identifier and a teacher (De Lange, 2012). Teachers have been found (refer to Chapter 1, Section 1.2) to be lacking cybersafety skills to help school learners to be cybersafe. It is crucial that teachers fully understand cybersafety threats and the related risks themselves before they attempt to educate learners. As such, this framework recommends that teachers are exposed to learning materials and participate in courses to improve their subject knowledge base. This can be done through a combination of using available, existing resources (i.e. utilising initiatives that have proven good practice in SA and other countries), help from the government, the researchers and the private sector. In this instance, teachers can be regarded as learners since De Lange (2012) highlighted that teachers do not necessarily need to be experts in cybersafety, but they must be well informed. Cybersafety additionally requires teachers to monitor school learners when they are using ICT devices (Grey, 2019) and in return learners need to be secure in the knowledge that they can confide in and trust their teachers with any cyber-related issues that they encounter. Becta (2009) compiled a list of duties/responsibilities which teachers have with reference to cybersafety. These are in keeping with the ethos of this study's framework and are as follows:

- Contributing to the development of cybersafety policies and school rules;
- Adhering to teacher Acceptable Use Policy (AUP);
- Knowing when to escalate cybersafety issues to a higher level;
- Embedding cybersafety into the school curriculum where possible; and
- Maintaining a professional level of conduct in their personal use of ICT, both within and outside of school.

5.3.1.6. The Parents and Guardians

Chapter 1 (Section 1.2), identified parents as lacking the relevant skills and knowledge to assist school learners with cybersafety education. As with teachers, parents can also carry four distinct roles. They can be learners, identifiers, advisors, and teachers to children (De Lange, 2012). It is the parents' obligation to make sure that their children develop safe and responsible online behaviour. Therefore, when delivering

cybersafety education in schools, the school must ensure that parents are invited to be involved and that they are actively included in awareness campaigns (Becta, 2009).

There is a direct correspondence between parents' awareness of ICT and the boundaries that they put in place with regards to their children's use of ICT. Valcke, De Wever, Van Keer, and Schellens (2011) highlighted that an increase in parental awareness leads to an increase in rules. In addition to this, De Lange (2012) found that younger parents tend to have more ICT knowledge than their older counterparts and so were much stricter in setting rules and boundaries for their children's ICT usage. Parents should be educated in the early warning signs of their children having what can be deemed as an unhealthy or a problematic relationship with ICT. This can take many forms such as spending long hours on the Internet, disengagement from physical and social activities, reluctance to discuss their online activities, behaviour changes, changes in eating and sleeping patterns and turning off the monitor when the parent enters the room. Therefore, empowering parents with the skills and knowledge required to appropriately address these issues, if and when necessary, is an essential part of this framework. In return, they should display a commitment to and be willing and open to discuss cybersafety with their children. Listed below are the parents' responsibilities as classified by Becta (2009) which also align with the fundermentals of this study's proposed framework as they emphasise collaboration between the schools, the parent and the learner:

- Be able to contribute to the development of cybersafety policies and school rules;
- Use the resources the school recommends appropriately; and
- Discuss cybersafety issues with children and reinforce the approaches and behaviours the school is trying to enforce.

5.3.1.7. The Learners/Target audience

As role players, the learners have been acknowledged to be vulnerable to cyber-attacks and are therefore the focus of this study. These learners need to be prepared for cybersafety education. However, their needs must be identified according to their age groups, thus meaning that the school must adapt to their needs. As with teachers and parents, school learners can undertake the roles of a teacher and an advisor alongside that of a learner. School learners should encourage and support one

another to be safe online through peer-mentoring; thus, demonstrating an advisory role. School learners often have a greater knowledge of ICT than their parents or teachers. This can be attributed to increased generation exposure which often results in learners becoming quick identifiers of problems arising with their peers' ICT usage and their cybersafety. In the event of such occurrences, pupils should undertake the responsibility to act as advisors to their peers (in addition to disclosing their concerns to an appropriate adult). Listed below are some of the responsibilities for school learners regarding cybersafety which have been included in the proposed framework to increase its prospects of success (Becta, 2009):

- Contribute to the development of cybersafety school rules and cybersafety policies;
- Adhere to school policies and rules;
- Keep themselves and others safe online;
- Understand the significance of reporting cybersafety issues;
- Understand the significance of adopting good cybersafety practices; and
- Openly discuss cybersafety issues with parents/guardians/teachers.

The proposed framework acknowledges that role players are a vitally important component in the success of cybersafety education. Therefore, all identified role players must accept their identified roles and collaborate in order to deliver cybersafety education to primary school learners in South Africa.

5.3.2. Key Constraints

The definition of a constraint is "something that controls what you do by keeping you within particular limits" (Procter, 1995).

This section provides details of various key constraints, listed in Table 5.2, that were considered for the proposed framework.

Table 5.2: Key Constraints

Key constraint	Sections
Age appropriateness	Sections 3.7; 4.4.7; 4.5.7; 4.6.6 and 4.6.7
Geographical location	Sections 1.3; 4.4.7; 4.5.7; 4.6.6 and 4.6.7

Key constraint	Sections
Language barrier	Sections 1.3; 4.4.7; 4.5.7; 4.6.6 and 4.6.7
Funding	Sections 1.3; 4.4.7; 4.5.7; 4.6.6 and 4.6.7
Infrastructure	Sections 1.3; 4.4.7; 4.5.7; 4.6.6 and 4.6.7
Teachers/Parent cybersafety knowledge base.	Section 1.3 and 1.4

The key constraints were identified from reviewing current literature and studies from within South Africa, Africa as a whole and the developed world. Figure 5.2 depicts the key constraints that have been considered applicable when implementing a cybersafety initiative in South Africa.

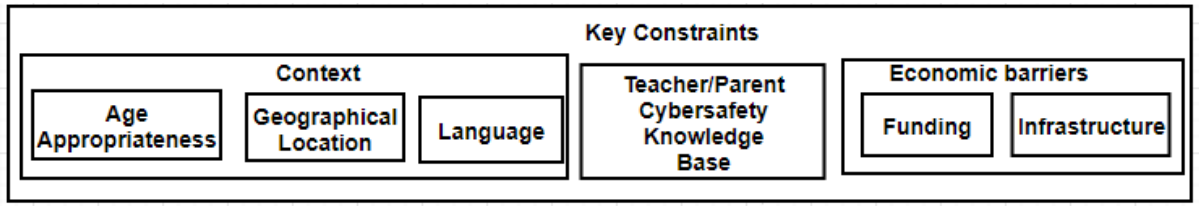


Figure 5.2: Key Constraints

The context of the framework is an umbrella term under which, age appropriateness (i.e. the target audience), geographical location (where the initiative is being delivered?) and identified language barriers (i.e. the language that it is being delivered in, is it in a home language of which there are 11 in South Africa?) fall under. Finances (i.e. funding), infrastructure and teacher/parent cybersafety knowledge base are also deemed to be key constraints. Therefore, when developing a cybersafety initiative it is critically important to factor in these constraints. In the initial stages, one must consider the budget for the cybersafety initiative, whether there are funds available and what measures can be taken to source funds, e.g. partnerships with the private sector, parent fundraising, government and/or research grants/initiatives.

Secondly, the infrastructure that the initiative requires must be identified. Does it need bandwidth or ICT resources? What space and input are required? Which role players need to be actively involved as overseers? This leads to the important role that parents and teachers play in delivering, identifying and advising learners about cybersafety.

As was identified earlier on, parents (Section 5.3.1.6) and teachers (Section 5.3.1.5) must be informed and knowledgeable about cybersafety in order to successfully promote and deliver cybersafety training. To date, there has been a large cybersafety knowledge gap in teachers and parents. Thus, to minimise this constraint, a clear path of training and development must be identified to address this cybersafety knowledge gap of parents and teachers.

Age, geographical location, and the language constraints are all influenced by the context in which the initiative is to be developed and they directly impact the delivery of the cybersafety initiative. It is crucial that the initiative is age appropriate in order to ensure that the learners not only understand the concepts being taught but also that these concepts are meaningful and have a relatable context to their life experiences. Geographical location holds a major key to the infrastructure and funding that is available, and to a large extent the existing knowledge that teachers/parents have. Rural areas have been found to have poor connectivity/available bandwidth and are more likely to be government schools with fewer resources, less collaboration with the private sector, and very limited cyber-based knowledge amongst older generations.

Model C schools, on the other hand, are more likely to be diverse in terms of languages utilised, particularly with the delivery of education largely being through the English medium, increased connectivity, higher level of exposure to ICT and more effective school collaborations with interested parties. Identifying the constraints assists one to know what delivery methods to consider. For example, in rural schools one would consider offline material such as printed materials or even offline games, to override the issue of infrastructure, and materials would need to be made available in-home languages to negate language barrier issues. A successful initiative is one that addresses its context; it cannot simply be a *'one size fits all'* (Von Solms & Fischer, 2017).

5.3.3. Key Resources

This section provides details of the key resources that were considered for the proposed framework as shown in Table 5.3

Table 5.3: Key Resources

Key resources	Sections
ThinkUKnow (UK)	Section 4.2.1
Netsafe (New Zealand)	Section 4.2.1
e-safety (Australia)	Section 4.2.1
Cybersafety for K-12 (USA)	Section 4.2.1
Stop.Think.Connect	Section 4.2.1
Cybersafety frameworks	Section 4.4.1
Cybersafety guidelines	Sections 1.3 and 4.4.1
Posters	Sections 1.3; 4.4.1 and 4.6.6
Board games	Sections 4.4.1 and 4.6.6
Online videos	Sections 4.4.1 and 4.6.6

As depicted in Table 5.3, these key resources have been discussed in various sections in the previous chapters.

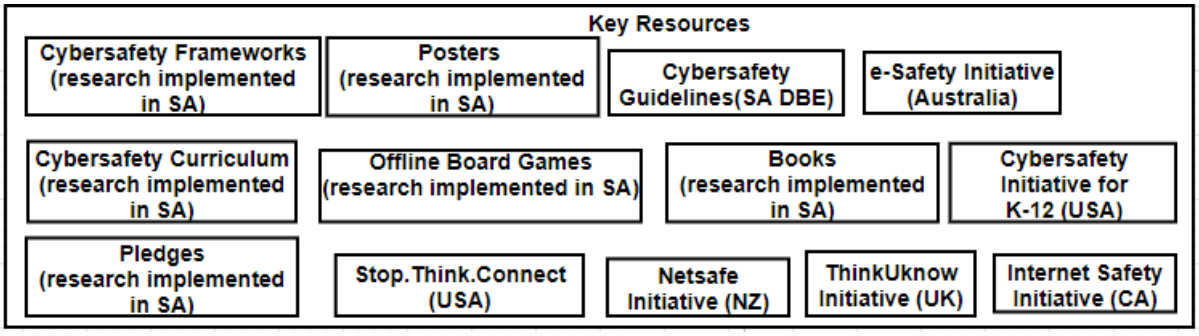


Figure 5.3: Key Resources

Figure 5.3 shows the key resources that are an integral part of the proposed framework for delivering cybersafety education. This study identified that several resources are available and relevant to developing and delivering cybersafety education in South Africa. These key resources have been made available in the form of guidelines (developed by the DBE), frameworks, books, private curricula for cybersafety (developed by researchers and the private sector) and initiatives taken from developed countries such as ThinkUKnow (UK) and Netsafe (NZ).

Chapter 1 (Section 1.2) and Chapter 4 (Section 4.7.2 and Section 4.7.3) found that whilst the government and researchers have devised both guidelines and a private curriculum (respectively) to address cybersafety education in South Africa, both have fallen short of providing a comprehensive solution. Issues such as the lack of funds, access to materials, knowledge of how to utilise ICT, and materials not being delivered in home languages have been acknowledged. Therefore, this proposed framework establishes that in order for resources to be effective, the role players responsible for the resources must firstly consider the constraints and how to overcome them.

Resources that are readily available have been incorporated into this proposed framework as they have been found to assist in implementing cybersafety educational interventions. These existing resources can also be adapted, prior to implementation, to suit the demographics of the school learners they are being delivered to, for example, the language they are communicated in, the infrastructure that they require, and the age group of the children being targeted. Even though the resources appear to be the final output, these can be used to produce new or improved interventions, for example, for developing relevant games and revising curricula. When using these resources, one must consider using effective delivery methods, as discussed in Life Skills curriculum.

5.3.4. Life Skills Curriculum

This section provides details on how Life Skills, as a current subject in the CAPS curriculum and previously discussed in Section 4.7.7, has been incorporated into the proposed framework.

As discussed in Chapter 4 (Section 4.7.7), Life Skills as a subject in the Curriculum Assessment Policy Statement (CAPS) has topics that can be related to cybersafety topics. These topics include physical bullying (which is addressed in Grade 4). The difference is in the environments in which they occur. Topics in cybersafety education include risks that can be identified as technological, but may have a physiological, psychological and sociological influence on school learners. Hence, it is advised to include cybersafety as part of a programme that incorporates learners' health, social, physical and personal wellbeing and development issues – and this is part of the Life Skills curriculum. Figure 5.4 illustrates the different aspects of the Life Skills curriculum and how cybersafety can be integrated into this curriculum.

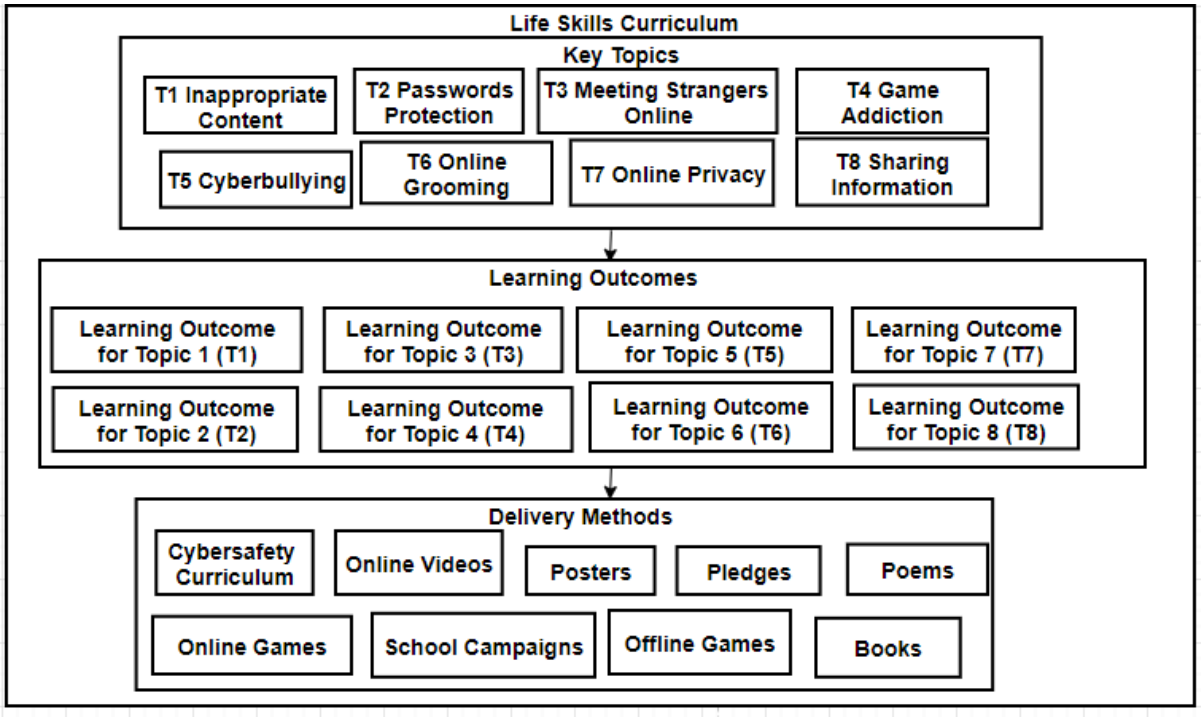


Figure 5.4: Integrating Cybersafety into the Life Skills Curriculum

5.3.5. Key Topics

Incorporating key topics into the Life Skills curriculum assists in ensuring that age and contextually appropriate subject matter is delivered to learners. These key topics, as depicted in Table 5.4, were compiled from the literature review, Chapter 3 (Section 3.7) and Chapter 4 (Sections 4.2.2, 4.4.2, & 4.5.4) in order to identify what material is appropriate for the targeted age group (learners aged between 10 and 12 years old). This section provides details outlining why identifying relevant key topics is an important contributory factor to the success of the proposed framework.

Table 5.4: Key Topics

Key topics	Sections
Inappropriate content	Sections 3.7.4; 4.4.2 and 4.5.4
Cyberbullying	Sections 3.7.1; 4.2.2; 4.4.2 and 4.5.4
Password protection	Sections 4.2.2 and 4.5.4
Online grooming	Sections 4.2.2 and 4.5.4
Meeting strangers online	Sections 3.7.10; 4.4.2 and 4.5.4
Online privacy	Sections 4.4.2 and 4.5.4
Game addiction	Sections 3.7.7; 4.4.2 and 4.5.4
Sharing information	Sections 3.7.6; 4.2.2; 4.4.2 and 4.5.4

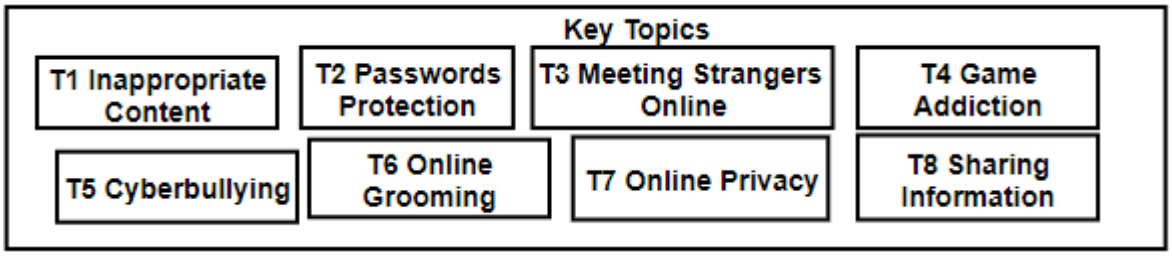


Figure 5.5: Key Topics

Table 5.5: Cybersafety Topics

Topic	Age appropriateness
Inappropriate or illegal online behaviours (T1)	10 to 12 years
Passwords protection (T2)	10 to 12 years
Talking to strangers online (T3)	10 to 12 years
Game addiction (T4)	10 to 12 years
Cyberbullying (T5)	10 to 12 years
Online grooming (T6)	10 to 12 years
Online privacy (T7)	10 to 12 years
Sharing information (T8)	10 to 12 years
Downloads/Plagiarism	13 + years
Sexting	13 + years

As depicted in Table 5.5, key topics are considered important when developing a cybersafety initiative. When determining the key topics for incorporation into a cybersafety programme, the school must ensure that they are appropriate for the target audience. For example, it is inappropriate to teach learners aged 10 to 12 years about sexting as they are not deemed mature enough to meaningfully engage in this subject matter (Clark, Lewis, Bradshaw, & Bradbury-Jones, 2018) .

Table 5.5 indicates the cybersafety topics that were identified in Chapter 3 (Section 3.7). Von Solms and Von Solms (2014) and Third, Forrest-Lawrence, Collier, Stranges, Ul Haq, Dunn, Lazarek (2019) managed to group these topics according to relevant age groups, which helped this study to identify what topics are appropriate for the intermediate phase learners. Furthermore, this study had to argue why some of the topics referred to in Table 5.5 are not appropriate for the intermediate phase. However, topics like inappropriate content, password protection, talking to strangers online, game addiction, cyberbullying, online grooming, online privacy and sharing of information, form the building blocks of the topics covered in specific initiatives such as curricula, games, books and frameworks. Overseers must make use of the previously mentioned resources (Section 5.3.3) to gather suitable materials which provide the information covered in the specified topics in order to impart that information to the learners.

5.3.6. Learning Outcomes

This section provides details for learning outcomes, discussed in Section 4.5.7, that were considered in the proposed framework. A learning outcome is defined as '*a clear statement of what a learner is expected to be able to do, know about and/or value at the end of a completion of a unit of study'* (Teaching and Learning, 2019)

Table 5.6: Cybersafety Topics and Related Learning Outcomes

Cybersafety Topics	**Learning Outcomes**
Inappropriate content (T1)	• Learners will know the risks associated with viewing and sharing inappropriate content.
Password Protection (T2)	• Learners will understand and be able to utilise effective password protection techniques.
Talking to strangers online (T3)	• Learners will be able to identify and understand the potential negative consequences/dangers of meeting strangers online and know how to react if someone requests them to do so.
Game addiction (T4)	• Learners will be able to recognise the signs and symptoms of gaming addiction, be aware of how to avoid becoming addicted and know where to seek help if they are suffering from game.
Cyberbullying (T5)	• Learners will know how to respond appropriately to cyberbullying.
Online grooming (T6)	• Learners will be able to identify online grooming techniques that are utilised by predators and be able to respond appropriately, e.g. stop conversing with the predator and inform a responsible adult.
Online privacy (T7)	• Learners will be aware of the importance of privacy settings and how to activate them.
Sharing Information (T8)	• Learners will understand and be able to implement measures to protect their personal details online.

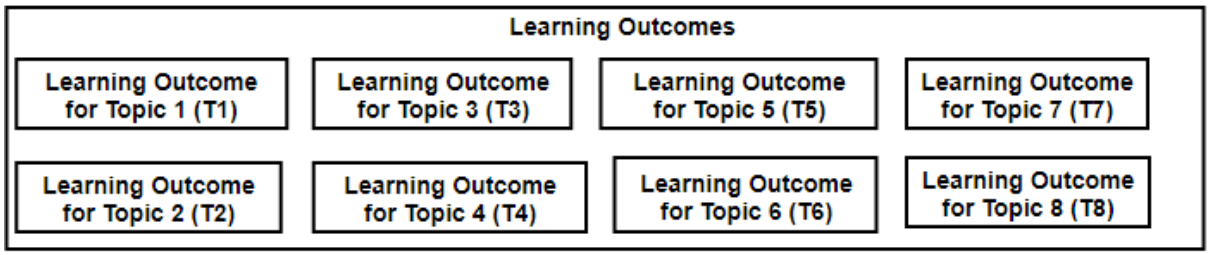


Figure 5.6: Learning Outcomes

This proposed framework has identified key topics that are appropriate for the target audience, together with learning outcomes associated with each topic. School learners must be able to master these learning outcomes at the end of studying each topic.

The achievement of learning outcomes should be measurable (either through formal or informal assessments) as they can be used to provide information about the level of understanding that the pupils have harvested upon completion of the topics. This can in turn be utilised to inform future teaching practice and delivery methods. As such, the learning outcomes play a vital role in determining the success of the proposed framework and the implementation of associated cybersafety initiatives.

5.3.7. Delivery Methods

The delivery methods are different mediums which information from the aforementioned topics (Section 5.3.5) that address cybersafety could be presented to the learners. To model this component of the framework, various delivery methods, as shown in Table 5.7, were considered.

Table 5.7: Delivery Methods

Delivery Methods	**Section**
Cybersafety Initiatives in South Africa	Sections 4.4.1; 4.5.8 and 4.6.7
Delivery method (offline games, online videos, books, cybersafety curriculums, posters, pledges, books)	Section 4.5.8
Delivery method (games; frameworks, books; curricula; guidelines)	Section 4.6.7

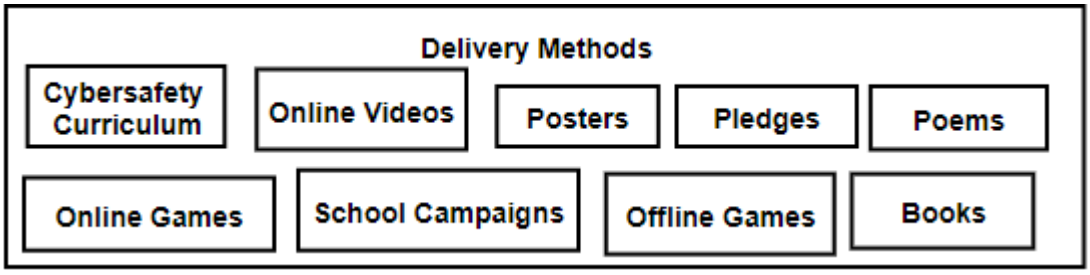


Figure 5.7: Delivery Methods

Delivery methods are an important aspect in every educational intervention. Chapter 4 (Section 4.7.7) detailed some of the delivery methods such as games, frameworks, books, curricula and guidelines, and elaborated upon the purpose that they serve. The delivery method must be informed by the context, the resources, the topics and the learning outcomes. It essential that all relevant information is gathered in order to ascertain how to deliver the initiative in a manner that is effective. For example, it should be delivered in the home language of the learners (where necessary), it can be online or offline, it should be affordable and encompass topics that are age appropriate which address the stated learning outcomes. The delivery methods must also be a method in which the teachers have received appropriate prior training. As highlighted under key constraints, teacher knowledge and skills are an essential component to the success of the proposed framework and associated cybersafety initiative.

This proposed framework recommends that cybersafety is incorporated into the current Life Skills curriculum as other researchers have recommended. Thus, all delivery methods would fall under Life Skills. However, there are multiple options available for delivering appropriate content of the cybersafety initiative. Delivery methods such as games, as discussed in Chapter 4 (Section 4.7.7), can address several of the key constraints that South Africa is currently facing, for example, the lack of funding. Games can be extremely cost effective, the language barrier can be addressed by translating into home languages, they can be reproduced, they typically have a set rules and so are relatively easy to teach educators, parents and learners how to deliver and participate in them (respectively) and they can be presented in offline environments especially for those schools who have limited or no bandwidth.

Mahlangu (2019) has long upheld the belief that combined methods for learning are most beneficial. Therefore, this proposed framework recommends that combined

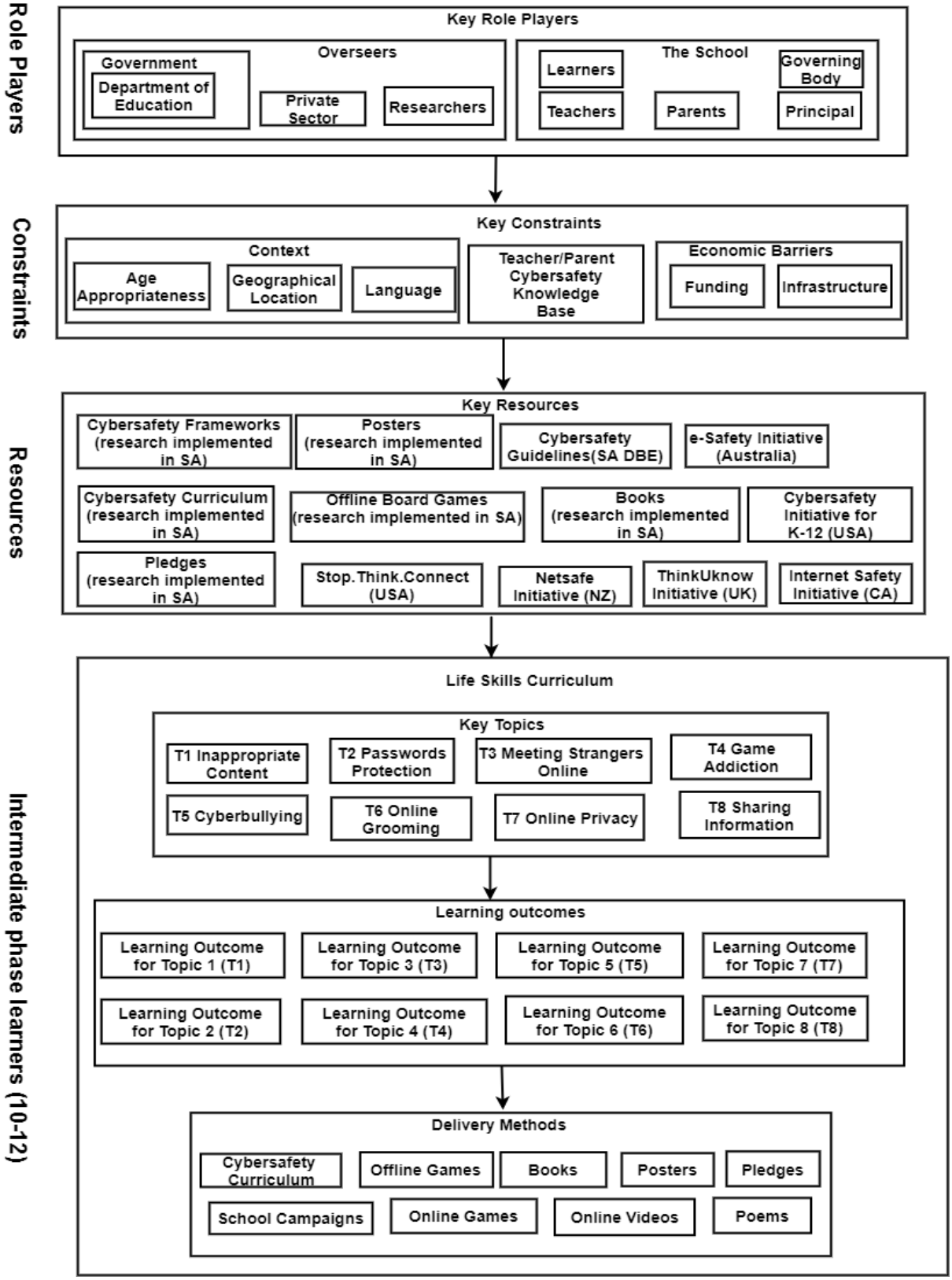
delivery methods be used to implement cybersafety education. Having combined or multiple delivery methods that appeal to a target audience is effective in consolidating information and thus in learners obtaining the stipulated learning outcomes. It was identified that a cybersafety curriculum blended with games can assist school learners to understand cybersafety education in a more comprehensive manner. It was highlighted that school learners enjoy games as a learning tool, and they can be adapted to outdoor activities which are also preferable for learners. Poems, posters, books and school campaigns are highly visible media meaning that they can reach a larger target audience more quickly than online material. They are also effective delivery methods as they can be adapted to different levels of understanding, incorporate a variety of topics or be topic specific, are cost effective as they can be reused, and they can be produced in numerous languages. These have been specifically included in this proposed framework, not only to broaden the learners' understanding, but also to address the identified key constraints in a country as diverse as South Africa. This framework also proposes making use of some of the existing cybersafety curricula that have already been developed. The framework could amalgamate them with the existing Life Skills curriculum and wherever possible adapt them into home languages and offline activities.

Online activities and games are included as delivery methods as the key topic within cybersafety. It is clearly beneficial for learners to be able to put into practice, online, what they learn in the classroom through the initiatives. However, as previously highlighted, access to bandwidth varies vastly in South Africa depending on geographical location and socio-economic factors (amongst other factors).

5.4. THE PROPOSED CYBERSAFETY EDUCATIONAL FRAMEWORK

Figure 5.8 depicts the proposed cybersafety educational framework for primary school learners, aged between 10 and 12 years, in South Africa, which can be applied to the various types of schools as described in Section 5.2.

Figure 5.8: The Proposed Framework



5.5. IMPLEMENTATION OF THE PROPOSED FRAMEWORK

Section 5.2 investigated the three different education systems available in South Africa. Two of these were selected as examples of how to implement the proposed cybersafety framework in Figure 5.8, namely Public schools in South Africa and Model C schools in South Africa. This study utilised all of the information gathered and presented in the previous sections, which was in turn informed from the previous chapters, in order to implement the proposed solution into these two different school settings. However, the research did not focus on Private schools as they appear to have most sufficient technology resources available as indicated in Section 5.2.3. This research was conducted to provide a solution to less privileged schools.

The point of entry into the framework for cybersafety is the overseers, who were described in detail in Section 5.3.1. Regardless of whether a school is a public or a Model C school, the role of the overseers is crucial. They are responsible for delegating the cybersafety initiative to other role players. This framework emphasises that role players are important in every initiative; these are the government (including the Department of Education), private sector, researchers, governing bodies, principals, teachers, parents, and finally learners. Within this framework, the government maintains the responsibility for funding the initiatives, providing both a public curriculum and a cybersafety curriculum (using Life Skills as an umbrella subject) through the DBE.

As there is an acknowledged shortage in government funds, particularly affecting Public schools, this framework seeks to engage the private sector and researchers in collaborating with the government to be overseers. This could prove to be particularly beneficial to public schools and schools in rural areas lacking in both funds and infrastructure. Such collaboration could ensure cohesion between what learners attending both, Public and Model C schools, throughout the country are taught. It is with such cohesion in mind that the framework has set out the topics that are required to be delivered within the intermediate phase of primary school. Government experts, researchers and the private sector are responsible for defining these topics as areas of learning which should fall under Life Skills and be taught in all Public and Model C classrooms across the country.

The governing bodies and the school principals must engage in the initiative, and they must ensure that school rules and policies are put into place that align with the cybersafety curricula. Being the holders of the day-to-day running of the school, the principals must also ensure that they actively identify and address gaps in knowledge and skills that their teaching staff may have. Once these are identified they must pursue appropriate recourse – seek training and monitor the effectiveness of that training. The government and the private sector will be sought to design and offer appropriate training to teaching staff in their roles as overseers. Governing bodies, principals and teachers must work hand in hand in order to foster a greater understanding of cybersafety amongst the parents of their learners. They can do this by holding workshops, seminars, and community programmes and using media resources such as posters, leaflets and information books. Again, due to budgetary constraints, this framework would seek assistance in funding for such measures from the private sector and researchers. In Model C schools, parent-led funding would also be sought. The framework makes ample provision for offline resources (such as books, poems, posters, offline games, etc.) which will more likely be the main delivery methods for Public schools; particularly in rural areas. When selecting such resources, emphasis must be placed on whether or not they are age appropriate, they align with the framework's specified topics, and that they are able to be delivered in home languages and not just English, as has previously been the case.

Whilst many Model C schools have been shown to deliver the majority of their learning through the medium of English, the same cannot be said for Public schools. Thus, in order to negate language as a barrier to learning, multilingual versions of the resources are vital. As this framework is based in the school setting, teachers will be the key facilitators of the initiatives. It is vital that they equip themselves with the knowledge and understanding in order to do this. The teachers will be the primary initiators of the usage of the specified resources. They must ensure that all the specified topics are covered within the designated time frame and that the associated learning outcomes are met by their learners. The framework puts emphasis on utilising combinations of resources in order to improve and consolidate the learners' subject knowledge. The teachers hold the responsibility for ensuring that this happens. Formal and informal assessments should be utilised in order to both measure the success of this and inform future delivery/learning.

The proposed framework is aimed at intermediate phase school learners in South Africa, from 10 to 12-year olds. This is applicable to both Public and Model C schools as the stipulated primary school phases are the same in both schools. The learners have a duty of responsibility to engage in their education and follow the school rules and policies. In acknowledging the impact that peers can have on one another, the framework seeks to encourage learners to also assume the roles of advisors and identifiers. In these roles, learners become quick identifiers of problems arising with their peers' ICT usage and their cybersafety. Peer group compliance and peer pressure are common phenomena that expand across both geographical location and socio-economic development and are common to both Public and Model C schools.

Collaboration of all interested parties can be seen to be the key to the success of this proposed framework for cybersafety. The need for such collaboration is common to both Public and Model C schools. However, the degree to which the various role players are engaged is dependent on and reflective of the individual schools' needs. This is primarily determined by the constraints that they face. Both subsets of schools must utilise each step of the framework in order to ensure that they use the components that are most applicable to their circumstances, particularly with regards to resources and delivery methods. This could in turn foster consistency and exemplary learning.

5.6. CONCLUSION

This chapter introduced a cybersafety framework for primary school learners in South Africa. The cybersafety framework has various components that were considered, and these include:

- Role players
- Constraints
- Resources
- Topics
- Learning outcomes
- Delivery methods

Different role players were identified, each with specific responsibilities. These role players are greatly important, and they should work together to implement cybersafety

education amongst primary school learners in South Africa. If this framework is implemented and managed properly it could contribute towards raising cybersafety education among primary school learners in South Africa, improve the relevant skills and assist in cultivating a cybersafe culture. This chapter has accomplished the primary objective of this study, which is to propose a framework that will assist primary school learners in South Africa in creating a cybersafe culture in cyberspace. The following chapter concludes this study.

CHAPTER 6 CONCLUSION

6.1. INTRODUCTION

This research study focused on cybersafety education, with the emphasis being placed on primary school learners. It has been revealed that primary school learners are the most vulnerable in cyberspace as they are at the age when children start to experiment with technology; however, they are often unaware of the potential risks and threats associated with ICT use. Hence, there is a clear need for the development of the knowledge and the skills required to protect them from cybersafety risks and threats. Although the South African government has made some commitments towards cybersafety education, they have been deemed as insufficient in supporting the majority of teachers to assist school learners with cybersafety. Therefore, the aim of this study was to propose a framework for cybersafety education for primary school learners in South Africa, which was presented in Chapter 5.

This chapter forms the conclusion of the study, it provides a summary of the primary findings and arguments from the previous chapters, revisits the objectives to ascertain whether or not they have been met and finally discusses the limitations of and applications of the study for possible future research.

6.2. SUMMARY OF CHAPTERS

Chapter 1

Chapter 1 demonstrated that a growing number of school learners, who are at the age of primary school education, are experimenting with and are being exposed to technology, which subsequently makes them extremely vulnerable in cyberspace. This is due to the fact that they are unaware of the risks and threats associated with cyberspace. It has been highlighted that the South African government has been in a position to and holds the primary responsibility of addressing cybersafety education throughout primary schools in South Africa. In spite of this, there is currently no formal curriculum for cybersafety education in place. Instead the DBE formulated guidelines to address cybersafety education. De Lange (2012) research similarly concluded that these guidelines are not enough to address the complexity of cybersafety education in South Africa. Nevertheless, initiatives have been implemented in select schools by researchers from various South African universities. These researchers have

developed their own curricula, resources and materials to be utilised in schools to tackle cybersafety.

The delivery of these independent research programmes is sporadic at present and so cannot be seen as an effective solution to tackle the identified problems. Another issue highlighted by the research in this study is that many primary school teachers in South Africa are ill-equipped to implement cybersafety initiatives, leading to learners that are vulnerable to cyber-related threats. Teachers are the key role players in delivering the topics, formed by educational frameworks, to learners. Whilst many teachers lack the knowledge and skills along with the materials and resources, to effectively deliver cybersafety education, the learners will possibly not be enlightened and will continue to be at risk. The research objectives and processes were formulated from the information gathered in this chapter and are discussed in the following sections.

Chapter 2

The purpose of this chapter was to introduce the research process and the design methods used in this study, namely the qualitative approach. It provided reasoning for why this approach was preferable to other approaches in addressing the objectives. This research approach involved undertaking a literature review, a content analysis, comparative analysis, critical reasoning, modelling and argumentation.

Chapter 3

In the modern world, cyberspace has become part of the daily lives of millions of people worldwide; introducing technologies and applications that make life easier and more efficient. Further, in this modern world, cyberspace is increasingly becoming more of a necessity than a luxury. School learners visit cyberspace for many reasons such as social networking, entertainment and education. The cyberspace has brought many advantages to daily life. However, cyberspace is a complex environment because there are few enforceable rules governing it, and thus it has introduced exposure to a new set of risks. As such, it is imperative that school learners are taught to be able to identify the benefits and risks associated with cyberspace and how to protect themselves from the risks. Therefore, the purpose of Chapter 3 was to identify the key cybersafety threats and related risks to primary school learners (SO1). In order to achieve this, the researcher investigated cyberspace, defined cybersecurity,

cybersafety and cyberethics and their relationship to one another. It was ascertained that the most common threats among primary school learners include cyberbullying, access to inappropriate content, online grooming, game addiction, password protection, meeting online strangers, sharing of information and online privacy.

Chapter 4

Cybersafety education plays an important role in cultivating a cybersafe culture amongst school learners. Chapter 4 investigated current cybersafety initiatives globally, in Africa and in South Africa (SO2) (i.e. in both developed and developing countries). The investigation focus was to identify the main challenges relating to cybersafety education in the South African context (SO3). The following were subsequently identified as main the challenges: South Africa has no formal cybersafety education curriculum in place and is therefore currently lagging behind the progress being made in developed countries.

South Africa has 11 official languages, yet most initiatives are conducted in English. This can prove to be a highly problematic language barrier which consequently restricts pupils' learning. Additional factors affecting cybersafety education in South Africa include limited delivery methods, lack of skills and knowledge from the teachers and parents, insufficient infrastructure, funding and geographical location. It was concluded that educating primary school learners on cybersafety should be a priority, since it is the entry point of education. Therefore, it is important that the government of South Africa channels some of its resources to schools in order to equip school learners on cybersafety.

Based on the commonalities, gaps and findings identified, key components were constructed with the goal of overcoming the challenges identified in addressing the cybersafety education of primary school learners in South Africa (SO4). Therefore, this study proposed a framework for the cybersafety education of primary school learners in South Africa – the details of which are dealt with in the next section.

Chapter 5

Chapter 5 introduced a solution to the problem defined this study, which is a cybersafety framework for primary school learners in South Africa. To address the challenges in South Africa, this framework was proposed as a solution with the following components:

- Role players
- Constraints
- Resources
- Life skills
- Topics
- Learning outcomes
- Delivery methods.

These components were drawn from thematic questions used for the content analysis as well as the deduction and conclusion in Chapter 4. These thematic questions were derived from previous similar studies and were concluded to be important when implementing a cybersafety initiative.

The framework places a large emphasis on identifying and addressing the constraints to delivering cybersafety in South African primary schools. The language barrier, geographical location, funding, target audience, infrastructure, lack of teacher's knowledge base and limited delivery output were the commonly identified constraints and as such they were woven into the framework. Furthermore, the framework recognises that in every initiative it is essential to identify the role players and ensure that they have clearly defined roles.

Topics from which learning outcomes are taken are an important component of the framework as they seek to address the cybersafety threats and related risks which have been identified as relevant to the age group. They provide a focus for the learning resources and delivery methods to tackle. These topics can be identified from existing resources which can either be external (developed countries) or internal (local); the priority is for them to overcome the constraints that were identified in the planning phase of the initiative.

The final component discussed was the delivery methods. This communicates the methods that will be utilised in order use the resources to communicate the curriculum. For example, board games, books, existing frameworks etc. The delivery methods are how the teachers impart the relevant information to the learners. This framework places an emphasis on combining delivery methods in order to increase their efficacy; improving and consolidating learners' knowledge. The framework emphasises combining Life Skills topics and cybersafety topics to communicate cybersafety

education to primary school learners in an effective way that they understand. More so, it emphasises incorporating cybersafety education to be part of Life Skills curriculum.

6.3. MEETING THE RESEARCH OBJECTIVES

The primary objective of this study as stated in Chapter 1 (Section 1.4.1) was to develop a framework for the cybersafety education of primary school learners in South Africa, in order to overcome the cybersafety threats and related risks that these learners are exposed to. The purpose of this is to address the need to educate primary school learners and teachers about cybersafety threats, since many teachers are ill-equipped to implement cybersafety initiatives by themselves. To achieve the primary objective, the following secondary objectives were identified: to pinpoint the key cybersafety threats and related risks to primary school learners (SO1); to investigate current cybersafety initiatives globally and in South Africa (SO2); to identify the main challenges relating to cybersafety education in the South African context (SO3); and to identify key components required to overcome challenges identified in addressing the cybersafety education of primary school learners in South Africa (SO4).

Chapter 2 discussed how the research process was conducted and the design methods that were applied. Chapter 3 addressed the first secondary objective, i.e. to identify the key cybersafety threats and related risks to primary school learners (SO1). This was achieved through a literature review which distinguished the key cybersafety threats learners face, such as cyberbullying, online privacy, protection of passwords, online grooming, inappropriate content, addiction to games, sharing of information and meeting online strangers. It was noted that as school learners are becoming cyber citizens, they are at risk of falling prey to some of the threats associated with cyberspace; hence, they need to be taught how to identify these online cybersafety threats. The identified threats and related risks were then used (in Chapter 5) to form cybersafety topics which were incorporated into the proposed cybersafety framework for primary school learners in South Africa.

The second secondary objective was to investigate current cybersafety initiatives globally and in South Africa (SO2) and this was addressed in Chapter 4 through a literature review and qualitative content analysis. Through a qualitative content analysis, the study recognised that both developed and developing countries have

promoted cybersafety education within primary schools; however, the spectrum of these initiatives differs vastly between the developed and the developing world.

A comparative analysis, literature view and argumentation were used to identify the main challenges relating to cybersafety education in the South African context (SO3). Through this comparative analysis it was established that most developed countries educate school learners about cybersafety in primary school, as it is the entry point of education and the age of learning about and experimenting with technology. In addition, it was discovered that Africa as a whole is lagging behind in terms of cybersafety (though some countries like Mauritius, Tunisia, Kenya, Ghana, Cameroon, Egypt and Rwanda have started to implement cybersafety education in schools). South Africa specifically is failing its learners as there is currently no formal cybersafety curriculum in place. This has been determined (primarily) to be the responsibility of the government which, in spite of recent promises to enable all school learners' access to ICT, has shown very little commitment to developing, funding and implementing these promises.

Through the processes of a literature review, arguments and critical reasoning, key components required to overcome challenges to address the cybersafety education of primary school learners in South Africa (SO4) were identified. These key components were used to develop the proposed solution for a framework for cybersafety education for primary school learners in South Africa. The following are the key components the framework identifies: recognising all of the role players needed, considering the constraints before implementing any cybersafety education, making use of available resources to improve or create new initiatives, incorporating cybersafety education into Life Skills, identifying age appropriate topics, formulating the topics learning outcomes and making use of combined delivery methods. It was through the amalgamation of these key components that the framework for this study was created. Hence the research has succeeded in addressing the primary objective, which was to develop a framework for cybersafety education of primary school learners in South Africa.

6.4. RESEARCH CONTRIBUTION

The primary objective of this research was to develop a framework for cybersafety education of primary school learners in South Africa, in order to overcome the

cybersafety threats and related risks that these learners are exposed to. Hence, the contribution of this research is the developed framework.

The primary objective of this research was met in Chapter 5 where the framework for cybersafety education of primary school learners in South Africa was proposed in Section 5.3. The proposed framework is presented to include the following key components: The role players, the constraints, the resources, the Life Skills, the topics, the learning outcomes and the delivery methods. This framework was developed to assist primary school teachers in implementing cybersafety education in schools. The main aim of this framework is to try and focus on the constraints which various schools encounter when implementing cybersafety education. Therefore, the framework suggests that before implementing, one should in the planning phase always look out for the constraints that might have an impact on the success of cybersafety education in different schools. More so, the framework suggests cybersafety education must be part of Life Skills as a subject in South Africa. Therefore, teachers can blend cybersafety topics with Life Skills topics for school learners to have a better understanding since both of the subjects equip pupils with Life Skills.

In addition, the framework suggests that every topic in cybersafety education must have learning outcomes that students must master at the end of each lesson. Lastly, the framework suggests that to deliver cybersafety education, teachers can ensure multiple delivery methods to try and help learners understand better cybersafety education. For example, there can be a curriculum that can be presented in class, and a game can be designed for every cybersafety topic as outdoor activities to help learners enjoy and better understand cybersafety education in a relaxed environment. To illustrate how the proposed framework could be implemented by teachers, the implementation was discussed in Chapter 5 (Section 5.3.2).

6.5. FUTURE RESEARCH

Cybersafety education forms the foundation of a cybersafety culture. This culture of awareness is increasingly needed in today's environment where more and more online activities are taking place, transcending age groups, cultures, religions and geographical locations. In this study, a framework was proposed to assist teachers to educate primary school learners in South Africa in creating cybersafety education. The framework will provide the necessary cybersafety understanding and knowledge to

South African primary school learners this would therefore contribute to the creation of the envisioned cybersafe culture.

The framework is acknowledged to be a small step towards the envisioned cybersafety culture. It has been devised in such a way that it is applicable and adaptable to different school environments. However, this study had its limitations, one of which is that it did not focus on measuring the effectiveness of the framework. Therefore, this study recommends that any future research deliberates on measuring the effectiveness of the implementation of the proposed framework.

6.6. LIMITATIONS OF THIS RESEARCH STUDY

The study focused on primary school learners in the South African school environment. However, the research has identified that there is a need for cybersafety principles to be transferable to everyone.

As identified in Section 6.4, this research did not include measuring the effectiveness of the framework. It relies on the assumption that the learning outcomes alone will be used as a benchmark for success.

The proposed framework relies heavily on the governments' compliance to funding, designing and implementing a cybersafety curriculum to be incorporated into the current Life Skills curriculum. It also emphasises the need for collaboration amongst many interested parties in order to be fully effective. Such collaborations can bring issues of organisation, governance and accountability. They have also to date proven to be implemented on a small scale and not on national basis.

6.7. FINAL WORD

Cyberspace is being adopted by humans at a rapid rate. Increasingly, cyberspace is redefining the way school learners communicate, gain access to information, share information and entertain themselves (Kortjan & Von Solms, 2014; Stone, 2013). School learners are growing up as cyber citizens, surrounded by and using many ICT technologies, environments, and services. However, although cyberspace comes with such benefits, school learners will continue to use and access cyberspace unsafely and insecurely if not taught or made aware of this secure conduct in cyberspace (Sawyer, 2017). This is problematic, as school learners will continue to access cyberspace throughout their lifetimes and will always be exposed to cyber risks

(Sawyer, 2017). Therefore, school learners are a subgroup of society who particularly need cybersafety solutions, and the relevant knowledge and skill sets to implement them. School learners are amongst the most vulnerable members of society to cybersafety risks (Von Solms & Von Solms, 2014).

This study discovered that primary school education plays a key role in embedding cybersafety into modern culture. As such, this study developed and discussed a cybersafety framework that will be instrumental in assisting teachers to educate primary school learners in South Africa. This framework serves to foster, facilitate and promote a culture of cybersafety amongst primary school learners in South Africa.

REFERENCES

Atkinson, S., Furnell, S. & Phippen, A. (2009). Securing the next generation: enhancing e-safety awareness among young people. *Computer Fraud and Security*, 2009(7):13–19. Available: https://doi.org/10.1016/S1361-3723(09)70088-0 [Accessed: 4 April 2019].

Australian Government. (2014). *Enhancing online safety for Children Bill 2014*. Available: https://www.legislation.gov.au/Details/C2014B00254/Explanatory%20Memorandum/Text [Accessed: 24 March 2019].

Bada, M. (2017). *A Study into the Cybersecurity Awareness Initiatives for School Learners in South Africa and the UK*. (May). https://doi.org/10.1007/978-3-319-58553-6

Badenhorst, C. (2011). Legal responses to cyber bullying and sexting in South Africa. *Centre for Justice and Crime Prevention*, *August*(10), 1–20. Retrieved from http://www.childlinesa.org.za/index2.php?option=com_docman&task=doc_view&gid=221&Itemid=64

Becta. (2009). Establishing safe and responsible online behaviours. *Becta*, (February). Retrieved from http://www.teachtoday.eu/sitecore/shell/Applications/~/media/Files/United Kingdom/Becta/Becta AUPs in context - downloaded on 25 January 2011.ashx?db=master&la=en&vs=1&ts=20110704T1820334896

Berson, M.J., & Berson, I.R. (2004). Developing thoughtful “cybercitizens”. *Social Studies and the Young Learner,* 16(4):5–8.

Boote, D.N., & Beile, P. (2005). Scholars before researchers: On the centrality of the dissertation literature review in research preparation. *Educational Researcher*, 34(6):3–15

Boren, Z.D. (2014). There are officially more mobile phones than people in the world. *The Independent, UK*, 7 October.

Boyes, H. (2015). Cybersecurity and Cyber-Resilient Supply Chains. *Technology Innovation Management Review*, *5*(4), 28–34.

https://doi.org/10.22215/timreview888.

Burton, P. & Mutongwizo, T. (2009). *Inescapable violence: Cyberbullying and electronic violence against young people in South Africa. Centre for Justice and Crime Prevention (CJCP) Issue Paper*. 1–12. Retrieved from http://cyberbullying.ezipezi.com/downloads/IssuePaper8-InescapableViolence-CyberAggression.pdf

Byron, T. (2008). *Safer Children in a Digital World The Report of the Byron Review*.

Chandrashekhar, A., Muktha, G., & Anjana, D. (2016). Cyberstalking and cyberbullying: Effects and prevention measures. *Imperial Journal of Interdisciplinary Research*, 2(3):95–102.

Clark, M., Lewis, A., Bradshaw, S., & Bradbury-Jones, C., (2018). How public health nurses' deal with sexting among young people: A qualitative inquiry using the critical incident technique. *BMC Public Health*, *18*(1), 1–10. https://doi.org/10.1186/s12889-018-5642-z

Creswell, J. (2003). *Research design: Qualitative, quantitative and mixed methods approaches* (2nd ed.). Thousand Oaks, CA: SAGE Publications.

Cross, D., Shaw, T., Hadwen, K., Cardoso, P., Slee, P., Roberts, C., Barnes, A. (2016). Longitudinal impact of the cyber friendly schools program on adolescents' cyberbullying behavior. *Aggressive Behavior*, 42(2):166–180. Available: https://doi.org/10.1002/ab.21609 [Accessed: 21 September 2019].

Czerniewicz, L. 2010. 'Mobile Is My Soul': More about cell phones in the South of Africa. Guest post May 22, 2010. E- literate. http://mfeldstein.com/mobileis-my-soul-cell-phones-in-south-afric/. [13 April 2012]

D'Antona, R., Kevorkian, M., Russom, A. & Lauderdale, F. (2010). Sexting, Texting, Cyberbullying and Keeping Youth Safe Online. 6(4), 523–528.

DCAF. (2018). *The Ministry of Education and DCAF Tunisia organize conference on "Promoting a Culture of Cybersecurity in Schools".* Retrieved from DCAF: http://www.dcaf-tunisie.org/En/activite-partenaires/the-ministry-of-education-and-dcaf-tunisia-organize-a-conference-on-promoting-a-culture-of-cybersecurity-in-schools/87/10329.

De Barros, M.J.Z. & Lazarek, H. (2018). A Cyber Safety Model for Schools in Mozambique. (Icissp), 251–258. https://doi.org/10.5220/0006573802510258

De Lange, M. (2012). Guidelines to Establish an e-Safety Awareness in South Africa. 217. Submitted in fulfilment of the requirements for the degree M IT in Information Systems In the Faculty of Engineering Built and Information Technology. Nelson Mandela Metropolitan University.

De Lange, M. & Von Solms, R. (2012). An e-safety educational framework in South Africa. In *Proceedings of the Southern Africa Telecommunication Networks and Applications Conference (SATNAC)*.

De Wet, W., Koekemoer, E., & Nel, J.A. (2016). Exploring the impact of information and communication technology on employees' work and personal lives. *SA Journal of Industrial Psychology*, 42(1). Available: https://doi.org/10.4102/sajip.v42i1.1330 [Accessed: 23 September 2019].

Department of Basic Education (DBE). (2010). *Guidelines on e-Safety in Schools : Educating towards responsible , accountable and ethical use of ICT in education*. Retrieved from http://goo.gl/mxK0xa

Department of Communications and the Arts, Australia. (2014). *Enhancing online Safety for Children Bill 2014*. Available: https://goo.gl/rmfpqU [Accessed: 3 October 2019].

Dlamini, I. Z., Taute, B., & Radebe, J. (2011). Framework for an African Policy Towards Creating Cyber Security Awareness. Proceedings of Southern African Cyber Security Awareness Workshop (SACSAW). Retrieved April 24, 2019, from http://researchspace.csir.co.za/dspace/handle/10204/5163.

Dlamini, Z. & Modise, M. (2012). Cyber security awareness initiatives in South Africa: a synergy approach. *7th International Conference on Information Warfare and Security*, 10. Available: https://doi.org/10.1007/978-3-8349-4134-3_3 [Accessed 24 April 2019].

Eagle, C. (2018). More youth at risk to online predators. *Cochranetoday*, 25 January. Available: https://www.cochranetoday.ca/our-view/more-youth-at-risk-to-online-predators-1454602 [Accessed: 26 September 2019].

Farrell, N. (2014). *Government to give kids cyber security lessons*. Available: http://www.techradar.com/news/software/security-software/government-to-give-kids-cyber-security-lessons-1233480?src=rss&ttr=al [Accessed: 27 September 2019].

Fisch, S.M. (2005). Making educational computer games educational. In Proceedings of the 2005 conference on niteraction design and children (pp. 56-61). ACM. Available: https://doi.org/10.1145/1109540.1109548 [Accessed: 24 May 2019].

Furnell, S. (2010). Jumping security hurdles. Computer Fraud & Security Bulletin, 2010(6), 10–14. https://doi.org/10.1016/S1361-3723(10)70067-1.

Giannakas, F., Kambourakis, G. & Gritzalis, S. (2015). CyberAware: A mobile game-based app for cybersecurity education and awareness. Proceedings of 2015 International Conference on Interactive Mobile Communication Technologies and *Learning, IMCL 2015*, (November), 54–58. https://doi.org/10.1109/IMCTL.2015.7359553

Grey, A. (2019). Cybersafety in Early Childhood Education. *Australasian Journal of Early Childhood*, *36*(2), 77–81. https://doi.org/10.1177/183693911103600210

Google (2017). “Make safety choices that fit your family” Available http://www.google.co.za/safetycenter/families/start/ (Accessed 14 August 2017).

Gous, N. (2019). Pretoria girl commits suicide allegedly after cyberbullying. *Sunday Times*, 19 February. Available: https://www.timeslive.co.za/news/south-africa/2019-02-19-pretoria-girl-commits-suicide-allegedly-after-cyberbullying/ [Accessed: 26 September 2019].

Halder, D. (2015). *Children of internet era : A critical analysis of vulnerability of children in the darker sides of social media and WhatsApp*.Conference proceedings of two days international conference on Accompanying social networking in teacher education held on 26-27 March 2015, Loyola College of Education, Chennai, 17-24.

ISO/IEC 27002. (2005). Information technology — Security techniques — Code of practice for information security management. Information technology —

Security techniques — Code of practice for information security management, p. 115.

ISO/IEC 27032:2012. (2012). Information technology — Security techniques — Guidelines for cybersecurity. Information technology — Security techniques — Guidelines for cybersecurity, p. 50.

Jossel, L. (2016). *South African kids online: A glimpse into children's internet use and online activities*. Available: http://www.cjcp.org.za/uploads/2/7/8/4/27845461/south_africa_kids_online_full_report.pdf [Accessed: 24 November 2019].

Khanyile, N. (2019).*Screen time versus real time*. Retrieved from *https://www.news24.com/SouthAfrica/News/screen-time-vs-real-time-20190121*

Kingson, J.W, (2019). *National Cyber Security Center takes cyber education to schools*. Retrieved from http://newsghana.com.gh/national-cyber-security-center-takes-cyber-education-to-schools/

Klaper, D. & Hovy, E. (2014). A taxonomy and a knowledge portal for cybersecurity. *ACM International Conference Proceeding Series*, 79–85. https://doi.org/10.1145/2612733.2612759

Kortjan, N. (2013). *A Cyber Security Awareness and Education Framework for South Africa*. 219. Retrieved from http://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=6&ved=0CEUQFjAF&url=http://contentpro.seals.ac.za/iii/cpro/app?id=0865119265660214&itemId=1014829&lang=eng&service=blob&suite=def&ei=L6tpVMuILYOrPMLXgdAC&usg=AFQjCNEihfIKD7OdI4JytH67NSl3lSqDTg&s

Kortjan, N. & Von Solms, R. (2014). A conceptual framework for cyber-security awareness and education in SA. *South African Computer Journal*, *52*(1):29–41.

Kosseff, J. (2018). *Cybersecurity law*. 1st ed. Hoboken, NJ: Wiley.

Krippendorff, K. (1980). *Content analysis: An introduction to its methodology*. Newbury Park: Sage Publications.

Kritzinger, E. (2017a). Cultivating a cyber-safety culture among school learners in South Africa *Africa Education Review*, 14(1):22–41. Available:

https://doi.org/10.1080/18146627.2016.1224561 [Accessed: 24 November 2019].

Kritzinger, E. (2017b). Growing a cyber-safety culture amongst school learners in South Africa through gaming. *South African Computer Journal*, *29*(2), 16–35. https://doi.org/10.18489/sacj.v29i2.471

Kritzinger, E. (2016). Short-term initiatives for enhancing cyber-safety within South African schools. *South African Computer Journal*, *28*(1), 1–17. https://doi.org/10.18489/sacj.v28i1.369

Kritzinger, E. (2015). Enhancing cyber safety awareness among school children in South Africa through gaming. *Proceedings of the 2015 Science and Information Conference, SAI 2015*, 1243–1248. https://doi.org/10.1109/SAI.2015.7237303

Kritzinger, E. (2014a). Online safety in South Africa -A cause for growing concern. *2014 Information Security for South Africa - Proceedings of the ISSA 2014 Conference*. https://doi.org/10.1109/ISSA.2014.6950502

Kritzinger, E. (2014b). *Cyber Safety: A South African perspective*. 1–10. Retrieved from https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/Cybersafety_Awareness_Southafrica_0.pdf

Kritzinger, E. (2011). *Children Edition: Cyber Security Awareness Workbook*. Available: https://www.fpb.org.za/wp-content/uploads/2017/05/Cyber-Security-workbook-_Children_Edition_Final-Sipho-Edits.pdf [Accessed: 24 March 2019].

Kritzinger, E. & Padayachee, K. (2013). Engendering an e-safety awareness culture within the South African context. *IEEE AFRICON Conference*. https://doi.org/10.1109/AFRCON.2013.6757708

Kritzinger, E. & Padayachee, K. (2007). Teaching Safe and Secure usage of ICTs in South African Schools. *Proceedings of the 2nd International Conference on Society and Information Technologies*, 1–6.

Kritzinger, E., Bada, M. & Nurse, J.R.C. (2017). A study into the cybersecurity awareness initiatives for school learners in South Africa and the UK. *Wise 10, Ifip*, (May). https://doi.org/10.1007/978-3-319-58553-6_10

Lai, E.R. (2011). *Critical thinking: A literature review*. Pearson. Available: https://images.pearsonassessments.com/images/tmrs/CriticalThinkingReviewFI

NAL.pdf [Accessed: 23 November 2019].

Livingstone, S. & Smith, S.K. (2015). Annual research review: Harms experienced by child users of online and mobile technologies: The nature, prevalence and management of sexual and aggressive risks in the digital age. *Journal of Child Psychology and Psychiatry, 55*(6), 635–654.

Longe, O.B., Ngwa, O., Wada, F. & Mbarika, V.W.A. (2009). *Criminal Uses of Information & Communication Technologies in Sub-Saharan Africa : Journal of Information Technology Impact*. (January).

Mafuwane, B.M. (2011). *The contribution of instructional leadership to learner performance*. Unpublished PhD dissertation. Pretoria: University of Pretoria.

Magumane, K. (2012). SA not taking cybercrime seriously enough, experts warn. *BusinessDay Live*, 25 September. Retrieved from: http://www.bdlive.co.za/business/technology/2012/09/25/sa-not-taking-cyber-crime-seriously-enough- experts-warn

Mahlangu, T.M.Z.D. (2019). *Proceedings for the 14th International Conference on Cyber Warfare and Security (ICCWS)*.

Matthews, B. & Ross, L. (2010). *Research methods: A practical guide for the social sciences*. Canada: Pearson Education.

Miles, D. (2011). Youth protection: Digital citizenship – Principles and new resources. In *Second Worldwide Cybersecurity Summit (WCS)* (pp. 1–3). IEEE.

Mills, M., Van de Bunt, G.G., & De Bruijn, J. (2006). Comparative research: Persistent problems and promising solutions. *International Sociology*, 21(5):619–631.

Miniwatts Marketing Group. (2019). *Internet world users.* Retrieved from Internet World Stats: https://www.internetworldstats.com/stats.htm

Mochiko, T. (2012). Cybercrime costs SA R3.7bn over past year. *BusinessDay Live.* Available: http://www.bdlive.co.za/ business/technology/2012/10/25/cybercrime-costs-sa-r3.7bn-over-past-year [Accessed February 28, 2014].

Mzekandaba, S. (2019). *Public sector priorities 2019 – Special report.* Rivonia: ITWeb Limited.

Online Safety and Technology Working Group (OSTWG). (2010). *Youth safety on a living internet.* Available: https://www.ntia.doc.gov/report/2010/youth-safety-living-internet

Paraiso, E.L. (2019). *Introduction – Background towards a cyber safety information framework for South African parents.* Submitted in fulfilment of the requirements for the degree M IT in Information Systems In the Faculty of Engineering Built and Information Technology At th. (January).

Paraiso, E.L. & Matthee, M. (2016). Towards a Cyber Safety Information Framework for South African parents Proceedings of the African Cyber Citizenship 31 October – 1 Npvermber 2016, 85-96.

Park, S., Na, E.Y. & Kim, E.M. (2014). The relationship between online activities, netiquette and cyberbullying. *Children and Youth Services Review*, *42*, 74–81. https://doi.org/10.1016/j.childyouth.2014.04.002

Presidency Republic of South Africa. (2019). *State of the Nation Address (SONA)*. Available: https://www.gov.za/sona2019 [Accessed: 29 November 2019].

Pretorius, L. (2019). Special Report: Data costs are falling, say Vodacom, MTN, Cell C, Telkom. *Fin24,* 15 January. Available: https://www.fin24.com/Companies/ICT/special-report-data-costs-are-falling-say-vodacom-mtn-cell-c-telkom-20190115-2 [Accessed: 26 September 2019].

Procter, P. (1995). *Cambridge International Dictionary of English*. Cambridge/New York: Cambridge University Press.

Pruitt-Mentle, D. (2001). C3 Matrix – A companion to the augmented technology literacy standards for students. The IKeepSafe Digital Citizenship C3 Matrix.

Pusey, P. & Sadera, W.A. (2011). Cyberethics, Cybersafety, and Cybersecurity: Preservice Teacher Knowledge, Preparedness, and the Need for Teacher Education to Make a Difference. Journal of Digital Learning in Teacher Education, 28(2), 82–85. https://doi.org/10.1080/21532974.2011.10784684.

Radoll, P. (2014). Cyber-safety and Indigenous youth. *Indigenous Law Bulletin*, *8*(12), 11–14. https://doi.org/10.1525/sp.2007.54.1.23.

Reid, R. & Van Niekerk, J. (2014). Snakes and ladders for digital natives: information

security education for the youth. *Information Management & Computer Security*, *22*(2), 179–190. https://doi.org/10.1108/IMCS-09-2013-0063

Reid, R. & Van Niekerk, J. (2013). Towards an education campaign for fostering a societal, cyber security culture. Proceedings of the Eighth International Symposium on Human Aspects of Information Security & Assurance (HAISA), pp. 174-184.

Richmond Magazine. (2019). *Private Schools Guide 2019*. Available: https://www.scribd.com/document/421861445/Private-Schools-Guide-2019 [Accessed: 24 November 2019].

Rigby, K. (2017). School perspectives on bullying and preventative strategies: An exploratory study. *Australian Journal of Education*, 61(1):24–39. Available: https://doi.org/10.1177/0004944116685622 [Accessed: 24 September 2019].

Saunders, M.N.K., Lewis, P., & Thornhill, A. (2009). *Research methods for business students*. New York: Pearson.

Sawyer, R. (2017). *Emergent trends in risk: Disruptive Cyber threats.* CIO Applications. Available: https://sales-tech.cioapplications.com/cxoinsights/emergent-trends-in-risk-disruptive-cyber-threats-nid-1354.html [Accessed: 24 November 2019].

Singer, P.W., & Friedman, A. (2014). *Cybersecurity and cyberware*. Oxford: Oxford University Press.

Smit, D.M. (2015). Cyberbullying in South African and American schools: A legal comparative study. *South African Journal of Education*, *35*(2), 1–11. https://doi.org/10.15700/saje.v35n2a1076

Smith, P., Mahdavi, J., Carvalho, M. & Tippett, N. (2006). An investigation into cyberbullying , its forms, awareness and impact, and the relationship between age and gender in cyberbullying. *Research Brief*, (July), 1–69. Available: https://doi.org/421 [Accessed: 2 March 2019].

South African Cyber Security Academic Alliance (SACSAA) (2011). *Homepage*. Available: http://www.cyberaware.org.za

South West Grid for Learning Trust (SWGfL). (2010). *Homepage*. Available:

https://swgfl.org.uk/ [Accessed: 23 September 2019].

Srivastava, J.S. (2017). Cybercrime: Kids as soft targets. *International Journal of Innovative Computer Science and Engineering*, 4(1):31–36.

Stone, K. (2013). *Keeping children and young people safe online: balancing risk and opportunity*. (February), 1–8. Retrieved from http://www.eastrenfrewshire.gov.uk/CHttpHandler.ashx?id=11003&p=0

Storypark. (2018). *Document and support children's learning, together*. Available: Storypark.com. [Accessed: 29 November 2018].

Symantec. (2013). *2013 Norton Report.* Available: https://www.symantec.com/content/en/us/about/presskits/b-norton-report-2013-south-africa.pdf [Accessed: 13 November 2019].

Biggs, J., & Tang, C. (2011). *Teaching for quality learning at university* (4th ed). Maidenhead, Berkshire, England: Open University Press/McGraw-Hill.

Vlasceanu, L., Grunberg, L., & Parlea, D. (2007). *Quality assurance and accreditation: A glossary of basic terms and definitions*. Bucharest: UNESCO.

Tekeni, L., Botha, R.A. & Thomson, K.L. (2016). A multi-faceted model for IP-based service authorization in the eduroam network. *South African Institute of Electrical Engineers, 106*(2), 83–92.

Third, A., Forrest-Lawrence, P. & Collier, A. (2014). *Addressing the CyberSafety Challenge :* Retrieved from http://apo.org.au/resource/addressing-cyber-safety-challenge-risk-resilience

Third, A., Forrest-Lawrence, P., Collier, A., Stranges, M.K.W., Ul Haq, S., Dunn, D.G., Lazarek, H. (2019). Social media: how can governments regulate it? *Proceedings Of the 4th International Conference on Information Systems Security and Privacy (ICISSP 2018), 50*(2018), 1–7. https://doi.org/10.1109/TIA.2014.2306979.

Tomhave, B.L. (2005). Alphabet soup: Making sense of models, frameworks, and methodologies. *Egov.Ufsc.Br*, 1–57. Retrieved from http://egov.ufsc.br/portal/sites/default/files/alphabet_soup.pdf%5Cnwww.secureconsulting.net/Papers/Alphabet_Soup.pdf%5Cnhttp://secureconsulting.net/papers-publications.html

United Nations Children's Fund (UNICEF). (2012). South African mobile generation Study on South African young people on mobiles. *Study on South African Young People on Mobiles*, 1–47.

Unisa. (2017). “Cyber Security Awareness”. [WWW Document]. URL http://eagle.unisa.ac.za/elmarie/ [Accessed 14 August 2017 8.14.17].

University of Pretoria. (2017), “African Centre of Excellence for Information Ethics”. [WWW Document]. African Cent. Excell. Inf. Ethics. URL http://www.up.ac.za/en/african-centre-of-excellence-for-information-ethics [Accessed 14 August 2017].

Valcke, M., De Wever, B., Van Keer, H. & Schellens, T. (2011). Long-term study of safe Internet use of young children. *Computers and Education*, *57*(1), 1292–1305. https://doi.org/10.1016/j.compedu.2011.01.010

Van Eemeren, F.H., & Grootendorst, R. (2004). *A systematic theory of argumentation: The Pragma-Dialectical Approach*. Cambridge: Cambridge University Press.

Van Niekerk, J.F. & Thomson, J.-L. (2010). Evaluating the Cisco Networking Academy Program's Instructional Model against Bloom's Taxonomy for the purpose of information security education for organizational end-users. In N. Reynolds & M. Turcsányi-Szabó (eds), *Evaluating the CNAP Instructional Model against Bloom's Taxonomy* (pp. 412-423). IFIP.

Von Solms, S. & Fischer, R. (2017). Digital Wellness : Concepts of Cybersecurity Presented Visually for Children. (Haisa), 156–166.

Von Solms, R. & Van Niekerk, J. (2013). Information security culture: A management perspective. Computers & Security, 29(1):476–486.

Von Solms, R. & Von Solms, S. (2015). Cyber Safety Education in Developing Countries. *Journal of Systemics, Cybernetics and Informatics*, 13(2):14–19.

Von Solms, S. & Von Solms, R. (2014). Towards cyber safety education in primary schools in Africa. In *Proceedings of the Eighth International Symposium on Human Aspects of Information Security and Assurance* (HAISA 2014) (pp. 185–197).

Walliman, N. (2010). *Research methods: The basics*. London/New York: Routledge.

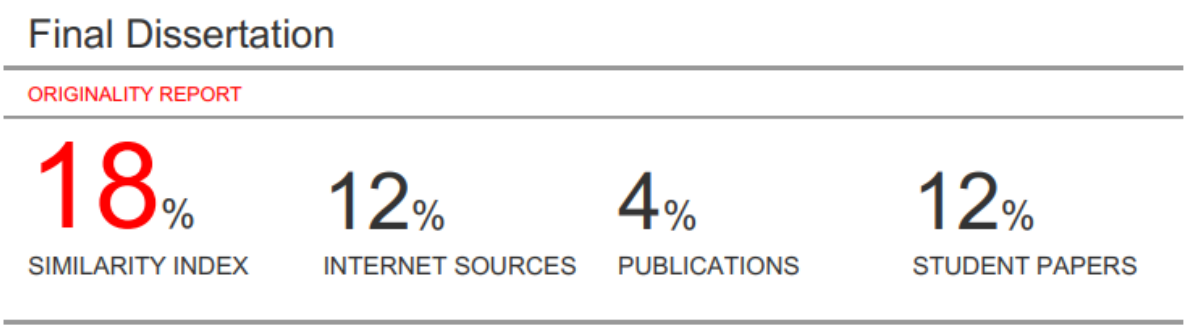
Williams, C. (2007). Research methods. *Journal of Business & Economic Research*, 5(3):65–72.

Wolfpack. (2013). *The South African Cyber Threat Barometer.* Available: http://www.cyanre.co.za/wp-content/uploads/2016/08/cyber-threat-barometer.pdf [Accessed: 24 July 2019].

Writer, S. (2018). *Here's how many South African schools don't have the internet or a computer lab – and what it will cost to fix the problem.* Retrieved from Bussiness Tech: https://businesstech.co.za/news/internet/259171/heres-how-many-south-african-schools-dont-have-the-internet-or-a-computer-lab-and-what-it-will-cost-to-fix-the-problem/. [Accessed 24 July 2019]

Zucule de Barros, J.M., & Lazarek, H. (2018). A Cyber Safety Model for Schools in Mozambique, (Icissp), 251–258. https://doi.org/10.5220/0006573802510258

TURNITIN REPORT



APPENDIX A – Identified Cybersafety Threats and Global Educational Initiatives

Cybersafety Threat Topics	ThinkUKnow (UK)	Safer internet Centre (UK)	UKCCIS (USA)	Stop.Think. Connect (USA)	Cybersafety K-12 (USA)	Internet Safety (Canada)	e-safety (Australia)	Netsafe (New Zealand)	Total sources n=8
Cyberbullying	×		×	×	×	×	×	×	7
Sharing information	×	×			×	×	×		5
Social networking	×					×	×	×	4
Sexting			×		×	×		×	4
Online grooming/predators			×	×	×			×	4
Protecting Passwords	×					×	×		3
Identity theft				×		×	×		3
Online pedestrian		×		×		×			3
Online Privacy	×						×	×	3
Inappropriate content			×		×			×	3
Copyrights						×	×		3
Online addiction	×							×	2
Games addiction							×	×	2
Online etiquette	×							×	2

Meeting strangers online		×					×		2
Tell an adult that you are online	×	×							2
Hacking			×						1
Ransomware					×				1
Viruses						×			1
Cyberstalking						×			1
Free downloads							×		1

APPENDIX B – Identified Cybersafety Threats and African Educational Initiatives

Cybersafety threat topics	National Computer board (Mauritius)	Cyberteq (Rwanda)	A Cyber Safety Model for Schools in Mozambique, 2018	Total sources n=3
Cyberbullying	×	×	×	3
Online etiquette	×		×	2
Social networking		×	×	2
Identity theft		×	×	2
Online grooming/predators		×		1
Sharing information		×		1
Inappropriate content	×		×	2
Meeting strangers online	×			1
Online addiction	×			1
Sexting			×	1
Online Privacy			×	1

APPENDIX C – Identified Cybersafety Threats and South African Educational Initiatives

Cybersafety threat topics	Kritzinger & Padayachee, 2007	Kritzinger & Padayachee, 2013	DBE, 2010	Kritzinger, 2015	Kritzinger, 2017b	Von Solms & Fischer, 2017	Kritzinger, 2011
Cyberbullying	×	×	×	×	×	×	×
Inappropriate content	×	×	×	×	×		×
Identity theft	×	×	×	×	×		×
Sexting	×		×	×	×		
Sharing information						×	
Meeting strangers online			×			×	×
Online Privacy						×	
Games addiction					×		×
Copyrights			×				×
Cyberstalking	×						×
Online addiction			×		×	×	
Protecting Passwords						×	
Social networking					×		

Online etiquette						×	×
Tell an adult that you are online							
Viruses/Phishing						×	×
Online grooming/predators							×
Hacking						×	×

Identified Cybersafety Threats and South African Educational Initiatives (continued)

Cybersafety threat topics	Kritzinger, 2017a	Reid & Van Niekerk, 2014	Niekerk, Thomson, & Reid, 2013	Von Solms & Von Solms, 2015	Von Solms & Von Solms, 2014	De Lange & Von Solms, 2012	**Total of Sources n=13**
Cyberbullying	×		×	×	×	×	12
Inappropriate content	×			×		×	9
Identity theft	×					×	8
Sexting	×			×		×	7
Sharing information	×		×		×	×	5
Meeting strangers online			×		×		5
Online Privacy	×		×	×			4
Games addiction	×				×	×	5
Copyrights			×			×	4
Online etiquette	×						3
Viruses		×					3
Cyberstalking	×					×	4
Online addiction						×	4
Protecting Passwords		×	×				3
Social networking	×	×					3

Online grooming/predators							2
Tell an adult that you are online			×		×		2
Cookies/Malware				×			2
Phishing scams	×						1
Hacking							1
Digital footprint							1

PROOF OF EDITING CERTIFICATE
TO WHOM IT MAY CONCERN

Language editing

I, Jeanne Enslin, acknowledge that I did the language editing of **Lean Kucherera's** dissertation submitted in fulfilment of the requirements for the degree of Master of Information Technology, at Nelson Mandela University.

The title of the dissertation is:

A cybersafety educational framework
for primary school learners in South Africa.

Detailed feedback of all the language editing done has been provided to Lean in writing and is evident in the dissertation in track changes and with comments – sent to her on 13 January 2020. The quality of the final document, in terms of language, formatting and references, remains the student's responsibility.

Jeanne Enslin

Language editor
082 696 1224

Technical editing

I, Ronel Gallie, acknowledge that I did all aspects of the technical formatting and all references of **Lean Kucherera's** dissertation submitted in fulfilment of the requirements for the degree of Master of Information Technology, at Nelson Mandela University. Detailed feedback about the work done has been provided to Lean – on 13 January 2020.

Ronèl Gallie

Technical editor
084 7780 292