



NAMIBIA UNIVERSITY
OF SCIENCE AND TECHNOLOGY

FACULTY OF COMPUTING AND INFORMATICS
SCHOOL OF INFORMATICS, JOURNALISM, AND MEDIA TECHNOLOGY
DEPARTMENT OF INFORMATICS

**CO-DESIGNING A CYBERSECURITY PRACTICES FRAMEWORK FOR UNDERSERVED RURAL
COMMUNITIES**

By
Gabriel Tuhafeni Nhinda
(200742175)

Submitted in fulfilment of the requirements for the degree

Doctor of Philosophy in Informatics
in the

Department of Informatics

at the

NAMIBIA UNIVERSITY OF SCIENCE AND TECHNOLOGY

Supervisor: Professor Fungai Bhunu Shava

Date Submitted: June 2024

DECLARATION

I, GABRIEL TUHAFENI NHINDA, student number 200742175, hereby declare that the work contained in the thesis for the degree DOCTOR OF PHILOSOPHY IN INFORMATICS, entitled:

“CO-DESIGNING A CYBERSECURITY PRACTICES FRAMEWORK FOR UNDERSERVED RURAL COMMUNITIES” is my original work and I have not previously in its entirety or part submitted it at any university or other higher education institution for the award of a degree.

I further declare that all sources used or referred to have been acknowledged. I am aware of the Namibia University of Science and Technology’s policy on plagiarism, and I have taken every precaution to comply with the regulations.

Any findings, opinions, recommendations, or assertions expressed in this research are those of the author and do not necessarily reflect the views of the aforementioned institution.

Signature:



Date:

30 June 2024

RETENTION AND USE OF THESIS

I, GABRIEL TUHAFENI NHINDA being a candidate for the degree of DOCTOR OF PHILOSOPHY IN INFORMATICS Accept the requirements of the Namibia University of Science and Technology relating to the retention and use of thesis deposited in the Library and Information Services. In terms of these conditions, I agree that the original of my thesis deposited in the Library and Information Services will be accessible for purposes of study and research, in accordance with the normal conditions established by the Librarian for the care, loan or reproduction of thesis.

Signature:



Date:

30 June 2024

DEDICATION

This thesis, I dedicate to God, my parents, my wife and daughter, and the communities without whom this work would not have been possible.

ACKNOWLEDGEMENTS

I thank God the provider of and for ALL, without whom this journey would never have started nor come to this triumphant conclusion. I thank Him for the anointing, blessing of life, and the good health He has given unto me.

I would like to thank my supervisor, Prof Fungai Bhunu Shava, for her guidance and mentorship; and for believing in me even when I faltered.

To my examiners, thank you for the great comments on improving this timely work.

I thank my family, and my parents, thank you for investing in my education, and believing in my dreams even when they did not make sense. Dad for always pushing for excellence, Mom for always having a kind word and reassurance. My wife for believing in my vision and loving me unconditionally, for holding my hand as I pressed that submit button several times. I thank my wife for holding the fort down as I complete this work. My daughter for being the ray of sunshine even when it seemed gloomy. For the infectious laugh and inquisitive mind. To my sister, for always reminding me of what having a support system is all about, al while being a wife, mother, and daughter, you always stepped up and made me remember my childhood dreams.

I thank my colleagues for always checking up on me and constantly offering to be sounding boards. I also thank my fellow postgraduate students for their constant encouragement to push past my fears and worries and for walking this journey with me.

My expert reviewers, I thank you for the critical engagement with my outputs, ensuring that the communities that this research problem faces enjoy equitably safe Internet access.

Most importantly, I would like to thank the community of the Engela Constituency, who continues to teach me so much and I know our collaboration will be long-lived.

I thank Mobile Telecommunications Company Ltd (MTC) for the financial support to conduct fieldwork and the Namibia University of Science and Technology (NUST) for the staff development scholarship.

ABSTRACT

The increasing ubiquity of digital technologies and the Internet has resulted in societies becoming heavily dependent on them for communication, healthcare, education, business operations, and social interaction. While digital transformation promises many benefits, it also presents significant challenges, particularly in ensuring safe and secure online participation. Cybersecurity, as a critical enabler of digital trust, is essential for inclusive and resilient digital societies. However, in underserved rural communities, especially in the Global South, cybersecurity practices remain largely unfamiliar due to limited telecommunications infrastructure, socio-economic inequality, and low digital literacy. This study addresses this gap by co-designing a cybersecurity practices framework with and for underserved rural communities. Rooted in a multidisciplinary approach, the research integrates elements of human-computer interaction (HCI), community engagement, and behavioural insights. A qualitative methodology was employed, using co-design sessions, focus group discussions, and interviews, to understand community-specific perceptions and practices of cybersecurity. The study draws on indigenous philosophies of Ubuntu and Uushiindaism to contextualise security as a communal, ethical, and relational construct. The research was conducted in the Engela Constituency within the OuKwanyama Kingdom, Namibia, during the COVID-19 pandemic—a period that revealed new socio-digital vulnerabilities. Data were gathered in four villages, primarily in Oshikwanyama, with English and Portuguese used as supporting languages. Thematic analysis revealed how the pandemic reshaped rural community compositions, with an influx of displaced students and unemployed urban workers returning to the villages, creating both opportunities and tensions around digital access and safety. A co-designed community engagement protocol emerged from collaboration with local headmen, political figures, and community members. This protocol, informed by local norms, provided the foundation for the development of a cybersecurity framework that is locally grounded yet globally informed. Anchored in the design science research paradigm, the final framework comprises five interconnected components: people and community; international standards; a co-designed community engagement protocol; co-designed cybersecurity practices; and the national regulatory and policy environment. The framework was evaluated through a two-

pronged process: expert focus groups (ex-post) and community-based co-design sessions (ex-ante and ex-post). Evaluation centred on ecological utility—ensuring contextual relevance, cultural fidelity, sustainability, comprehensibility, and local ownership. The study further maps key actors and relationships influencing cybersecurity practices in rural contexts, including interactions with national agencies, community policing units, local radio, and ministries responsible for awareness and legislation. This research contributes to a more inclusive understanding of cybersecurity by recognising the socio-cultural dynamics that shape digital safety in underserved communities. It bridges the gap between globally dominant cybersecurity paradigms and the lived realities of rural African users. The framework empowers communities to engage confidently with technology, facilitates digital access to essential services, promotes skills transfer through seasonal resident engagement, and supports the preservation of indigenous languages. For policymakers, developers, and educators, it offers actionable insights into designing secure, contextually appropriate technologies for the margins, while ensuring broader applicability across user groups

Keywords: Co-design, cybersecurity practices, underserved rural communities, community engagement, afro-centric

LIST OF PUBLICATIONS

Four peer-reviewed publications (1 Journal Paper, 2 full conference papers, and 1 extended abstract) emanated from this research study. Within this thesis document, they are presented in Appendix D. They are also presented below according to the latest year of publication. Paper IV problematises the research area and positions participatory methods as critical for cybersecurity research within underserved communities in Africa, therefore proposing a methodological approach and grounding for this research study. Paper III was an extended abstract presented on the approach used to co-create cyber-secure practices for underserved communities in Africa, with a focus on Northern Namibia (the study site). Paper II elucidated on the existing cybersecurity practices of underserved communities under study, and paper I is a Journal publication that presents a co-designed community engagement protocol, which was key for the success of this research study.

All the papers below present various components of the co-designed cybersecurity practices framework.

Journal Paper

- I. Nhinda, G. T., & Bhunu Shava, F. (2023). Co-CEP: A co-designed community engagement protocol as a catalyst for cybersecurity research in Africa: The case of northern Namibia. *Journal of Information and Optimization Sciences*, 44(3), 475–492. <https://doi.org/10.47974/jios-1407>

Peer-reviewed Conference Papers

- I. Nhinda, G. T., & Bhunu Shava F. (2023). Cybersecurity Practices of Rural Underserved Communities in Africa: A Case Study from Northern Namibia. In *2023 International Conference on Artificial Intelligence, Big Data, Computing and Data Communication Systems (icABCD)*, Durban, South Africa, 2023, (pp. 1-7). Doi: 10.1109/icABCD59051.2023.10220449. IEEE

- II. Nhinda, G. T. & Bhunu Shava, F. (2022). *Using Co-Design to craft Cybersecurity secure practices for rural communities in Africa: A case study from Northern Namibia* [Conference presentation extended abstract]. Cybersecurity Capacity Building: The Global Constellation Annual Conference, Cape Town, South Africa.
<https://c3sa.co.za/wp-content/uploads/2022/11/THE-GLOBAL-CONSTELLATION-ANNUAL-CONFERENCE-2.pdf>
- III. Nhinda, G. T., & Bhunu Shava, F. (2021, November). Towards the use of Participatory Methods in Cybersecurity research in rural Africa: A grassroots Approach. In *2021 3rd International Multidisciplinary Information Technology and Engineering Conference (IMITEC)* (pp. 1-7). IEEE.

LIST OF TABLES

Table 1.1: The relationship between the research questions, data collection technique, and the expected outcomes	11
Table 2.1: The MINDSPACE framework for behaviour change.	38
Table 2.2: Legislation, policies, and strategies that enable or constrain cybersecurity.	1
Table 3.1: Philosophical assumptions and their descriptions	4
Table 3.2: Popular paradigms in computing.....	6
Table 3.3: Design science research principles	10
Table 3.4: Research questions and data collection methods with their respective outcomes	24
Table 4.1: Interviewee profiles.....	39
Table 4.2: Overall focus group and co-design session participants.....	46
Table 5.1: Assumed role of the main components of the proposed framework	81
Table 5.2: Cybersecurity practices themes in underserved rural communities	92
Table 6.1: Design Science Research Guidelines (Hevner et al., 2004).....	101
Table 6.2: Focus group framework evaluation demographics	108
Table 6.3: Explanation of the framework symbols.....	115

LIST OF FIGURES

Figure 1.1: Adapted design science research.	8
Figure 2.1: NIST cybersecurity framework components	34
Figure 2.2: NIST functions and categories for organisational cybersecurity and risk management	35
Figure 2.3: NIST framework implementation tiers for risk management	36
Figure 2.4: NIST framework profiles.....	37
Figure 3.1: Factors that affect paradigm choice.....	8
Figure 3.2: Three cycle design science research process	13
Figure 3.3: Design science research steps.....	14
Figure 3.4: The DSRM process model.....	15
Figure 3.5: Participatory research approach for cybersecurity research in Africa	16
Figure 3.6: Adapted design science research process model for the current study	19
Figure 3.7: Framework evaluation approach	20
Figure 3.8: Case study process	22
Figure 3.9: Data collection process	23
Figure 3.10: Five analytic phases approach.....	27
Figure 4.1: Case study setting	35
Figure 4.2: Data collection process	37

Figure 4.3: Interview in Onghala village under a tree	41
Figure 4.4: Interview underway in the Ouhongo Uakondja village under a tree in the middle of the Omahangu field.....	42
Figure 4.5: Interview in Engela village within the homestead of the senior village headman.	43
Figure 4.6: Co-designed community engagement protocol (see Appendix D.1 for further reading)	53
Figure 5.1: Adaptation of the design science research cycles	77
Figure 5.2: 8-Steps in building a conceptual framework.....	78
Figure 5.3: Framework design steps followed for CCSPF-4-URC.....	79
Figure 5.4: Individual and community component	82
Figure 5.5: Existing frameworks in cybersecurity.....	87
Figure 5.6: Information flow within communities for cybersecurity research.....	88
Figure 5.7: Co-designed community engagement protocol.....	91
Figure 5.8: Co-designed cybersecurity practices framework for underserved rural communities- CCSPF-4-URC	98
Figure 6.1: Framework evaluation falls within the rigour and relevance cycles of DSR.....	104
Figure 6.2: Framework evaluation approach	107
Figure 6.3: CCSPF-4-URC framework.....	117

LIST OF ABBREVIATIONS

CCSPF-4-URC	Co-design Cybersecurity Practices Framework for Underserved Rural Communities
CRAN	Communications Regulatory Authority of Namibia
DSR	Design Science Research
HCI	Human-Computer Interaction
HCISec	Human-Computer Interaction Security
ICT	Information Communication Technology
IoT	Internet of Things
IS	Information System
IT	Information Technology
ITU	International Telecommunication Union
MICT	Ministry of Information and Communication Technology
MTC	Mobile Telecommunications Limited - Namibia
MTN	Mobile Telephone Networks
NGO	Non-Governmental Organisation
NIST	National Institute of Standards and Technology
NIST	National Institute of Standards and Technology
NSA	Namibia Statistics Agency
NUST	Namibia University of Science and Technology
PMT	Protection Motivation Theory RESEARCH
TN Mobile	Telecom Namibia Mobile
TPB	Theory of Planned Behaviour
UCD	User-Centred Design
UN	United Nations

TABLE OF CONTENTS

DECLARATION.....	I
DEDICATION	II
ACKNOWLEDGEMENTS	IV
ABSTRACT.....	VI
LIST OF PUBLICATIONS	VIII
LIST OF TABLES.....	X
LIST OF FIGURES.....	XI
LIST OF ABBREVIATIONS	XIII
TABLE OF CONTENTS.....	XIV
1. CHAPTER 1: RESEARCH INTRODUCTION	1
1.1 INTRODUCTION	1
1.2 RESEARCH BACKGROUND	2
1.3 PROBLEM STATEMENT.....	4
1.4 RESEARCH QUESTIONS.....	5
1.5 RESEARCH OBJECTIVES	5
1.6 METHODOLOGY	6
1.6.1 Research Philosophy	6
1.6.2 Research Approach	7
1.6.3 Research Strategy	7
1.6.4 Data Collection	10
1.6.5 Population	10
1.6.6 Sampling Strategy	10
1.6.7 Data Analysis	13
1.7 ETHICAL CONSIDERATIONS	13
1.8 DELINEATIONS AND LIMITATIONS OF THE STUDY	14

1.8.1 DELINEATIONS.....	14
1.8.2 LIMITATIONS	14
1.9 CONTRIBUTION OF THE RESEARCH	14
1.10 THESIS CHAPTER BREAKDOWN	15
2. CHAPTER 2: THEORETICAL FRAMEWORK	18
2.1 INTRODUCTION	18
2.2 AFROCENTRICITY IN AFRICAN PHILOSOPHY	18
2.2.1 African Philosophy	18
2.2.2 Afro-centricity	20
2.3 UNDERSERVED RURAL COMMUNITIES	24
2.3.1 Defining rural communities.....	24
2.3.2 Why rural communities.....	26
2.3.3 Underserved communities	27
2.3.4 Structure of rural communities in Namibia.....	29
2.4 SERVICES IN UNDERSERVED RURAL AREAS	30
2.4.1 Types of services offered in rural areas	30
2.4.2 Factors impacting the cost-of-service delivery in rural areas	31
2.5 CYBERSECURITY PRACTICES FRAMEWORKS	32
2.5.1 Cybersecurity	32
2.5.2 Cybersecurity best practices frameworks	33
2.6 PERSONAL CYBERSECURITY PRACTICES	41
2.7 HUMAN-COMPUTER INTERACTION.....	42
2.7.1 Participatory design methods	42
2.7.2 Co-design and co-creation	43
2.7.3 HCI security.....	44
2.8 BEHAVIOURAL THEORIES IN HUMAN-COMPUTER INTERACTION SECURITY	44
2.8.1 Protection Motivation Theory.....	45
2.8.2 Theory of Planned Behaviour.....	45
2.8.3 The Cultural Theory of Risk	46
2.8.4 Cultural Tightness-Looseness Theory.....	47

2.9 REVIEW OF ICT EFFORTS IN NAMIBIA IN FAVOUR OF CYBERSECURITY.....	48
2.9.1 Cyber infrastructure	48
2.9.2 Access to affordable broadband	50
2.9.3 Legislation and compliance efforts	50
2.10 CHAPTER SUMMARY.....	1
3. CHAPTER 3: RESEARCH METHODOLOGY	3
3.1 INTRODUCTION	3
3.2 RESEARCH PARADIGM AND PHILOSOPHY	3
3.2.1 Various research paradigms explained	5
3.2.2 Determinants of paradigm choice.....	8
3.3 RESEARCH PARADIGM AND PHILOSOPHY APPLICABLE TO THE CURRENT STUDY.....	8
3.4 RESEARCH STRATEGIES	9
3.5 DESIGN SCIENCE RESEARCH	10
3.5.1 Design science research models.	12
3.5.2 Methodology used in this study.....	15
3.5.3 Design science research model used in this study	18
3.6 CASE STUDY AND DATA COLLECTION METHODS	20
3.6.1 Case studies.....	20
3.6.2 Data collection methods	23
3.6.3 Data analysis	25
3.7 POPULATION	27
3.8 SAMPLING STRATEGY	28
3.9 CASE SITE.....	29
3.10 ETHICAL CONSIDERATIONS	30
3.11 CHAPTER SUMMARY.....	31
4. CHAPTER 4: DATA COLLECTION AND ANALYSIS.....	33
4.1 INTRODUCTION	33
4.2 CONTEXTUALISATION OF CASE SITE	33

4.3 DATA COLLECTION PROCEDURE	35
4.4 DATA COLLECTION EXPERIENCE	38
4.4.1 Interviews.....	38
4.4.2 Focus groups and co-design sessions.....	43
4.5 FINDINGS PRESENTATION.....	46
4.6 PRESENTATION OF THE EIGHT THEMES.....	49
4.6.1 Theme 1: Co-designed community engagement protocol.....	49
4.6.2 Theme 2: Existing security practices	53
4.6.3 Theme 3: Technology usage patterns and device ownership	53
4.6.4 Theme 4: Online security practices (cyber-hygiene).....	62
4.6.5 Theme 5: Current cybersecurity practices	66
4.6.6 Theme 6: Legislation for cybersecurity	71
4.6.7 Theme 7: Telecentres.....	71
4.6.8 Theme 8: Community peer education	72
4.7 CHAPTER SUMMARY.....	73
5. CHAPTER 5: CO-DESIGNED CYBERSECURITY PRACTICES FRAMEWORK FOR	
UNDERSERVED RURAL COMMUNITIES (CCSPF-4-URC)	75
5.1 INTRODUCTION	75
5.2 CCSPF-4-URC FRAMEWORK DEVELOPMENT	75
5.2.1 Step 1 – Extensive reading and categorising of selected data	79
5.2.2 Step 2 – Identifying and naming concepts	80
5.2.3 Step 3 – Integrating the concepts	94
5.2.4 Step 4 – Validating the conceptual framework.....	96
5.2.5 Step 5 - Rethinking the framework.	96
5.3 PROPOSED FRAMEWORK.....	96
5.4 CHAPTER SUMMARY.....	98
6. CHAPTER 6: EVALUATION OF THE CCSPF-4-URC	100
6.1 INTRODUCTION	100
6.2 CCSPF-4-URC FRAMEWORK EVALUATION	100

6.3 EVALUATION RESULTS	106
6.3.1 Ex-ante framework component evaluation and validation through co-design sessions	106
6.3.2 Ex-post framework evaluation through expert focus group discussions	107
6.4 REFINED CCSPF-4-URC FRAMEWORK	114
6.5 FRAMEWORK LIMITATIONS	118
6.6 CHAPTER SUMMARY.....	119
7. CHAPTER 7: RESEARCH CONCLUSION.....	120
7.1 INTRODUCTION	120
7.2 RESEARCH OVERVIEW.....	120
7.3 CONTRIBUTION TO THE BODY OF KNOWLEDGE	124
7.4 LIMITATIONS OF THE STUDY	127
7.5 REFLECTIONS ON THE STUDY	128
7.5.1 Scientific reflection.....	128
7.5.2 Methodological reflection.....	129
7.5.3 Personal reflection	130
7.6 FUTURE WORK.....	131
7.7 CONCLUDING REMARKS	132
REFERENCES.....	133
APPENDICES.....	I
APPENDIX A: ETHICAL CLEARANCE	I
APPENDIX B: RESEARCH PERMISSION FROM CLUSTER HEADMAN	II
APPENDIX C: PERMISSION FROM CONSTITUENCY COUNCILLOR.....	IV
APPENDIX D.1: EXTRACT FROM JOURNAL PAPER I	V
APPENDIX D.2: EXTRACT FROM CONFERENCE PAPER II	VI
APPENDIX D.3: EXTRACT FROM CONFERENCE EXTENDED ABSTRACT III	VII
APPENDIX D.4: EXTRACT FROM CONFERENCE PAPER IV	VIII

APPENDIX E: COMMUNITY MEMBERS' INFORMED CONSENT FORM.....	IX
APPENDIX F: CO-DESIGN WORKSHOP DATA COLLECTION INSTRUMENT	XI
APPENDIX G: INTERVIEW GUIDE FOR COMMUNITY MEMBERS.....	XII
APPENDIX H: INTERVIEW GUIDE FOR THE MINISTRY	XVI
APPENDIX I: MINISTRY INFORMED CONSENT FORM.....	XVII
APPENDIX J: FOCUS GROUP OF EXPERTS EVALUATION TOOL.....	XVIII
APPENDIX J: EDITORS LETTER.....	XX

CHAPTER 1: RESEARCH INTRODUCTION

This Chapter introduces the research study. It makes the case and presents the research gap that exists. In this Chapter the background, research problem, research questions, objectives and the significance of this study are presented.

1.1 INTRODUCTION

Technology has become a critical part of our daily lives and has permeated personal boundaries past thought impenetrable. To this effect, mobile and pervasive technologies such as mobile devices enabled with various actuators and sensors, web 2.0, Internet technology, and Internet of Things (IoT) devices have made it into our daily lives (Prasad & Rohokale, 2020). These technologies enable users to perform tasks from the comfort of their homes. Internet technology has opened new opportunities as well as new challenges for individuals. One such opportunity is the ability to connect and transact online from nearly anywhere. Albeit all the opportunities, challenges such as the availability of mobile broadband, the cost of Internet-enabled devices, and the cost of mobile data persist in developing countries (Hasbi & Dubus, 2020). Among other challenges, the most alarming is the online safety of technology users.

According to the International Telecommunications Union (2022), in 2016, Namibia had 31% of the population using the Internet, and 62.2% in 2022 for individuals aged 15 and above. This statistic shows that the number of Internet users in Namibia doubled within a space of 6 years. The same report indicates that 100% of the entire population has been covered by a mobile cellular network. The data by the ITU is an estimate based on universal and meaningful connectivity factor. The universal and meaningful connectivity seeks to have internet users use the experience satisfying, safe, productive, and enriching online experiences (International Telecommunications Union, 2022). However, when it comes to online user safety, uninformed technology users can be seen as the low hanging fruits for cyber-attacks by cybercriminals (Kritzinger & Solms, 2013; Sultan, 2020). Over the years, a consensus has been reached that the weakest link within a cybersecurity programme is the human element/factor, more specifically the end-users (Bhunu Shava & Van Greunen, 2014; El Hajal et al., 2021; Gcaza & von Solms, 2017;

Kainda et al., 2010; Mathiasen & Bodker, 2008; Quayyum & Freberg, 2023; Zimmermann & Renaud, 2019).

Even though nations/states have invested in cyber defences and offense capabilities, minimal efforts have been directed at the underserved communities (Sultan, 2020). This populace is disproportionately vulnerable to cyber-crime and may not even know when they have become victims (Sultan, 2020). From a technical perspective, there exists a plethora of interventions that aim to mitigate, prevent, and circumvent any attacks that an individual might experience online. These interventions, however, often fall short as they aim at targeting users' change in behaviour Mathiasen & Bodker (2008) and are not modelled with and for users' ways of being. Human-computer interaction studies have proven that involving users at the end of technological interventions does not yield adoptability (Nandi et al., 2016), nor encourage the confidence of users (Marufu & Sibanda, 2013). West (2008) argues that despite security training, there remains a pocket of users that often find it difficult to understand technical security mechanisms (Gcaza & von Solms, 2017). The users thereby continue failing to recognise security risks (Ekandjo et al., 2018) and have auxiliary trouble with information meant to cue them towards secure online behaviour. The current approaches are thus not effective along all fronts and for all people to be able to secure their online experiences.

1.2 RESEARCH BACKGROUND

In most developing countries, cybersecurity programmes and awareness initiatives focus on knowledge transfer by experts to rural communities (Grobler, Dlamini, et al., 2011). Though these approaches are intended to fortify the knowledge base of rural communities and usually underserved communities about cybersecurity and best practices to secure themselves in the cyberspace, they often do not have long-lasting results (Bada et al., 2015). Underserved communities are plagued with intermittent connectivity to networks and lacklustre Internet availability (Dlamini et al., 2016; Grobler, Dlamini, et al., 2011; Grobler, van Vuuren, et al., 2011; van Vuuren et al., 2012). Furthermore, there exists digital skills drain by the youth leaving rural areas in search of education and job opportunities in cities (Fröhlich et al., 2018). This leaves behind old people and children, who may not have the requisite English level knowledge to

understand security messaging nor have the digital skillsets to secure themselves online when using technological devices (Fröhlich & Peters, 2017).

The Namibia Statistics Agency (NSA) preliminary population and housing census report for 2023 indicates that Namibia has a population of 3 022 401, which represents a 909,324 population increase since the last census which was conducted in 2011 (Namibia Statistics Agency, 2024). In 2011 approximately 52.1% of the population resided in rural areas, the 2023 census found that there was an increase in the rural population by 26.3% between the two census years bringing the total rural population to 1 527 409 (Namibia Statistics Agency, 2017b, 2024; Republic of Namibia, 2017). The national census data analysis is not complete, additional details regarding digital device ownership, and Internet access, will be released in a Census Basic Report within the third quarter of the 2024/25 financial year, with a tentative release date of October 2024 (Namibia Statistics Agency, 2024). Therefore, further contextualisation of the research background will rely on the 2011 census data.

The Namibia Statistics Agency (2017a) reported that 94% of households in Namibia have access to mobile phones and 29.2% have access to the Internet. Of the 29.2% that have Internet access, only 19.7% reside in rural areas while 80.3% reside in urban areas. The Namibia Statistics Agency (NSA) reports that approximately 79.2% of Namibians older than 15 years of age own a mobile phone, of these 88% are based in urban areas as opposed to 69.9% in rural areas (Namibia Statistics Agency, 2017b). Furthermore, the NSA reports that only 11.8% of the rural population owns smartphones, while 73.1% and 15.1% own basic phones and feature phones respectively. Additionally, 92.7% of the population that resided in rural areas had not used the Internet within the last 3 months of this report. Of those that did have Internet access, only 2.8% used it on their own mobile phones and 3.1% on a variety of mobile devices. The Communication Regulatory Authority of Namibia (CRAN) reported that as of 2019 there was an overall mobile penetration rate of 120%, however, it does not provide updated figures on rural and urban mobile penetration rates (Communications Regulatory Authority of Namibia, 2019). Additionally, the penetration rate has been reported as such since 2016. Conversely, CRAN concedes that “availability and access to telecommunication services in rural areas remains a challenge, largely

due to uneven access to electricity and the high unit cost of rolling out Information Communication Technology (ICT) infrastructure throughout a vast geographic area” (Communications Regulatory Authority of Namibia, 2019, p. 69).

Namibia has three major Telecommunication companies that offer mobile networking services, namely, Telecom Namibia Mobile (TN Mobile), Mobile Telecommunications Networks (MTN), and Mobile Telecommunications Limited (MTC). Of these, MTC claims that it has a 91% market share and a 97% mobile network coverage of Namibia’s population (Mobile Telecommunications Limited, 2019). Even though it seems the digital divide is shrinking based on the statistics presented above in terms of an increase in the number of mobile phone users and coverage claimed by the leading Telecommunications company, there still exists the issue of lack of network access and infrastructure in most rural areas. As this digital divide shrinks, a new one has emerged, “...between those who can manage and mitigate potential cybersecurity threats and those who cannot” (Sultan, 2020).

1.3 PROBLEM STATEMENT

The world is in the thick of the 4th Industrial Revolution and on the brink of the 5th Industrial Revolution (Pathak et al., 2019). Technology and security are evolving at an exponential rate. However, there are pockets of marginalised communities whose access to the internet and technology is not well understood, especially in Namibia. More so, the internet experiences of those accessing it in underserved communities are not known as there are no publications on this. As such, existing models and frameworks are not designed to address their mental models hence, they are not applicable to educate and create awareness about secure cyber practices without understanding the norms in these setups first. Thus, underserved and rural communities are vulnerable to online exploitation, and this is further compounded by being the weakest link in the entire technology ecosystem. Currently, there is no evidence in the existing literature that aims to understand the security practices of underserved populations in rural areas.

Underserved communities are usually rich in contextual factors, such as cultural beliefs, habits, and natural behaviours (Fröhlich et al., 2018). As such, for any interventions to be successful, a

co-design approach needs to be taken. Co-designing ensures that the underserved community's contextual factors are taken into consideration as they relate to security and perceptions of risks and dangers (Bada et al., 2015; Fröhlich et al., 2018). The present study uses the co-design approach to design a secure practices framework, to increase the chances of rural underserved communities embodying secure practices when utilising technology and when accessing cyberspace.

1.4 RESEARCH QUESTIONS

Main research question

How can a cybersecurity best practices framework be co-designed with underserved rural communities?

Sub-research questions

1. What are the current security practices for underserved rural communities?
2. What risks exist for underserved rural communities as they interact with technology?
3. What are the best practices for a secure online experience for underserved rural communities?
4. Which components are required for the co-design of a cybersecurity best practice framework for underserved rural communities?
5. How can a cybersecurity best practices framework for underserved rural communities be evaluated?

1.5 RESEARCH OBJECTIVES

Main research objective

To co-design a cybersecurity best practices framework for underserved rural communities.

Sub-research objectives

1. To determine current security practices of underserved rural communities.

2. To investigate possible risks that exist in the current technology use of underserved rural communities.
3. To evaluate online security best practices for underserved rural communities.
4. To identify components required for the development of a cybersecurity best practice framework for underserved rural communities.
5. To evaluate the cybersecurity best practices framework for underserved rural communities.

The next section discusses relevant literature around cybersecurity frameworks as well as predominant behavioural models embodied in these frameworks.

1.6 RESEARCH METHODOLOGY

This section elucidates the methodology that guided the attainment of the research objectives, through data collection, data analysis, interpretation of the study findings and eventually answering the research questions. It begins with philosophical underpinnings, research approaches, strategies, and choices.

1.6.1 Research Philosophy

Research presents an opportunity to understand the nature of a problem. It is therefore imperative that any research study infers based on the philosophical paradigm it follows to determine the validity of the epistemological understanding of the problem (Oates, 2012). The two dominant philosophical paradigms are positivism and interpretivism (Cleven et al., 2009). According to Oates (2012), the positivist paradigm aims to study events without interacting with them. The positivist paradigm is not suitable for this study as it is based on the critical theory which assumes a singular realism (Yin, 2016). In this study, we took the interpretivism paradigm as we sought to understand user behaviours and risks when interacting with technology and co-designing a secure practices framework with an underserved rural community. This requires an in-depth understanding of practices and ways of being by allowing researchers to be active social

actors (Rowley, 2002). This philosophical stance is key to understanding the phenomenon that makes the reality that is socially constructed by different people within a community.

1.6.2 Research Approach

In this study, we used a combination of deductive and inductive qualitative research approaches within a case study design. The deductive approach moves from a theory-based approach, allowing theory to determine the data to be collected (Yin, 2016), allowing users to extract Afrocentric tenets (unity, reciprocity, hospitality, trust, etc.). The inductive qualitative approach allows researchers to gain an in-depth understanding of the phenomenon being studied in the field as part of a dataset (Creswell & Creswell, 2018; Oates, 2012; Yin, 2016). Furthermore, the inductive approach enabled the researchers to understand the social constructs (language, shared meanings, etc.) of a case study including factors arising from politics, power dynamics, and relationships within a given context (Yin, 2016). Users' behaviour and security practices were studied to elucidate components for a framework design.

1.6.3 Research Strategy

According to Creswell & Creswell (2018), interpretivist scholars concern themselves with the transferability and dependability of research outcomes. The case study strategy is used for this study, as it enabled an in-depth understanding of a problem through a variety of data collection techniques (Rowley, 2002; Yin, 2016). According to Rowley (2002), a case study strategy is well suited for an exploratory study that investigates a phenomenon within its context. This study makes use of qualitative interviews, focus groups, and literature review as data-gathering techniques to inform the co-design of a secure practice's framework. We further made use of an adapted design science research (DSR) as a strategy for the design of a framework for secure practices. Suero Montero a Kapinga (2019) advises that, for artifacts developed within DSR to be contextualised, foster a stronger sense of social acceptance and sense of ownership co-design should be embedded in all stages of the design cycle, "influencing also the relevance and rigour cycles as well as the impact of the artifact in the broader socio-technical context". According to Hevner (2007), the three cycles of design science research have an impact on the outcome of

design artifacts. The relevance cycle is a bridge between the contextual environment and design activities. The rigor cycle marries the design activities to the existing body of knowledge, experiences, and expertise while the design cycle forms the iterative nature of core activities involved in building artefacts and processes. The customised cycles are illustrated in Figure 1.

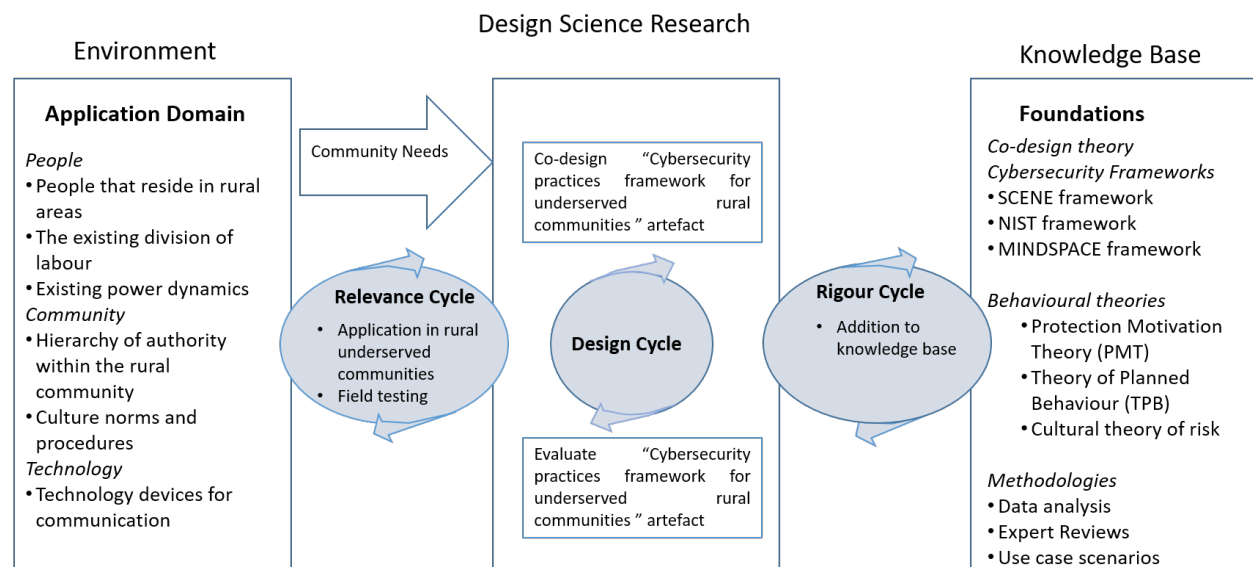


Figure 1.1: Adapted design science research.

For the evaluation (within the relevance cycle) of the designed framework via design science research, the current study made use of

1. Evaluation by the community through the co-design feedback process (Relevance and design cycles).
2. Focus group of experts knowledgeable in cybersecurity frameworks, human-computer interaction, and indigenous knowledge management.

Case sites

Five villages in Engela Constituency: Engela, Ouhongo Uakondja, Onghala, and Omatunda Anghala.

This study follows a case study strategy; therefore, the case sites need to be identified. The research objectives, coupled with literature, provided guidance on the selection criteria as well

as the definition of underserved rural communities. The study was conducted in Engela, a constituency in the Ohangwena region. Although a 2023 preliminary census report has been released, there are no findings about internet access or digital device ownership within the constituencies provided. Additional details of the national census are earmarked for release through the Census Basic Report within the third quarter of the 2024/25 financial year, with a tentative release date of October 2024 (Namibia Statistics Agency, 2024). However, the preliminary census report indicates that the population for the Engela constituency in 2023 was recorded at 30,004 inhabitants, with a population density of 97.5 per square kilometre, significantly higher than the 3.7 per square kilometre national average (Namibia Statistics Agency, 2024).

In 2011, the Namibia National Census reported that 53.1% of Ohangwena Region households owned a mobile device, however, households in Engela were reported to have 69% mobile phone ownership per household, considerably higher than the regional average (Namibia Statistics Agency, 2014b). In the same census, households in the Engela constituency had less than 1 percent access to the internet in the home and less than 1 percent access to a computer or laptop. Similarly, Shihomeka (2019) also found that rural areas in Ohangwena region were plagued with poor network connectivity and radio frequencies but reported mobile phones as being widely used within these communities in the Oshikango, Ondobe, and Omundaungilo constituencies. According to the researcher, the youth within these communities utilise mobile phones for communication with friends and family, social media, and educational purposes. Shihomeka (2019) further reported that some of the youths who participated in his study went as many as three days without charging their mobile phones due to the distances to areas with electricity. Additionally, he found that at homesteads that make use of solar electricity, youths are charged as much as 5 Namibian Dollars per charge cycle for their mobile phones. This amount may not always be available due to high unemployment in the region.

Language and culture are specifically identified to have an impact on a participatory design project. In this study, the researcher is a native speaker of the Oshikwanyama language, which is the language spoken in the case study site, and is from that OvaKwanyama group, and thus is

familiar with the culture. This is also to avoid misunderstandings that may lead to inappropriate questions, as highlighted by Winschiers-Theophilus et al. (2010) who caution about the importance of understanding the local culture and customs in technology projects within communities. Other criteria like familiarity with ICT4D are indicated as local communities would be better suited to understanding participatory design practices.

1.6.4 Data Collection

The current study used the following data collection techniques: focus groups, co-design sessions, qualitative interviews, observations, and literature review. Qualitative data collection techniques are used to gather varied evidence on a phenomenon within a case study for purposes of data triangulation (Yin, 2016); the output of which will enable the design of a framework according to the simplified 5-step process for framework design of Jabareen (2009).

1.6.5 Population

The population for this study comprised residents of an underserved rural community. Population sampling was conducted to ensure maximum variance, which included salient participants given the hierarchical nature of the case site setting. The study did not include minors; however, it included residents who have used computing devices and or the internet.

1.6.6 Sampling Strategy

Sampling involves the selection of representatives within a population for a given purpose. In research studies convenience, snowball, random, and purposive are the most used (Yin, 2016). Convenience sampling is underpinned by the selection of a data collection unit for availability, this approach is criticised for potentially generating a degree of incompleteness. Snowball sampling deals with selecting new data collection units because of the branch of an existing one, precaution needs to be taken to ensure that snowballing is purposive (Yin, 2016, p. 95). Random sampling deals with selecting a statistically defined sample from a known population, utilised more in quantitative studies, within qualitative studies, random sampling may yield a biased hand (Miles et al., 2014, p. 32). Purposive sampling deals with the selection of data collection units

based on their potential to yield the most relevant and information-rich based on the topic of the study. Kuzel (1992) as cited in Miles et al. (2014) advises that the selection of units should seek to obtain the broadest range of information, including maximum variation.

The current study makes use of purposive sampling for qualitative interviews of persons “adult’s residents in the case site under investigation” within the case site allowing for an in-depth study of the problem at hand. According to Mason (2010), the minimum sample size range of 15 to 31 is required to achieve data saturation. Yin (2016) postulates that the number of interviewees for qualitative studies ranges between 25 and 50. Due to the relatively heterogeneous nature of the population, a sample size of 30 was sufficient to reach theoretical saturation for qualitative interviews for this study. Saturation is the point at which little new information is forthcoming from additional data collection instances (Mason, 2010; Yin, 2016, p. 98). It is however worth noting that within qualitative studies, providing a definite sample size needs to be approached cautiously as the sample size and variant may evolve during data collection (Miles et al., 2014). Similarly, due to the nature of community-based projects, no sample size can be determined for focus groups, participants will self-select hence convenience will be the consideration, as often, in communities, members show up to meetings for an egalitarian approach to decision-making (Winschiers-Theophilus et al., 2013a). Table 1 shows the relationship between the research questions, data collection methods, and the perceived outcomes.

Table 1.1: The relationship between the research questions, data collection technique, and the expected outcomes

Questions		Data Collection Techniques	Outcomes
Main-RQ	How can a cybersecurity best practices framework be co-designed with rural underserved communities?	Literature review, Case study	• Co-designed cybersecurity practices framework for underserved rural communities. • Conceptual framework in Chapters 5 and 6

Sub-RQ1	What are the current security practices for rural underserved communities?	qualitative focus groups, interviews in a case study, observations	• Current cybersecurity practices • Research paper on existing cybersecurity practices in underserved rural communities (see Appendix D.2) • Presented in Chapter 4 Section 4.5.
Sub-RQ2	What risks exist for rural underserved communities as they interact with technology?	Participant observation, qualitative interviews within the case site	• Cybersecurity risks of rural underserved communities
Sub-RQ3	What are the best practices for a secure online experience for rural underserved communities?	Participant observations, qualitative interviews within the case site	• Evaluation of best practices secure framework • This is presented in Chapter 5 Section 5.3.4
Sub-RQ4	Which components are required for the development of a cybersecurity best practice framework for underserved rural communities?	Literature review, qualitative focus groups, interviews, co-design sessions	• Components for designing the cybersecurity practices framework for underserved rural communities. • Presented in Chapter 5 Section 5.3
Sub-RQ5	How can a cybersecurity best practices framework for underserved rural communities be evaluated?	Field feedback through the co-design process, focus group of experts	• Chapter 6 provides the evaluation of the co-design framework

1.6.7 Data Analysis

Qualitative data generated within a single case study requires careful analysis to ensure that the complexities of real life are captured. This study used the five analytic phases approach as outlined by (Yin, 2016, pp. 184–245). This is an iterative approach across the five phases. Phase 1 is the compilation and sorting of field notes (qualitative interviews, literature review, co-design sessions, and focus groups), a form of data triangulation of the data collected via the various data collection methods used in this study. Phase 2 is the disassembling of the compiled data into “codes”. All the data collected are coded independently of each other using open coding. Phase 3 is the reassembling of the coded data into different groupings and sequences. Phase 4 is the interpretation of the themes to create a new narrative. Phase 5 is the conclusion that is derived from phase 4 and the entire cycle (Yin, 2016).

1.7 ETHICAL CONSIDERATIONS

For this study, all ethical procedures of the Namibia University of Science and Technology are followed. Ethical clearance was sought from the university and all entities involved in this research. Throughout the research process, interactions and community ethics were agreed upon with the community. All participants voluntarily signed an informed consent and were informed that their participation was voluntary and that they could withdraw at any stage. In the instance that community members (participants) wished to be acknowledged for their contribution to the study, the researcher obliged those participants; however, for those participants that did not wish to be acknowledged, their anonymity was maintained. Furthermore, the researcher adhered to the minimal ethical standards for ICTD/ICT4D research (Dearden & Kleine, 2018) which encouraged the researcher’s reflective practice on the methods and choices throughout the research process.

1.8 DELINEATIONS AND LIMITATIONS OF THE STUDY

1.8.1 DELINEATIONS

The research was delineated to ‘cybersecurity practices within a rural underserved community’. Technical aspects of cybersecurity were not considered. Furthermore, the research also delineated a single case site in northern Namibia.

1.8.2 LIMITATIONS

This research was carried out in one rural community, and as such, the results may not be generalisable to other rural communities. The designed framework, however, was evaluated within the study and a different community for validation purposes. Another limitation is that the case site is in Namibia, and cybersecurity as a research area has not fully matured from industry, governmental, and academic perspectives. Therefore, participants may not be familiar with the concept, and as such, participants were introduced to the concept before data collection. Similarly, the research relied on existing studies from other countries in the global south. Furthermore, the existing security practice models and frameworks originate from industry and government; ours followed an academic approach to framework design. The focus group of experts may curtail this limitation, as explained in section 1.6.3. Co-designing secure practice frameworks is an unconventional approach to developing frameworks for the industry and that may face resistance as such it is the first of its kind. This limitation was addressed by infusing some elements of frameworks such as SCENE that have utilised an element of co-design activities that emanate from the industry.

1.9 CONTRIBUTION OF THE RESEARCH

This research study contributes to the area of universality in end-user privacy and security. It provides both researchers and practitioners with a framework to be utilised when developing software systems to build in cues to enforce security practices programmatically. The present study further contributes to the application of co-design to cybersecurity research. Most significantly, this study addresses a gap that exists in the literature on how people in rural,

underserved communities utilise technological devices and their thought processes around the concept of security and staying safe when using technology. This study also contributes to participatory design practices within communities. The findings may add new understanding to the role of the researcher within a community-based co-design project within an information security context.

1.10 THESIS CHAPTER BREAKDOWN

This thesis is arranged in the following manner.

Chapter 1: Introduction

This Chapter covers the introduction and background of the research and defines all terms. Additionally, the problem statement, research questions, objectives, and significance are addressed.

Chapter 2: Theoretical Framework

The second Chapter provides the framing of the literature on cybersecurity trends and existing secure practices frameworks. Furthermore, a comparison of common approaches to the development of cybersecurity practices frameworks will be discussed. Additionally, behavioural models and theories that are at the core of these frameworks are interrogated.

This Chapter highlights key ideas and literature in the types of services that are available in rural underserved areas and their impact on rural communities. The focus is given to rural communities in terms of access to ICT's and alternatives to connecting the last mile. Special focus is given to existing cyber-secure practices.

Chapter 3: Research Methodology

In this Chapter, the philosophical underpinnings of this research are unpacked. It highlights the contextual methodological approach of the research. The innovative approach of community co-

design in cybersecurity is addressed. Additionally, the overarching research methodology and ethical considerations are discussed in this Chapter.

Chapter 4: Data Collection and Analysis

This Chapter presents the data collection process as applied in this study; in addition, the data collection experience is presented. The analysis, as presented in Chapter 3, is done, and the findings are presented. The findings are interpreted according to an Afrocentric lens. Eight major themes emanated from the data analysis, and in this Chapter, they are expounded upon.

Chapter 6: Co-designed cybersecurity practices framework for underserved rural communities (CCSPF-4-URC) design

In this Chapter, 5-step simplified approach to framework design is provided, and it was followed to co-design the CCSPF-4-URC framework. Subsequently, the 5 major components of the proposed framework are explained. The Chapter provides a detailed outlay design of the proposed framework.

Chapter 7: Evaluation of the CCSPF-4-URC

Using the framework designed and developed in Chapter 6, this Chapter provides feedback on the evaluation of the framework. The evaluation of the CCSPF-4-URC framework was conducted both ex-ante and ex-post. Ex-ante, through co-design session validation and evaluation in the field, to allow for iteration and ex-post through expert focus groups. The main objectives of this evaluation were to assess the utility and efficacy of the proposed framework. Finally, the Chapter presents a refined CCSPF-4-URC framework.

Chapter 8: Conclusions, recommendations, and future work

This Chapter concludes the present study, giving a research overview of the study and reflections on the study from scientific, methodological, and personal levels. Additionally, future work and research direction are proposed.

CHAPTER 2: THEORETICAL FRAMEWORK

2.1 INTRODUCTION

The previous Chapter introduced the thesis, presenting the problem and the objectives of this thesis. This Chapter provides an overview of the relevant literature. The Chapter provides a critical understanding of underserved communities and the various services within those communities. It proceeds to give an overview of various frameworks within cybersecurity, personal cybersecurity practices, and different behavioural models used to design cybersecurity frameworks within human-computer interaction. Afrocentric literature on how African people have been perceived in contemporary research studies is presented, and we centre these as guiding principles within this thesis. To further contextualise, this thesis presents various efforts to ensure digital connectivity through strategies, policies, and various legislations. It also elucidates components that have been identified from the literature for the co-designed cybersecurity practices framework. The Chapter concludes with a summary of key points discussed within it.

2.2 AFROCENTRICITY IN AFRICAN PHILOSOPHY

2.2.1 African Philosophy

African philosophy had its beginning at a time when Western philosophers tried to make meaning (African Phenomenon) of the “African”, concluding that “a people are innately culturally, politically and economically inadequate and deficient” (Pellerin, 2012). In his impactful seminal and formative African Philosophy paper, Houtondji (1956) argued that African Philosophy is a “set of texts written by Africans and described as philosophical by their authors themselves.”. Houtondji (1956) further posits that many philosophers, some revered, practice various forms of philosophy, ethnophilosophy (Bantu philosophy), as popularised by the Belgian Missionary Placide Tempels. Ethnophilosophy aimed to challenge prevalent notions of the “primitive African” popularised by Levy-Bruhl and his school of thought, which in the 1800s was deemed insensitive to contradiction. Tempels, according to Houtondji (1956), asserted that Africans have

a different world view to that of Europeans; there is indeed a systematic conception of the universe albeit different, and as such, it deserved to be considered “philosophy” (Houtondji, 1956, p. 1). Houtondji (1956) asserts that a critical investigation of Tempel's work on African Philosophy may seem to benefit the African “black man” by dispelling and dismantling prevalent views at the time of the “primitive mentality”. However, a further critical look at Chapters like the “Bantu philosophy and our mission to civilize” provide a clear picture that the works were written for colonials and missionaries.

Bodunrin (1981) presents that philosophy begins with wonder. The universe provided the first instance of wonder, with questions about how the universe was formed, the stars, life, death, the living, the fate of the dead, and the purpose of life for the living. He argues that almost all societies had answers to these pivotal questions that formed the fabric of the community. These answers are often not questions qua external impetus.

Africans have always had interactions (through trade and other means) between the various societies and communities. However, according to Bodunrin (1981) the traditional worldviews, societal organisation, and cultures of these communities were not sufficiently dissimilar that it warranted questioning the existential answers. However, the clash with European world views through colonisation introduction of writing, forced a change in the world view which resulted in missionaries and colonisers studying Africans. These resulted in different approaches to African philosophy.

Bodunrin (1981) presents 4 approaches to African philosophy.

1. Ethnophilosophy

Ethnophilosophy was originally coined by Houtondji, who surmised that philosophers in this approach present a collective worldview of the African people, folklores, myths, and folk-wisdom as philosophy. The selling point of this approach is the emotional appeal.

2. Philosophic sagacity

This approach posits that there are men in Africa unaffected by foreign sources and influence who are capable of dialectical and critical inquiry. Additionally, these men are

perceived to have inborn insight and can reason. Thus, they seek out men in society who are reputed for their wisdom as opposed to communal consensus.

3. Nationalist-ideological philosophy

This approach has its essence in political theory that puts forward that for true liberation there is a need for a return to African humanism, having familyhood, and traditional African socialism as its foundation.

4. Professional philosophy

In this approach, professionally trained philosophers are said to be the key proponents of philosophy. They take a universal view of all philosophy which should have the same meaning in all cultures and reject ethno-philosophy. However, this approach puts forward that when dealing with various people priority be given through cultural biases and ways of being in the society that philosophers operate. They, however, are adamant that the work be done by African Philosophers and be set in some African context although the philosopher is not necessarily in that context.

However, according to Wiredu (1988) there is a need to “decolonize African Philosophy” from undue influence. The influence he argues is not all bad, but African philosophers need to doubly be critical of western philosophy.

2.2.2 Afro-centricity

The origins of Afrocentricity as an area of study are not articulated in literature with certainty (Chawane, 2000). Afrocentricity is a philosophical stance that aims to advocate for the centring of Africans and the African phenomenon within research, studying them from their own “cultures, histories, experiences, and perspectives” (Pellerin, 2012). This centring imposes that Africans are “self-willed” agents as opposed to subjections of investigation (Pellerin, 2012) for his own best interest. This stance was necessitated by the crisis of decentring Africans from their narrative (Asante, 2017a).

Afrocentricity is not anti-European as some opponents of this paradigm shift claim, Chawane (2000) states that this is a common misconception and that Afrocentrists' objective is anti-

oppression. Asante (2017b) postulated that for research works that aim to explore the narratives of African people and understand the phenomenon “the opening consciousness is assumed to be an awareness of the off-centeredness of Africans as a result of Arab and European and military, cultural, and social intrusions that have dislocated African people”.

Asante (2017a) argued that there is a set of characteristics that should be present within any research project to be considered “Afrocentric”. These characteristics emphasise the centring of Africans within discourse with the Afrocentric framework. These characteristics are:

1. Psychological location

The psychological location refers to how a person relates to African information. Therefore, within the Afrocentric sense, location refers to the cultural, historical, psychological, or personal place a person occupies, be it temporal, fixed, or permanent. Thus resulting in the person being centred or marginal concerning his or her culture. Even for those outside the community in question, their Afrocentric location can be gauged by their analysis of the African phenomenon.

2. A commitment to finding the African subject place

Afrocentricity postulates that scholars within this paradigm look for the place of the African within ideas, texts, events, and activities. Although this is difficult, “we must commit to discovering where the African person, idea, or concept enters a text, event, or phenomena, as a subject”

3. The defence of African cultural elements

Afrocentric scholars should aim to protect and defend the African place to creativity through respect for the African personality. Therefore, the use of language, psychology, philosophy, and sociology is necessary to defend African cultural elements. There is no assumption that all things African are good; however, when there are opponents to African beliefs, values, customs, habits, behaviours, religions, and thought, the

Afrocentric scholar looks for an authentic African understanding of the elements devoid of Eurocentric or non-African interpretation imposition.

4. A commitment to lexical refinement

This commitment empowers researchers to interrogate the words used to describe African reality.

“Thus, the genuine Afrocentrist seeks to rid the language of negations of African beings as agents within the sphere of Africa’s history. This should not have been perceived a problem in scholarship and literature except the condition of Western education was such that all references to Africa or African people, with the exceptions of a limited number of progressive thinkers, sought to see Africa as helpless, second-class, inferior, nonhuman, not a part of human history, and indeed, in some instances, savage. These were Europe’s contributions to the lexicon of African history.” (p. 152)

Therefore, if researchers are unsure of how to represent the reality for African persons, further seeking clarification is key to avoid misrepresentation.

5. A commitment to correcting the historical narrative of Africa

Historically, in every subject field, from African literature, African philosophy, economics, psychology, etc., the European writer has placed the African in an inferior place, a deliberate falsification of the record. Therefore, the Afrocentrist researcher should endeavour to tell the reality of Africans from their perspective, thereby dismantling falsehoods through the agency of the researcher and the Africans themselves.

Therefore, studies conducted in African rural areas situating them and understanding the philosophy and world views of inhabitants of these communities present a unique opportunity to centre the “African” by African researchers.

Building on this notion of Afrocentricity within technology research, scholars like Winschiers-Theophilus and Bidwell (2013) began to interrogate issues of epistemology in the design of

technological interfaces. In essence, arguing for what Pellerin (2012) terms as centering Africans as “self-willing” agents, subjects, and actors and not only as objects of observation as Mkabela (2005) put it.

2.2.2.1 Ubuntu

Ubuntu is an African philosophy that is centred on humanness and a set of values espoused by a people that believe in a certain way of life (Mkabela, 2005). Ubuntu values include collective unity, group solidarity, compassion, human dignity, respect, conformity, humility, love, hospitality, and humanistic orientation (Mkabela, 2005; Mokobane & Botha, 2020). The philosophy of Ubuntu is loosely translated to ‘I am because of who we all are’, in Oshikwanyama it is rendered as ‘Omunhu, ovanhu’, assuming that there is a collective sense of responsibility, preferring harmony over conflict, actions within a collective context, and decision making in an egalitarian manner. The individual gives way to the social good of the community. Additionally, conformity to established communal ethics governs accepted behaviour. However, this philosophy does not judge based on background, language, or opinions (Mkabela, 2005). This philosophy has been applied in information security research, arguing that it enables the success of social engineering attacks on individuals as trust, compassion, and a desire to help others are exploited by social engineers to gather sensitive information for dubious purposes (Mokobane & Botha, 2020).

Thaler and Sunstein (2008) as cited in (Coventry, Briggs, Jeske, et al., 2014) argue that people can be cued to behave in a certain way. Their stance assumes that a person is motivated to change, can change and that there are enough “environmental triggers” for the desired behaviour to occur. By environmental triggers, Coventry et al. (2014) refer to technological interruptions like dialog boxes, etc. However, these assumptions do not take issues like newness to technology, cultural ways of being, traditions in communication, uncertainty avoidance, collectivism-individualism, power distance relationships within the community individuals reside in, and the ethos of a user among many other factors into consideration. Additionally, these assumptions are applied to technological artefacts and not to online behaviour. The present study aims to

understand how rural underserved communities perceive risk and then co-design a secure practices framework.

2.2.2.2 Uushiindaism

Uushiindaism is a theory that emanated from social sciences, looking to exploit areas of African personhood for poverty eradication. According to Mbenzi and Ashikuti (2018) Uushiindaism is an indigenous tool used by the Aawambo, borrowing tenets from existing collectivist theory and socio-economic growth strategies. As a concept, Uushiindaism draws parallels from other Bantu-speaking theories like *llima/litsema*, which means collective effort. Which in essence relies on tenets of reciprocity and mutual respect (Mbenzi & Ashikuti, 2018). This theory has not been used within cybersecurity research; however, the collectivist undertones make it appropriate to study the OvaKwanyama people to whom the construct belongs.

2.3 UNDERSERVED RURAL COMMUNITIES

This section provides an understanding of what rural means to frame the context. We also endeavour to clarify the notion of underserved communities and their various intricacies. The section ends with a summary and structure of rural communities.

2.3.1 Defining rural communities

Within Human-computer interaction studies, rural communities have been the subject of investigation (Bidwell, Winschiers-Theophilus, Koch Kapuire, & Rehm, 2011; Dutta & Das, 2016; Fröhlich et al., 2018). There is a notion that studying rural areas and populations could yield a wealth of knowledge that may aid socio-technical systems (Hardy et al., 2019). According to Hardy et al. (2019), definitions of rural communities have often been limited to describing what the authors view as rural and rarely include community-specific descriptors to provide contextual definitions of what a rural community” is. On the one hand, the International Telecommunication Union (2020) cautions that national and regional differences in the definition of rural areas need to be taken into consideration. On the other hand, rural areas in literature are often characterised and described by either their socio-economic status, population density, or age distribution and

in some instances, by the migration patterns (Hardy et al., 2019). Since the early 1970's scholars have been trying to define what rurality means. Scholars such as Smith and Parvin (1973) have endeavoured to sum up the various definitions of rural with development works. They concluded that the definitions of the time were limited in the variations in rurality that exist among different areas and, as such create classifications that are arbitrary resulting in confounded characters of these areas. They further added that a predominant definition of the time was open land. In Namibia, rural areas are defined by their relation to open land (countryside) and urban areas (municipalities and townships) as follows "all of the countryside other than those Municipalities and Townships proclaimed by the government" (Ministry of Urban and Rural Development, 2017).

Hardy et al. (2019) argue that rural definitions are in three main categories: descriptive, sociocultural, and symbolic. These categories are intended to provide HCI researchers with a more holistic understanding of place and technology, thereby also allowing for heterogeneous areas and communities to be compared. Furthermore, descriptive rural looks at those characteristics of a place that are observable and measurable. Characters like population size and density, distance from urban centres, and economic indicators (Hardy et al., 2019; van Vuuren et al., 2012). Also, socio-cultural definitions look at the ethos of a community, the perceptions, and values that govern the local culture while symbolic definitions of rural deal with ways in which rural is described sometimes from marketing materials. These can be attributed to words, concepts, and feelings that one uses to associate with a rural area, a classic example is the use of "traditional".

The latter definition enforces the notion that rural areas have traditions that urban areas do not. Although this may be familiar for most, there is the looming question of "does the place define a tradition or the people?" Getting an answer to this question gives rise to the embodied traditions of persons that hail from rural areas.

The above observations have not evolved significantly since the 1970s. In sociology, rural studies, and geography, there is a tendency to have set categories through which rural areas are defined, this inherently assumes that they have a level of homogeneity. Moreover, still, symbolic

definitions are utilised that base the definition of rural in contrast to urban (Bidwell et al., 2011). The predominant definitions of rural are along the lines of structure, location, and socioeconomic status.

For the current study, rural is defined as the ethos of a community, the perceptions, socioeconomic status, location, values that govern the local culture, and in the countryside and outside proclaimed municipalities and townships. The above definition is a combination of the descriptive, sociocultural, and the Republic of Namibia's definitions of rural areas and communities.

2.3.2 Why rural communities

Although rural communities have predominantly been characterised as being disconnected from the rest of the world, the steady development of technology has brought them into the global village (Bidwell et al., 2011). Over the years, rural communities have been connected to urban centres through mobile technologies, however, the evolution of communication technology has opened these communities to previously unknown dangers (Bidwell et al., 2011; Schia, 2018). Cyberspace is riddled with cybercriminals that are looking to scam, spam, and even phish for personal information (and other sensitive information) that can be sold online or used for identity theft purpose (Ekandjo et al., 2018; Mukiibi, 2019). Consequently, there exists a need to secure those communities that live in rural areas. As indicated in the next section, a place can be rural but not underserved, and even within an area demarcated as underserved and rural, not all the occupants fall within a given category on the concern. Mobile technology has permeated the rural-urban divide. According to Stork et al. (2013), this can be attributed to the relative ease of access to information on mobile devices which requires lower ICT skills, and the low power consumption nature of mobile devices that do not need as much electricity as desktop computers. As such rural communities are coming online at an unprecedented rate (van Vuuren et al., 2012). Stork et al. (2013) report that in 2007 approximately 49.3% of Namibians older than 15 years of age owned a mobile phone, they, however, did not indicate the rate for rural communities but indicated that they sampled 30% from rural areas in their data collection. The NSA reports that in 2017, 79.2% of the same population group owned a mobile phone which is a

29.9% increase within ten (10) years, of these 69.2% are in rural areas. Additionally, the NSA report states that of the 69.2% with mobile phones, 84.9% (73.1% basic phones and 11.8 smartphones) can connect to the internet (Namibia Statistics Agency, 2017b).

Existing security frameworks are mostly designed for government or organisational settings by experts in western settings. There is therefore a need to co-create a secure practices framework, which enables rural communities to practice secure online behaviour. This is further exacerbated by the lack of cybersecurity awareness; incomplete or distorted view of the online security landscape; cybersecurity information being unavailable in a language they are competent in; lack of familiarity nor comfort with computers, low confidence in their ability to protect themselves online; and inherent dangers of the Internet (Grobler, Dlamini, et al., 2011; Sultan, 2020; van Vuuren et al., 2012). Trust and culture are other aspects that differentiate rural communities from pre-existing awareness campaigns (Bada et al., 2015). These communities can be characterised as unique as the homogeneous nature of Internet culture has not yet overshadowed their innate ways of being, sense of security, and ways of life.

However, rural areas hold rich data that can impact the design of software and technology. Additionally, focusing on rural underserved communities has the potential to contribute to the knowledge of universal design, thus benefiting all populations (Wang, 2017).

2.3.3 Underserved communities

The literature on underserved populations often does not differentiate between the locality; rural or urban but rather uses other factors to make this distinction. According to Wang (2017) and Clark (2005) locality, religious beliefs, common values, age group, population, socio-economic status, and physical ability are factors that can be utilised to identify populations as underserved. However, Yang cautions that to best study security, one must use the intersectionality of these communities, as studying them along singular attributes may do more of a disservice. Furthermore, there is a need to realise that culture is another factor that has implications for the security culture of a population (Alsheri et al., 2019; Reichel & Peck, 2020; Wang, 2017). Sultan (2020) supports the notion of underserved communities existing in both

rural and urban areas, even within metropolitans there exist pockets of underserved communities.

Schia (2018) looked at the underserved from the perspective of network infrastructure, looking at the cost implications for Internet Service Providers (ISP) to install equipment in sparsely populated areas with low-income (Cousineau, 2004; Frohlich, 2017; Pais, 2007). A 2016 World Bank Report reported that the Global South is primarily dominated by wireless alternatives as opposed to fixed copper wire backbones present in the Global North yet neglecting to indicate the differences between underserved communities (Schia, 2018). Different sets of classifications of underserved communities in non-western/developing countries, are not classified along locality boundaries but rather using demographics. These communities range from older adults, children, youths, refugees, migrants, LGBTQ among others.

Predominant definitions of underserved and technology revolve around e-health studies (Venkatesh et al., 2020). Definitions focus on access, infrastructure availability, and cost of mobile broadband internet access, but not much on whether the presence of these leads to technology adoption (Hasbi & Dubus, 2020; Saleminck et al., 2017; Schia, 2018). De Paula (2013) reported unintended results of a bank foundation installing Internet access at a rural school where natives picky backed to facilitate communication, trade, and finances, however for a different population - the farmers - this was not true, hence mixed results. The above communities in both case studies are defined as underserved based on locality however, their liminary boundaries to access are no longer classified as underserved. This study used the definition of Clark (2005) of the underserved, to mean “those persons who lack adequate access to resources - technological devices, and mobile broadband - because of their geographic location, income level, education level, race, ethnicity, or physical capability.” In Namibia, most rural areas are underserved in terms of the definition by Clark, there is intermittent or lack of network availability, remoteness, geographic location, and education level (Namibia Statistics Agency, 2017b; Winschiers-Theophilus et al., 2013a).

For the present study, underserved rural communities are defined as

communities that lack adequate access to resources, who are governed by a communal ethos, have values that govern the local culture, in the countryside, and outside proclaimed municipalities and townships.

2.3.4 Structure of rural communities in Namibia

Namibia is a democracy that was emancipated in 1990 (Aludhilu & Bidwell, 2018). In Namibia, most of the population resides in rural areas (Fröhlich et al., 2021; Namibia Statistics Agency, 2014a). Most inhabitants occupy lands in proximity forming homesteads, villages, and temporary settlements. The homesteads are constructed using wood, thatch, mud, cow dung, and other locally available materials (Mbenzi & Ashikuti, 2018). However, in some areas, there is a mixture of modern and traditional structures. For food, many communities engage in subsistence with both crop growing and animal herding being the main source of sustenance (Mbenzi & Ashikuti, 2018).

Often these rural areas are organised within traditional local authorities which exist within political constituencies. Community governance structures exist where they are led by a traditional leader, a Chief, King, Queen, or other titles, essentially some consider these to be kingdoms. Namibia has diverse tribes and languages; hence various rural settings could have different configurations based on traditions and culture.

The next section will discuss the types of services that are available in underserved rural areas.

2.4 SERVICES IN UNDERSERVED RURAL AREAS

Service provision is anticipated by people and businesses regardless of where they settle or reside. These services can be categorised as public or private. They are important as they contribute to the economy of rural areas and the quality of life of the people. The services include telecommunications, healthcare, financial, business, advisory, postal, and transportation services. Rural areas are described as being underserved because of the type of services that are lacking or inadequate resource provisions (Clark, 2005, p. 431).

2.4.1 Types of services offered in rural areas

Telecommunication services are the most prevalent in rural areas, with the radio serving as a primary source of information (Nandi et al., 2016). Cellular network receptions are sporadic but not available in most rural underserved communities. Healthcare services, education, and training are often provided by government or non-profit organisations that are donor-funded (De Paula, 2013; Furuholt & Sæbø, 2018; Schia, 2018). Financial services are provided by banking institutions that establish small branches for transactional banking purposes.

In sub-Saharan Africa, postal services also offer financial extension services, with little to no transactional costs charged (Busumtwi-Sam, 2019). Business and advisory services are often offered through traditional authorities, in villages, the leader(s) is responsible for issuing land Rey-Moreno et al. (2016) and hunting permits and dispute resolution (Bidwell & Hardy, 2008; Bidwell, 2009). The transportation sector is often under-developed, shared, and monetised (Bidwell, 2009). The organisation of transport services is highly decentralised and informal. Governmental services are provided by way of extension and outreach programs by relevant ministries or through telecentres (Furuholt & Sæbø, 2018). This has been attributed to the lack of access via road networks and the remoteness of some rural communities. In Namibia, the postal service has the most extensive network of branches in rural areas providing services such as payment of salaries and wages, collection of premiums for various companies and mainly “targets poor people in unbanked or under-banked regions and provides tax-free interest rates” (Namibia Statistics Agency, 2017a).

2.4.2 Factors impacting the cost-of-service delivery in rural areas

Distance from urban areas impacts service provision and delivery in rural areas. This is mainly attributed to “companies value-price their services for people who can afford their tariffs and prioritise high revenue urban markets over the expense of deploying infrastructure in low-income remote areas” (Bidwell, 2020). Fröhlich et al., (2018) and Shihomeka (2019) postulate that Namibian rural areas are also plagued with poor electricity availability, road networks, and lack of access to clean water.

In Namibia, rural areas are characterised by low population densities as many emigrate to urban centres for school, jobs, and business opportunities (Winschiers-Theophilus et al., 2013a). The low populations that are often spread across vast areas do not present an attractive business case for organisations in service delivery (Bidwell, 2020). This rural-urban migration has resulted in low population densities leaving behind the older population. This new subset especially in Namibia comprises pensioners and very young children. Several of the pensioners are retirees and moved to rural areas ‘often back home to their villages’ (Bidwell, 2009; Fröhlich et al., 2018; Winschiers-Theophilus et al., 2013a).

The lack of adequate physical infrastructure has resulted in a few service providers venturing into rural areas since the setup of the physical infrastructure presents a higher cost, there is no incentive to set it up (Nandi et al., 2016). Thus, leaving rural populations underserved in terms of telecommunication services. In efforts to connect the unconnected, various approaches have been taken, including telecentres and community networks. Telecentres are often non-profit-making spaces that are donor-funded, either by international aid agencies or by governments (Furuholt & Sæbø, 2018, p. 2). They serve as access points to the Internet and electronic government services access (Dugdale et al., 2005; Furuholt & Sæbø, 2018; Islam & Hoq, 2010). Community networks on the other hand are established by community members and they maintain them. This approach has been successful in sub-Saharan Africa (Rey-Moreno & Graaf, 2016). Even with this new approach, there still exists the issue of connecting to the Internet, the cost of access remains too large a cost to rural communities. Another challenge is the legal

deployment of these technologies within the confines of national legislation (Rey-Moreno et al., 2015).

Notwithstanding the factors above, the penetration of mobile technologies in rural areas is increasing exponentially (Fröhlich et al., 2018). The risks associated with the presence of these technologies are not eliminated but rather compounded by the lack of investment in training and awareness campaigns in cybersecurity (Bada et al., 2015). Besides, even if those programs existed, it is not known if the existing frameworks and best practices that are mostly Western and Eurocentric would have the desired effect (Wang, 2017). This can be deduced from the ineffectiveness of cybersecurity programs in companies that are better resourced and where the participants are digitally literate and have a high level of competence in English.

It is therefore imperative that we study how rural communities practice safety, only then we can be assured that a framework co-designed with them as participants may be effective in instilling and retaining cybersecurity practices when they engage online.

2.5 CYBERSECURITY PRACTICES FRAMEWORKS

This section aims to define cybersecurity and how these definitions have evolved from organisation to including ordinary netizens. Various cybersecurity frameworks are presented that could have some relevance to this study. It is worth noting that given that the present research is novel in its application area (rural underserved communities), there are no known frameworks for these contexts, therefore we rely on existent frameworks like the NIST, SCENE and MINDSPACE.

2.5.1 Cybersecurity

Cybersecurity definitions predominantly focus on technical aspects of protecting information assets from malicious, unauthorised access from cyberspace within organisations (Craig et al., 2014; Dutton, 2017; Hussain et al., 2020). Craig et al. (2014) argue that the lack of a concise definition of cybersecurity could be attributed to its complex multidisciplinary nature. To provide

a holistic definition of cybersecurity, Craigen et al. (2014) conducted a literature survey and came to a new proposed definition of

Cybersecurity is the organization and collection of resources, processes, and structures used to protect cyberspace and cyberspace-enabled systems from occurrences that misalign de jure from de facto property rights.” (p. 17)

Dutton (2017) goes further to argue that cybersecurity is a broad term that is defined differently depending on the context and that there are contexts for which a definition is not provided. Dutton (2017) adds that the pervasive nature of the Internet means that the onus of cybersecurity protection now lies with all the various stakeholders involved in developing and utilizing the Internet while ensuring that end-users can use the powerful nature of the Internet. These definitions often refer to organisational contexts but never to the community.

2.5.2 Cybersecurity best practices frameworks

Best practices are often concerned with the protection of information resources (Dutton, 2017). There is a set of best-known practices that aim to guide end-users on how to stay safe online. Some of the most common being, using strong passwords and managing them securely; logging-out of websites after use, running updated anti-virus software; updating operating systems; using trusted connection; always providing a minimal amount of personal information; and reporting cybercrimes to authorities (Coventry, Briggs, Blythe, et al., 2014). These best practices are often implemented via frameworks and models that aim to instil behaviour change. However, Dutton (2017) suggests that we move away from best practices that do not enforce strong knowledge of cybersecurity and instead move towards a cybersecurity mindset. He adds that a cybersecurity mindset is not the same as a mental model, since existing methods are not effective for the retention of how cybersecurity may be compromised.

2.5.2.1 NIST-CSF Framework

In 2014 through the presidential executive order 13636, “Improving Critical Infrastructure Cybersecurity,” the United States Government developed version 1 National Institute of

Standards and Technology (NIST-CSF) framework Shen (2014) for organisations to manage and reduce cybersecurity risks (NIST, 2023). The NIST-CSF provides flexible risk-based approach, guidelines, and best practices to assist organisations of all sizes based on their cybersecurity needs. According to Shen (2014) the NIST framework has had positive impact on cybersecurity all over the world. Although the NIST framework was designed for organisations, since then many national cybersecurity frameworks have been developed based on it. This framework is voluntary and meant to complement existing organisational policy, procedures, and programmes. Shen (2014) states that “a framework adopts industry standards and best practices to provide a set of voluntary, risk-based measures that can be used by organizations to address their cybersecurity risk”. It, however, does not address end-user best practices for staying safe online.

The NIST framework comprises three components see Figure 3.2: 1) The framework core, 2) The implementation tiers, and 3) The profiles.

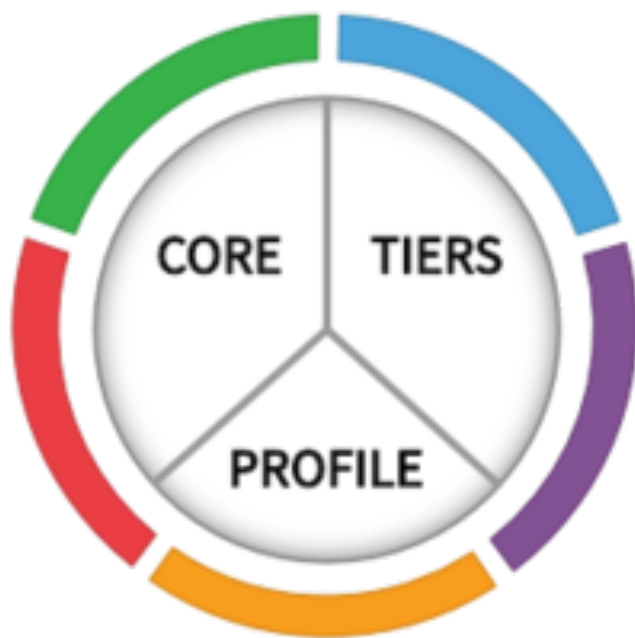


Figure 2.1: NIST cybersecurity framework components

The framework core uses non-technical language to enable and encourage communication between the various multi-disciplinary teams that work in cybersecurity and risk management.

Additionally, the core is made up of five (5) high level functions: identify, protect, detect, respond, and recover. See Figure 2.2 for the functions and the categories. The categories are intended to have a wide casting net for organisational cybersecurity objectives from personnel, cyber and physical topics.

Function	Category
Identify	Asset Management
	Business Environment
	Governance
	Risk Assessment
	Risk Management Strategy
	Supply Chain Risk Management
Protect	Identity Management and Access Control
	Awareness and Training
	Data Security
	Information Protection Processes & Procedures
	Maintenance
	Protective Technology
Detect	Anomalies and Events
	Security Continuous Monitoring
	Detection Processes
Respond	Response Planning
	Communications
	Analysis
	Mitigation
	Improvements
Recover	Recovery Planning
	Improvements
	Communications

Figure 2.2: NIST Functions and categories for organisational cybersecurity and risk management

The “Tiers” layer is a set out an organisations risk management practices as presented within the framework. However, these tiers do not serve as maturity levels of risk management nor

cybersecurity that an organisation has used to self-rank from 1 to 4. Four being the adaptive state which is desirable and 1 being a state wherein an organisation is not aware of their cybersecurity risk.

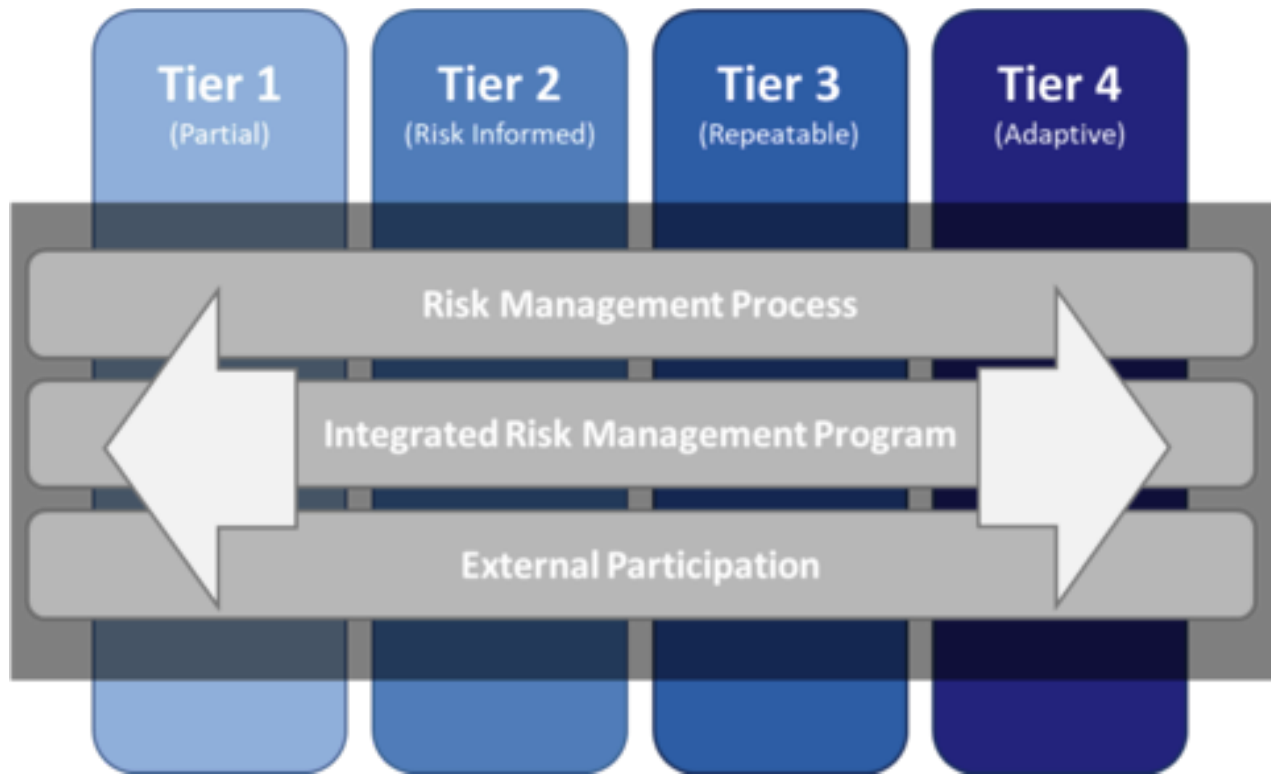


Figure 2.3: NIST Framework implementation tiers for risk management

The last layer of the NIST framework is the framework profiles, which shows the alignment of an organisation's objectives, risk appetite and outcomes against their preferred outcomes of the framework core.

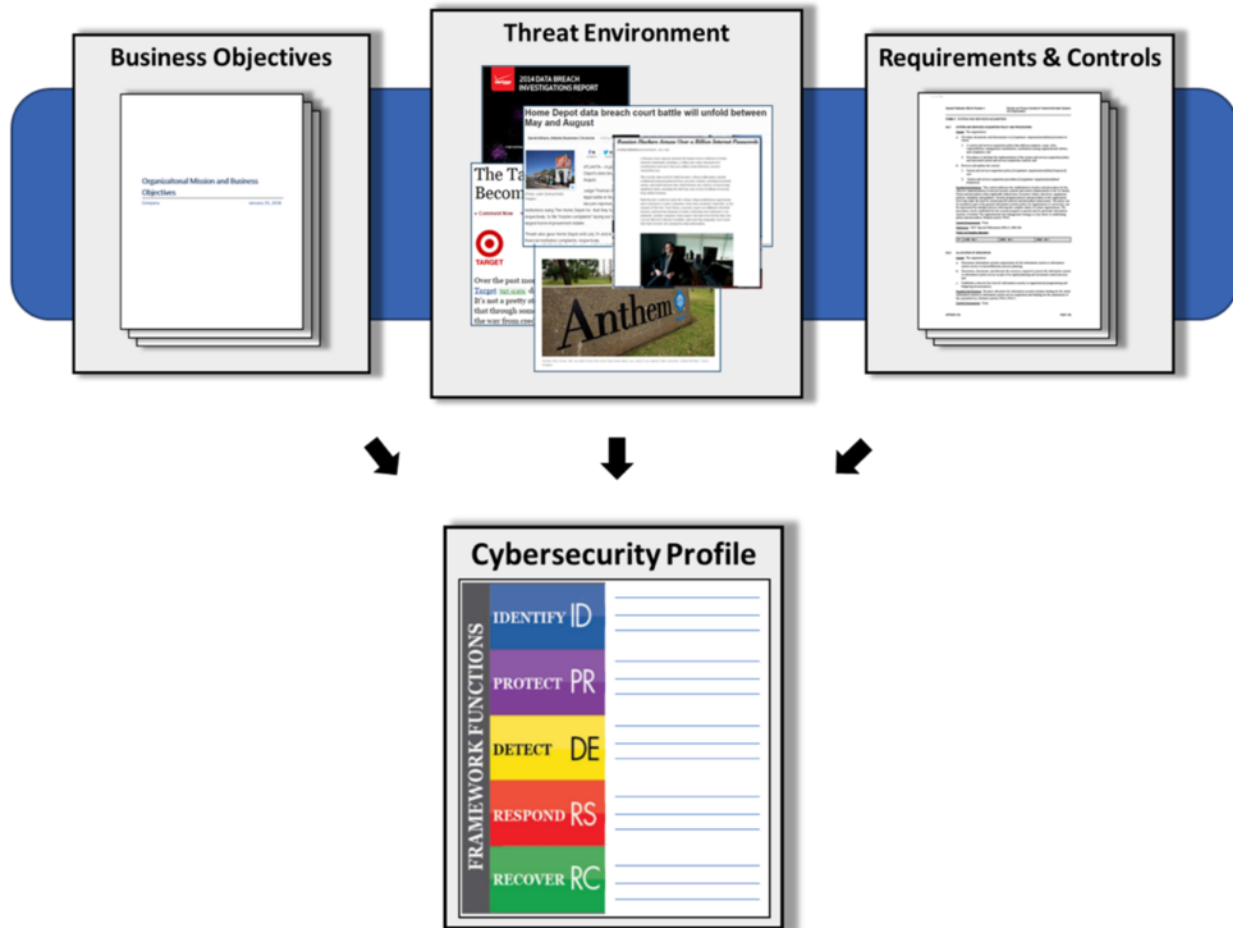


Figure 2.4: NIST framework Profiles

The NIST-CSF has seen a proposed version 2 that aims to introduce the governance function at its mid-layer in 2024. According to a concept note by NIST, the governance function aims to allow constructive alignment and accountability within the framework to bring risk management to the fore of cybersecurity management within the organisation. Starting with aligning the mission, vision, and risk management strategies, with clearly demarcated roles and responsibilities, while taking the organisational context into consideration (NIST, 2023).

The above framework was developed for businesses and other forms of organisations. However, although it caters to personnel protection and some best practices for securing the human within the organisation according to a set of policies, it does not provide best practices for individuals in rural underserved communities as it is targeted to organisations.

2.5.2.2 MINDSPACE framework

The MINDSPACE framework was developed by the Behavioural Insight Group in the Government of the United Kingdom to influence behaviour through changing the context within which behaviour and decisions for such behaviour are taken as opposed to changing minds through public policy (Paul Dolan, Hallsworth, Halpern, King, & Vlaev, 2010). The framework consists of nine non-coercive influences on behaviour, which make up the mnemonic MINDSPACE: messenger, incentives, norms, defaults, salience, priming, affect, commitment, and ego (Dolan et al., 2012). These influencers can be utilised in behaviour change paradigms and are based on behavioural theories (Briggs et al., 2017). Table 2.1 shows a succinct description of the MINDSPACE framework influencers and the behaviour that each target (Dolan et al., 2012).

Table 2.1: The MINDSPACE framework for behaviour change.

MINDSPACE cue	BEHAVIOUR
Messenger	We are heavily influenced by who communicates information to us.
Incentives	Our responses to incentives are shaped by predictable mental shortcuts such as strongly avoiding losses.
Norms	We are strongly influenced by what others do.
Defaults	‘We go with the flow’ of pre-set options.
Salience	Our attention is drawn to what is novel and seems relevant to us.
Priming	Our acts are often influenced by sub-conscious cues.
Affect	Our emotional associations can powerfully shape our actions.
Commitment	We seek to be consistent with our public promises and reciprocate acts.
Ego	We act in ways that make us feel better about ourselves.

An important influencer to note is incentives, according to Briggs et al. (2017) incentives though working to enforce strong cybersecurity behaviour do not always work. Therefore, the contrary which is sanctions sometimes works better. Other influencers like ego which depend on the

intrinsic nature of people to choose behaviours that make them feel better about themselves. Commitment is often effective when people make promises in public and do not wish to be seen going back on their word (Briggs et al., 2017). Ego tends to rely on the context of the individual; for those in individualistic settings, the Norms do not affect secure behaviour adherence (Dolan et al., 2012).

2.5.2.3 SCENE structured framework

The SCENE framework is based on MINDSPACE and aims to co-create behavioural nudges for secure practices and conformity to established policies within organisations (Coventry, Briggs, Jeske, et al., 2014). The framework is based on three main aspects: 1) the involvement of different stakeholders who might be affected by any changes in procedures; 2) the framework is iterative; 3) the framework aims to create joint ownership of security problems through the involvement of the different stakeholders. To achieve the above, the framework has five (5) stages; stage 1 begins scenario elicitation workshops, capturing poor security behaviour and the context within which they occur in the organisation. Stage 2 continues to the co-creation activity using the MINDSPACE influence factors. Resulting in possible nudges along with the influence factors that can be used to instil more secure behaviour. Stage 3 is the collective election of nudges to be implemented. This is done through a rating scheme for transparency and shows the different levels of support for solutions to security issues. In stage 4, the final nudge or intervention is developed in detail, either as a prototype or communication. It is worth noting that the intervention should not interrupt workflow unduly. The fifth stage deals with the evaluation of the developed prototype (Coventry, Briggs, Jeske, et al., 2014).

Although this framework takes a user-centred design approach, it is applied within organisations and mostly revolves around conformity to existing security policies.

The above frameworks are developed from a technical perspective without the involvement of end-users except for the SCENE framework. They are implemented by cybersecurity experts; however, studies have shown that for security to work well there is a need to design it for the

users with the users (Safa et al., 2015; Zurko, 2005; Zurko & Simon, 1996). The next section discusses user-centred design approaches to security solutions.

2.5.2.4 User-centred security design

User-centred design (UCD) as an approach aims to have the end-user of an outcome of a design process as the focal point (Sanders & Stappers, 2008). This approach (design) postulates that designers empathise with the end-user. The level of involvement of the end-user in the design process is that of a subject, who provides context (Sanders & Stappers, 2008). The intended outcome is improved user experience. However, this approach is open to empathetic bias, leading to the development of artefacts that misrepresent user needs, thus resulting in inappropriate design (Smeenk et al., 2019). The notion of UCD has crossed into cybersecurity practice and research. Zurko & Simon (1996) introduced the term user-centred security, which takes the user's needs "as a primary motivator" when designing security models and artefacts. Thereby marrying usability and security for the benefit of an end-user. They additionally state that an end-user can be a social unit, an application programmer, a group of users, or a system or security administrator. Zurko Simon define user-centred security as "security models, mechanisms, systems, and software that have usability as a primary motivation or goal." Still, the pitfall of the "user" as a subject persists. Theofanos (2020) writes that even though user-centred security has resulted in an area called usable security, end-users are still frustrated, confused, and overwhelmed by not knowing how to protect themselves and their technology. This, she adds, leads to security fatigue, a psychological state that a user experiences when confronted with a plethora of security decisions, thereby inhibiting good securing practices (Theofanos, 2020). This can be attributed to the design of security systems. The current study argues that we need to change the role of the users (human) from a subject to an active collaborator in the design process, taking a co-design approach, with the hope of having a long-lasting effort on their part to indulge in security positive behaviour.

2.6 PERSONAL CYBERSECURITY PRACTICES

The ubiquitous and pervasive nature of the Internet means that the responsibility of cybersecurity now lies with all users of the Internet (Craig et al., 2014; Dutton, 2017). Personal cybersecurity entails those practices that individuals rely on for the protection of their access and information assets from unwanted access. In this section, only those practices that are recommended for individual users outside of organisations are presented.

Dutton (2017) argues that practices like regularly updating antivirus software are futile for some end-users, as many end-users have outdated or expired antivirus software. He adds that there also exist countless videos online that provide tutorials on how to de-activate antivirus that block the installation of new software.

Passwords are the most common mode of authentication when using online accounts, which is attributed to their convenience, deployability, low cost, and immediacy (Golla et al., 2018; Markert et al., 2020). This is the most chosen method to secure online accounts although online accounts may provide additional security measures like 2-factor authentication or biometric authentication (Szumski, 2018). Golla et al. (2018) further add that there are also password managers that end-users can utilise but sometimes choose not to (Szumski, 2018). Additionally, end-users tend to re-use passwords across platforms, this practice has left many online accounts susceptible to password-based attacks. In their study on passwords, Golla et al. (2018) found that end-users sometimes do not trust alerts that inform them to change their passwords, fearing that this could be another attack (Szumski, 2018). They also found that end-users felt as though changing passwords would greatly increase the security of their accounts but did not intend to do so (Golla et al., 2018). In addition, end-users sometimes utilise strategies to create passwords; the choice of strategy depends on the end-user's perception of the security of the password as secure, memorable, and convenient for them (Markert et al., 2021).

According to Henning (2021), backing up mobile devices is a security practice that could save end-users should their devices break, get stolen, or be lost. He also adds that computers can be

backed up on local external storage devices, this practice also allows for the recovery of data when the need arises.

Therefore, a better understanding of how these practices look like for communities would provide better context for the design awareness campaigns, legislation, and national policies and the creation of new best practices for these communities (Huntinghawk et al., 2020).

2.7 HUMAN-COMPUTER INTERACTION

Design is as old as humanity itself, evolving from structural design for shelter to current pervasive computing technologies. Within the technology space and in this study, human-computer interaction can be defined as: the engagement of people with computers based on their context of use.

2.7.1 Participatory Design methods

Participatory design (PD) has been around since the 1970s in Europe (David et al., 2013). Participatory design changes the role of the designer “expert” - the researcher - to that of a social actor, and that of the user, enabling the communities to leverage collective creativity (Sanders & Stappers, 2008). This enables various stakeholders to participate in the design process from inception, thus resulting in better sustainability of solutions developed. However, participatory design methods are not without challenges, as designers or researchers, according to Wang (2017) still have “...to synthesize, select, adapt, implement, and evaluate iteratively.” Other challenges for community-based PD designers, according to Winschiers-Theophilus et al. (2009) are differing understandings of participation based on local value systems within different societies. Additionally, they argue that there are implicit and explicit rules that govern and guide participation by community members that outsiders (researchers) may not be aware of.

Participatory design, although applied in various environments globally, emanates from Western epistemology, which might present a challenge within African contexts. According to Smith et al. (2020), PD in essence already aligns well with decolonial practices based on its fundamentals of having those previously excluded participate in design and challenging existing power structures

in a bottom-up manner. They argue that decolonising PD goes beyond power structures within the already existing methods that seek generalisation and are devoid of values. They, much like Asante (2017a, 2017b) and Pellerin (2012), identified that change requires deeper critical introspection and inquiry to understand the cultural epistemologies better. Similarly, adding that traditional methods may not always work as orality remains a preferred method of expression even within post-colonial African youths.

2.7.2 Co-design and co-creation

Concepts like co-creation and co-designing have emerged as a move towards a more liberalised approach to problem-solving. According to Bourke et al. (2018) co-design has roots in PD, allowing users to become central to the design process, thereby advocating for themselves as experts in their lived experiences. These approaches allow the end-users to have the power to tell their own stories and control the narrative of their reality. David et al. (2013) postulate that co-design draws on a collective understanding of all stakeholders on shared goals, considering that they all come with different perspectives and expectations. They further argue that for co-design artefacts to be considered effective, they need to relate to the specific group that will benefit and reflect their views. Factors to consider before embarking on a co-design project with communities are the various stakeholders, social learning, sustainability, context, and ownership of the final artefact that emerges from design activities (David et al., 2013; Fröhlich et al., 2018; Villamarín-Salomón & Brustoloni, 2010).

Winschiers-Theophilus et al. (2013b), through their reflection on community-based co-design, argue that communities have more to offer than their descriptive nature. Further adding that co-design enabled them to 'see the world from within the community'. As such, the constructs that are created using a co-design approach embody locally meaningful knowledge (Muashekele et al., 2019). Kapuire et al. (2017), however, caution that for co-design activities to be successful, there is a need for consistent and harmonious mutual learning between communities and researchers. This can be achieved through the constant renegotiation of engagement through the values and protocols that guide participation. Co-design within rural communities has been practiced for some time now. There are levels of co-design within rural communities. Winschiers

et al. (2015) indicate that communities can either be informants, informed participants, validators, or co-researchers.

2.7.3 HCI Security

Applying participatory design methods to cybersecurity research has in the past been seen as the antithesis of progress (Akama et al., 2013). Although Coventry et al. (2014) have utilised co-creation as part of stage two (2) of the SCENE framework, cybersecurity research still suggests that the human is the weakest link in the security chain (Almansoori et al., 2023; Bhunu Shava & Van Greunen, 2014; Zimmermann & Renaud, 2019) and a problem (Akama et al., 2013). However, the current study utilised co-designing as it allows the researcher and community to collectively derive securing practices from the perspective of the perpetual end user. Akama et al. (2013) argue that treating users as a problem can limit the amount of innovation that can come out of user involvement. Thereby contributing to what Zimmermann and Renaud (2019) termed *“Cybersecurity Differently,”* who argue that the *“Differently”* mindset enables security researchers to treat humans as well-intentioned, thus allowing designers of security systems (and frameworks) to focus on “enhancing factors that contribute to positive outcomes and resilience”. Existing frameworks and approaches to securing the “weakest link” have not yielded the desired behavioural change outcomes intended. However, existing behavioural theories can be utilised in conjunction with participatory design practices to yield better results (Coventry, Briggs, Jeske, et al., 2014). The antithesis has been evidenced in technology adoption literature (Nandi et al., 2016; Venkatesh et al., 2020, p. 17). The next section explores dominant behavioural theories that can work for secure practice frameworks.

2.8 BEHAVIOURAL THEORIES IN HUMAN-COMPUTER INTERACTION SECURITY

Secure practice frameworks are often based on behavioural theories and models that aim to alter how people behave cumulatively. This approach is not only apparent in cybersecurity frameworks but also prevalent in software systems. It assumes the universality of applications; however, these assumptions are often western based (Crossler et al., 2013), are applied within organisations or governments, and often are not good predictors of actual change in behaviour

(Coventry, Briggs, Jeske, et al., 2014). This section looks at the dominant behavioural theories and models utilised in frameworks that aim to instil secure practices 'into' end-users.

Literature suggests that there are over eighty (80) behavioural theories and models (Coventry, Briggs, Jeske, et al., 2014). Within behavioural security research, theories and models that underpin secure practices frameworks can be broadly categorised into two: traditional psychological models and new age behavioural economics models. Traditional psychological models are more concerned with the relationship between behaviour and attitude, whilst new age behavioural economics models focus on changing a user's behaviour at the point of contact with an interactive system, assuming that users are completely selfish.

2.8.1 Protection motivation theory

As a theory, Protection Motivation Theory (PMT) was originally developed to provide a lens into how fear can be used as a motivator (Rogers, 1975). It was later extended to encompass the underlying factors in persuasive communications and messaging to influence risky behaviour. In cybersecurity, PMT is concerned with the individual's appraisal of threats, threat severity, and how an individuals' perceived susceptibility to such a threat (Shelton, 1985).

It also investigates how an individual would cope with such threats, taking into consideration the cost of responding to the threat and the individual's aptitude to respond to the threat (Briggs et al., 2017). This theory assumed that individuals have self-efficacy to perform a behaviour and is often applied within organisations.

2.8.2 Theory of planned behaviour

The Theory of Planned Behaviour (TPB) extends the Theory of Reasoned Action. TBP explores an individuals' motivation, and how that motivation leads to the intention to commit a particular behaviour (Ajzen, 1991). The intention is defined as the plan that an individual has devised to partake in a particular behaviour. The theory argues that the human behavioural intention is underpinned by three conceptually independent constructs: attitude towards the behaviour; subjective norm; and perceived behavioural control (Ajzen, 1991; Aurigemma & Panko, 2012).

Attitudes towards the behaviour refer to the beliefs/appraisal of an individual towards the outcomes of a behaviour. Subjective norm deals with the perceived social pressure to perform or not perform a behaviour. Perceived behavioural control deals with an individual's perception of factors that may aid or block the performance of a behaviour (Aurigemma & Panko, 2012). Perceived behavioural control according to Ajzen (2002) can further be described as the.

“... degree to which they can perform a given behaviour, the extent to which they have the requisite resources and believe they can overcome whatever obstacles they may encounter. Whether these resources and obstacles are internal or external to the person is immaterial.” (p. 677)

The Theory of planned behaviour details potential influences that affect that individual's decision to follow a given behaviour.

2.8.3 The cultural theory of risk

The cultural theory aims to explain risk perception. According to Olstedal et al. (2004), people choose how to act upon (risk perception, fear, etc.) their surroundings “more specifically the theory claims that this is largely determined by social aspects and cultural adherence” regarding collectivist or individualism cultures. The level of social unit bondedness (Reichel & Peck, 2020) is associated with the regulation within a social context, an individual's behaviour will tend to be more cohesive to the group (“cultural way of being”) if the context is restrictive and the opposite is true as well (Venkatesh et al., 2020). According to Tansey and O’riordan (1999) attitudes and judgements about risks are attributed to cultural relationships that guide the values and expectations for people belonging to a distinct group. Olstedal et al. (2004) further add that according to Douglas, an individual's worldview is either; individualistic; egalitarian; hierarchical or fatalistic. Again, an individual's attitude towards nature is interwoven with their worldview and risk perception. However, Da Veiga and Martins (2014) postulate that it is worth noting that even within organisations or across nation-states, there exist sub-cultures. Therefore, this theory is applicable in both organisations (departmental cultures), nation-states (ethnic units), and rural communities (groupings by generation).

2.8.4 Cultural tightness-looseness theory

The concept of culture tightness-looseness (TL) concept was first introduced by anthropologist Pelto in 1968 as a way of studying traditional societies along a spectrum. Witkin and Berry (1975 p. 16) as cited in Deckert and Schomaker (2022) introduced the dynamics of social control and group pressure to conform to existing norms. They posit that this is based on the hierarchical structure of the cultural context of the tightness-looseness. The theory of tightness-looseness theory emanated from the working paper of Gelfand et al. (2007). Tightness-looseness theory aims to study a dimension of culture and does not equate to collectivist and individualistic (IC) societies. Individualism and collectivism concern themselves with how societies emphasize ingroup ties as opposed to autonomy. While tightness-looseness refers to a society's ability to tolerate deviance from societal norms including sanctioning. Therefore, societies can have varying configurations of IC and TL.

People within communities tend to behave depending on the tightness or looseness of their communities. Here, the social norms that govern accepted interactions or actions is based on the sanctioning within those communities. Much like other scholars like Witkins and Berry who argued for the external influence of a person's behaviour, Gelfand et al. (2007) also posit that these are critical for understanding any phenomenon within these societies. The theory proposes a bottom-up and top-down approach, for instance linking an individual's psychological processes, organisational (societal) processes and the external societal constraints like the bondedness of sanctions and norms within a society. Furthermore, the theory aims to explain the relational issue of individual accountability and societal culture. Additionally, the theory also provides a lens in studying the variances within societies; these variances can be based on age, seniority, etc. within society.

Pelto (1968), as cited in Gelfand et al. (2007), argues that the looseness of a society can be attributed to antecedents like population density, kinsman systems, and economic systems. Adding that for communities (societies) where a unilineal kinship system exists (ability to trace roots to a female or male) and practice agricultural tend to be tight as opposed to bilateral kinship systems (trace roots to both a female and male) tend to be loose. The agricultural communities

Pelto argued, required stringent norms to ensure production coordination. Similarly, other scholars argue that societies that have tightly structured agricultural settings (as in the case of the current study) tend to exhibit lower psychological differentiation (lower sense of separation of the self from others in the society i.e. Ubuntu (Mkabela, 2005; Muwanga-Zake, 2009). Loosely put, homogeneous societies tend to be tight, while heterogeneous societies tend to be loose, where norms and values are flexible. Homogeneity ensures that there is little deviation from social norms, values, and behaviour for persons within a particular society.

For cybersecurity researchers, this theory has implications for a person wanting to adopt new technologies and cyber hygiene practices based on the looseness and tightness of the society.

2.9 REVIEW OF ICT EFFORTS IN NAMIBIA IN FAVOUR OF CYBERSECURITY

The ICT sector in Namibia has scant access to academic literature of status quo. As such, this section relies on corporate reports, industry reports, technical reports, and newspaper articles to provide a picture of the various efforts in Namibia that either foster or hinder cybersecurity within the country. According to the NSA (2014) report, 69% of Namibians have access to the radio, with rural populations having slightly reduced access at 65% compared to the 74% in urban areas.

2.9.1 Cyber infrastructure

Cyberinfrastructure as a concept was first mentioned in the National Science Foundation report on Information technology and computing resources to support scientific computation (Atkins et al., 2003). The definition of this term has since evolved to encompass the orchestration of people, computational systems, innovation, data storage, and research systems. Stewart et al. (2010) indicate that the most used definition of cyberinfrastructure is made up of various components like

computing systems, data storage systems, advanced instruments and data repositories, visualisation environments, and people all linked together by software and high-

performance networks to improve research productivity and enable breakthroughs not otherwise possible.

Another simplified definition of cyberinfrastructure looks at the importance of protecting critical infrastructure that is linked to cyberinfrastructure. More prominently, critical infrastructure can be viewed as all the smart-grid setups that are essential for economic growth and sustainable development. The Critical infrastructure ranges from energy and utilities, financial services, public health, water, transportation, and government systems to safety. Therefore, cyberinfrastructure can be defined as cyber-physical systems such as hardware, software, storage, processing and information communication required by critical infrastructure to function optimally (Enayaty-Ahangar et al., 2021).

Mwangala et al. (2023) argue that in Namibia, “Offices, Ministries, and Agencies are computerised and interconnected via a central network via Multiprotocol label switching (MPLS)”. MPLS connections are not encrypted; therefore, there is a need to protect this cyberinfrastructure from cybercriminals. As an extension to this notion Shapopi et al. (2023) report the existence of a national computing grid of high-performance computing computers housed at the two national universities for scientific computing purposes.

The interconnectedness of cyberinfrastructure in Namibia is supported by various network connections. Most notable are two undersea cable systems that follow the old telegraph lines: the West Africa Cable System (WACS) and the African Coast to Europe system (ACE) (Hone, 2016). The WACS cable connects Europe to South Africa with landing points in Swakopmund and became operational in 2012. The ACE cable connects France to South Africa through 15 000 kilometres of cable, also landing in Swakopmund in Namibia and going live in 2012. Although the two cable systems ushered in the potential to lower access costs, and dependency on international infrastructure, the development of the Internet Exchange Point in 2014 gives the potential for the power of the Internet to improve local access to the Internet (Hone, 2016). However, even though this connection has been up, (Dlodlo & Hamunyela, 2017) when reporting on challenges of health information systems, indicate that the regions (mostly rural areas as well) have very low speeds and in some instances a lack of connectivity is experienced. On a positive

note, Namibia's legislation through the Communication Act 8 of 2009 makes provision for potential infrastructure sharing between Mobile Network Operators, as regulated by the Communications Regulatory Authority of Namibia. The sharing of infrastructure like network towers would lessen the cost for setting up towers to the individual mobile operators and better serve the communities that need the connection (Republic of Namibia, 2009).

2.9.2 Access to affordable broadband

According to the corporate profile of the largest telecommunications provider in Namibia, coverage of 2G, 3G, and LTE was at 97%, and the Internet penetration stood at 51% in 2021 (MTC, 2021). However, there was no data on rural coverage. Similarly, data were scant on the number of Namibians that have access to technological devices and own devices capable of Internet access. The cost of access to the Internet is two-fold: firstly, on the cost of Internet-enabled devices and broadband access. The per capita cost is also attributed import taxes of technological devices. Namibia has 3 major Internet service providers (MTC, Telecom Namibia and Paratus Telecom), of these 2 provide broadband access.

Shihomeka (2017) when studying digital political engagement in the Ohangwena region, observed that some youths could not afford the cost of data bundles, nor the cost of the Internet-enabled mobile devices, to participate in political debate via social media platforms. In addition, the cost of charging the batteries of cell phones can be exponentially high as the rural areas are not electrified (Shihomeka, 2017). Shihomeka and Arora (2018) reported that feature phones cost between 200 and 500 NAD, which for most of the population is unaffordable given the unemployment rate in the region and the constituency. The cost of affordable broadband access in Namibia is not reported in the literature. However, third-party sources indicate that mobile data and voice basket as a percentage of Gross National Income (GNI) per capita stood at 2.5% (ITU, 2020). For Namibia this was reported at 4880 USD.

2.9.3 Legislation and compliance efforts

In Namibia there exists legislation that aims to be an enabler for the digital landscape in the country from a compliance and regulatory perspective. There are various laws that not only

provide legal recourse if needed but also prescribe how certain acts within the digital space should be accounted for and the constitution of various bodies that would bear the responsibility of implementing or monitoring the digital space.

Table 2.2: Legislation, policies, and strategies that enable or constrain cybersecurity

Legislation or Policy	Descriptor
Namibia National Cybersecurity Strategy	In 2020, the Ministry of Information and Communication Technology (MICT) constituted a committee of industry-led experts to develop the national cybersecurity strategy (NCS). This was on the recommendation of the EU, while the cybercrime bill is still in draft status (see section 2.9.3). The NCS was launched in 2022 and has the vision of creating “A secured cyberspace to enable an innovative Namibia and achievement of social and economic growth” (Republic of Namibia, 2022b). The vision is supported by 5 guiding pillars. 1. Enabling Legal Framework 2. Building National Capacity on Cybersecurity 3. Creating a Cybersecurity Awareness Program 4. Building National, Regional, and International Collaboration 5. Identification of Critical National Infrastructure
Overarching ICT Policy of 2017	The updated Policy seeks to solidify the Government’s focus on information security and privacy through legislation around data protection and privacy.
National Policy Broadband	The National Broadband Policy (NBP) was developed and approved in 2019 as the focal point for all broadband activities in Namibia. It defines broadband and acknowledges the importance of broadband to Internet access for the

	country across all sectors. Broadband, according to the policy, is “a minimum of 2 Mbps download speed available to 80% of the population”. It further makes provision for the establishment of the National Broadband Steering Committee, whose duty is to “oversee, coordinate, and report on the implementation of the NBP and its implementation action plan” (Republic of Namibia, 2019b). This policy acknowledges the high cost of broadband access, lack of legislation on cybersecurity, and limited broadband access in rural areas.
Access to Information Act of 2022	This Act makes provision for access to information held by public and private entities. This Act to provides for the promotion, creation, keeping, organisation and management of information in a form and manner that facilitates transparency, accountability, good governance and access to information (Republic of Namibia, 2022a).
Amended Communication Act of 2009	This Act provides for the regulation of telecommunications services and networks, broadcasting, postal services and the use and allocation of radio spectrum. Additionally, this Act makes provision of the Communications Regulatory Authority that has the powers among others to regulate the type of approval of electronic communication and computing devices. Moreover, this Act, advocates for the creation of an association to manage the Top-Level Domain Name (.na) space and all matters connected therewith (Republic of Namibia, 2009).
Electronic transaction act No. 4 of 2019	Provides provision regarding the contract concluded by e-mail, Internet, or electronic signatures. Additionally, the Act provides for admissibility of electronic evidence and consumer protection in e-commerce. Similarly, his Act also allows for legislation on matters of electronic caching, digital security through encryption and decryption, non-repudiation in terms of digital information access (Republic of Namibia, 2019a).

2.10 CHAPTER SUMMARY

This Chapter presented the theoretical foundations for this study. It begins by presenting the Afrocentric philosophy as the reflection of the authors' position. The Afrocentric philosophy posits that for any research with and about Africans, there is a need to centre the African in such academic discourse, to put right the wrongs of past representations of Africans in literature. The focus of this study is rural underserved communities, and these are explained with their characteristics and various services they possess. A further overview of cybersecurity practices is provided. These practices are often recommended through established best practice frameworks, of which three are dominant within cybersecurity discourse: NIST, SCENE, and MINSCAPE. The concept of human-computer interaction, which suggests that individuals engage with computers in different ways depending on contextual factors, is also introduced. Participatory methods, such as co-design, are highlighted for their relevance and suitability to research of this nature, particularly in relation to the democratisation and decentralisation of the research process. The chapter concludes with a discussion of various efforts to promote cybersecurity from a cyber-infrastructure perspective, including legislation and access to the Internet.

The theoretical framework provided gives an overview of the state of literature within the area of cybersecurity in rural contexts. However, research that studies cybersecurity from an indigenous lens is still in its infancy stages. The application of theories like Ubuntu within computing research, let alone cybersecurity, is limited. However, similar research is conducted by Huntinghawk et al. (2020), and Plosker and Srivastava (2021) within Canadian indigenous communities. Within the Namibian context, there is a gap in national policies and legislation. Often, key pieces of legislation like the Cybercrime bill and Data Protection bill, which are central to ensuring secure cyberspace experiences for all citizens, are still in draft status. Even though some legislation and a cybersecurity awareness strategy exist, these leave loopholes in the available legal recourse of those that fall prey to cybercriminals.

This Chapter presented the theoretical framework for this study, focusing on the utilisation of Afrocentric theories of Ubuntu and Uushiindaism to get an understanding of how the rural

communities interact with cyberspace and computing devices. Leading to the design of the cyber security practices framework.

CHAPTER 3: RESEARCH METHODOLOGY

3.1 INTRODUCTION

The previous Chapter framed the research problem and elucidated the research objectives of the present study. This Chapter frames the methodology that guided the attainment of the research objectives. It starts by discussing the espoused research paradigm and philosophical underpinnings of this study in Section 3.2, Section 3.3 provides the research strategies used. Section 3.4 presents the Design Science methodology as applied to this study, followed by the data collection and analysis methods in Section 3.5. The ethical considerations are presented in Section 3.6, and finally, the summary is in Section 3.7.

3.2 RESEARCH PARADIGM AND PHILOSOPHY

Research presents an opportunity to understand the nature of a problem. However, for research to meaningfully address research questions, the beliefs that guide the researcher(s) need to be stated. These beliefs are how the researcher views the world, essentially a paradigm (Creswell & Creswell, 2018). Lather (1986) explains research paradigms as those beliefs that “inherently reflect the researcher’s beliefs about the world that s/he lives in and wants to live in” (as cited in Kivunja and Kuyini (2017). The choice of paradigm is underpinned by four main philosophical assumptions, namely: 1) ontology, 2) epistemology, 3) axiology, and 4) methodology (Creswell & Creswell, 2018; Kivunja & Kuyini, 2017; Lincoln & Guba, 2000; Oates, 2012). These assumptions not only affect the choice of research methods but also the outcomes by way of data analysis within qualitative studies. Therefore, researchers must understand these assumptions to enable them to choose a paradigm that their methods will follow.

According to Lincoln & Guba (2000), the lines that divide many paradigms are blurring. There is a constant evolution and interweaving of paradigms based on disciplines, beliefs, culture, ideas, expectations, feelings, and perspectives (application of theories, i.e. Afrocentricity) (Kivunja & Kuyini, 2017). Lincoln and Guba (2000) argue that there are no paradigms that are superior to others but rather that discipline and perspective affect choice.

Table 3.1 elucidates the differences between the four main philosophical assumptions

Table 3.1: Philosophical assumptions and their descriptions

Philosophical Assumption	Description
Ontology	A study of being. This branch of philosophy refers to the nature of reality and how we come to determine if things make sense. The essence of any social phenomenon under investigation. These can either be classed as objectivism and subjectivism. • Objectivism states that fact is fact and reality exists' devoid of influence from social actors. • Subjectivism states that reality is a result of perception and is affected by social actors within it.
Epistemology	Study of knowledge. Deals with how we acquire knowledge about a phenomenon. Related also to asking the certainty with which we know.
Axiology	Deals with the study of value. Value as Ethics and Aesthetics. Ethical considerations concerning the research study. It concerns the value attributed to participants, community, data, and audience who will be prevued to the results of the research. Aesthetics deals with "harmony" and "beauty" of a product.
Methodology	A broad term referring to the research design, data collection, procedures, and approaches of a research study. It essentially encompasses the strategy to achieve given objectives for a research study.

As stated before, the choice of philosophical paradigm is preceded by the researchers' philosophical assumptions, as explained in Table 3.1. by Lincoln & Guba (2000) who in their ground-breaking 1985 Chapter asserted that there exist two opposite paradigms: positivism (single reality and evidence is derived from scientific rigour) and constructivism (multiple realities and context-specific findings). Over time a middle ground of paradigms has emerged, ranging from post-positivism, critical theory, transformative, pragmatism, social constructivism, realism, and postmodernism (Kivunja & Kuyini, 2017; Lincoln & Guba, 2000; Merriam, 2009; Oates, 2012; Vaishnavi & Kuechler, 2007; Yin, 2016). In the next section these paradigms are explained.

3.2.1 Various research paradigms explained

Positivism

Positivism is the most used and dominant research philosophy (Kivunja & Kuyini, 2017; Sefotho, 2015). This paradigm postulates the nature of reality as a singular truth within the natural sciences. Synonymously known as the “scientific method”. Oates (2012) states that positivism is the oldest paradigm and assumes that the world exists independent of our cognition and lived experiences. Studies under this paradigm operate in known facts and rely on deductive logic to derive solutions based on measurable outcomes.

Interpretivism / Constructivism

Within this paradigm, multiple realities are socially constructed (Oates, 2012). Constructivism also indicates that the context of the study influences the study results as the researcher brings their reality (multiple selves) to interpretation through reflection (Lincoln & Guba, 2000). Similarly, the interaction between the research and is mutually agreed upon, and interaction values are made explicit. Therefore, research conducted under the constructivist paradigm needs to follow the four trustworthiness and authenticity criteria of credibility, dependability, confirmability, and transferability. Credibility refers to the extent to which data analysis is believed to be authentic and trustworthy. dependability deals with the reproducibility of results given the same contextual conditions. Confirmability under constructivism deals with the ability of other scholars to confirm research findings. This criterion is aimed at encouraging researchers to minimise or preferably eliminate personal bias from “contaminating” the results of data analysis (Kivunja & Kuyini, 2017). The last criterion under constructivism deals with the transferability of results, providing enough contextual factors to enable others to relate the findings to their own contexts.

Participative

Participative paradigm scholars argue that politics and political agendas must be part and parcel of research inquiry (Creswell & Creswell, 2018; Oates, 2012). This paradigm further allows for

theoretical perspectives to be integrated to construct a picture of the people, group, or marginalised community's needs. Furthermore, participative worldviews need to be collaborative to enable the group or people being assisted to unshackle themselves from constraints within the context of the study.

Socio-technologist or developmentalist

The developmental paradigm argues that knowledge should exist objectively, however, the reality of this knowledge is “coded explicitly and is implicitly experienced through the behaviour of the system as interactions take place”(Gregg et al., 2001). Essentially combining the interpretivist and positivist paradigms to create multiple realities socially and technologically. Under this paradigm, developmentalists or socio-technologies believe that these multiple realities are created technologically to augment society and people. Gregg et al. (2001). The pioneers of this paradigm argue that it should be used in studies involved in high-quality software engineering research, hopefully enabling researchers to ask the right questions as opposed to using empirical evidence.

Within the present study, we only presented an analysis of design science, positivism, participative, and interpretivism paradigms with the popular paradigms in computing along with the philosophical assumptions of epistemology, ontology, methodology, and axiology as explained in Table 3.1 by (Creswell & Creswell, 2018; Kivunja & Kuyini, 2017; Lincoln & Guba, 2000; Merriam, 2009; Oates, 2012; Vaishnavi & Kuechler, 2007; Yin, 2016). The present study follows the interpretivist paradigm.

Table 3.2: Popular paradigms in computing

Philosophical paradigm	Ontology	Epistemology	Axiology	Methodology
Positivism	Devoid of context, social actors do not affect, objective with single truth	Objective, the researcher is detached from context, only that which is observable	Deductive logic, Hypothesis testing	Scientific method of investigation, experimentation, observation, quantitative

		is considered credible data		
Interpretivism (Constructivism)	Socially Constructed around consensus, dynamic, subjective, multiple realities, relative	Vicarious experience, subjective meaning based on social phenomena, context-based, sophisticated reconstruction, subjective epistemology	Exploratory, inductive logic, balanced	Qualitative, participatory, dialectical, naturalistic
Design Science	Context dependent, multiple truths socio-technologically enabled	Iterative design and knowledge through construction that is context based	Creation, artefact utility	Iterative process infused by knowledge based
Participative	Living knowledge, critical subjectivity	The persons under study are involved in the design of solutions, knowledge is co-created	Inductive logic	Iterative process

Table 3.2 succinctly sums up the four dominant paradigms within the computing sphere. For this study, which is exploratory, an interpretivist paradigm best suits the objectives of this study. The objectives of the current study are to understand how the communities within this case study understand security, how they practice cybersecurity, and how we can best collaboratively design a secure practices framework. The belief is that the values and norms that govern everyday life within these communities are socially constructed (Pellerin, 2012) and change with the interaction of community members with foreign objects like technology and the researcher.

3.2.2 Determinants of paradigm choice

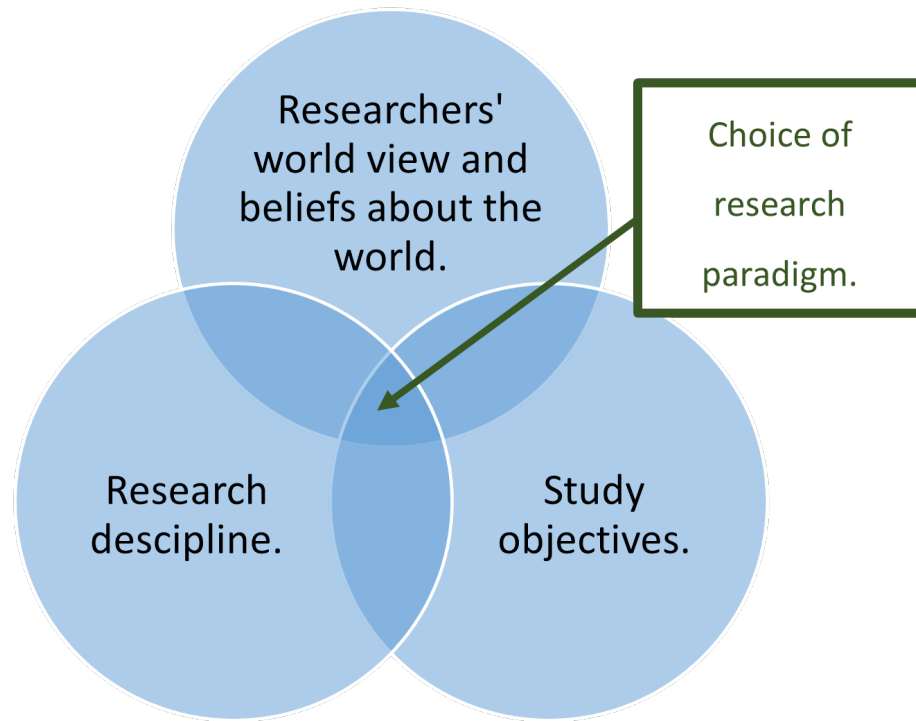


Figure 3.1: factors that affect paradigm choice

Paradigm choice is often an interplay between the researchers' view and beliefs about the world, discipline, and study objectives as indicated by the Venn diagram in Figure 3.1. Within the computing discipline, positivism and interpretivism are the most popular paradigms.

The present study is within the Human-Computer Interaction and Cybersecurity domains, both branches of the computing discipline, and focuses on co-designing for rural communities. As such, two additional paradigms of design science and participative also need to be considered as presented in the next section, which focuses on the paradigm used in this study.

3.3 RESEARCH PARADIGM AND PHILOSOPHY APPLICABLE TO THE PRESENT STUDY

This study is grounded in the interpretivist paradigm as we sought to understand and co-design with an underserved rural community; this requires *okushiiva* or an in-depth understanding of practices, ideas, feelings, and ways of being by allowing researchers to be active social actors

(Rowley, 2002). Ontologically, this philosophical stance is key to understanding the phenomenon that makes the reality that is socially constructed by different people within a community. It is worth acknowledging that even within a community, sub-communities exist, which may be divided along age, sex, literacy, digital literacy, technological skills and abilities, and English language proficiency. These sub-communities possess a microcosm of culture and may also have varying norms, values, and customs that govern interactions within them.

Epistemologically, user experience while using communication technologies is subjective and dynamic, relying on the lived experiences through interaction and end-user reflections. This study used co-design activities such as focus-group workshops, storytelling, and mind-mapping to collect data; thus, methodologically, it is qualitative. This results in the end products being built through reflection.

Interpretivism allows for a deeper understanding (*okushiiva*) of the phenomenon through the modified Design science methodology, the end-product will provide utility for the context as an intervention.

3.4 RESEARCH STRATEGIES

A research strategy is the blueprint to attaining research objectives for a given study. There exists a plethora of research strategies that depend on research choice (qualitative, quantitative, or mixed) and the paradigm of a study (interpretivism, participative, or design science research) (Oates, 2012) and study approach. The present study is qualitative in choice and uses the interpretivist paradigm. A research approach can either be deductive or inductive. The deductive approach moves from a theory-based approach, allowing theory to determine the data to be collected (Yin, 2016). The inductive qualitative approach allows researchers to gain an in-depth understanding of the phenomenon being studied (Creswell & Creswell, 2018; Oates, 2012; Yin, 2016). Furthermore, the inductive approach enables researchers to study the social constructs (language, shared meanings, norms, practices, etc.) of a case, including factors arising from politics, power dynamics, and relationships within a given context (Yin, 2016).

According to Creswell & Creswell (2018) interpretivist scholars concern themselves with the transferability and dependability of research outcomes. This study used the following data collection techniques: focus groups, qualitative interviews, observations, and literature review. These research strategies used gave varied evidence on the phenomenon under study within a case study for purposes of data triangulation (Yin, 2016), the output of which enabled the co-design of a secure practice’s framework. We further used a design science research strategy to design a framework for secure practices.

In the current study, we used the inductive qualitative research approach within a case study design. Users’ behaviour and security practices were studied to elucidate components for a framework design.

3.5 DESIGN SCIENCE RESEARCH

Design research emanated from the era of architectural designs. It has been popularised in information systems research by March and Smith (1995), Vaishnavi and Kuechler (2007), Hevner et al. (2004) and Peffers et al. (2007). Design Science research (DSR) is a problem-solving paradigm and can be utilised to solve “wicked problems” (Hevner et al., 2004). Wicked problems are defined as those that are complex, incomplete and have constantly changing requirements. There have been several design science models that aim to improve the reliability and validity of design science research while improving the artefacts that solve “wicked problems” (Hevner et al., 2004). Of note are the models by Hevner (2004), Peffers et al. (2008) and Vaishnavi and Kuechler (2007). Hevner et al. (2004) in IS research, DSR brings rigour to the IS domain which focuses on studying artefacts and their application. According to Hevner (2004), for any research study to be considered Design Science research, it must conform to seven (7) principles. These principles are presented in Table 3.3.

Table 3.3: Design Science Research Principles

Design Science Research Principles		
Principle	Explanation	Suitability for co-designing a secure practices framework

Design as an Artefact	Design science research must produce a viable artefact in the form of a construct, a model, a method, a framework, or an instantiation.	A framework is the outcome.
Problem relevance	The objective of design science research is to develop technology-based solutions to important and relevant business problems.	The framework provides rural communities with skills to protect their cyberspaces and practitioners with ways in which to better design security messaging and systems to cater for edge cases.
Design evaluation	The utility, quality, and efficacy of a design artefact must be rigorously demonstrated via well-executed evaluation methods.	The framework was evaluated in the context for which it was developed and through expert reviews for rigour.
Research contributions	Effective design science research must provide clear and verifiable contributions in the areas of the design artefact, design foundations, and/or design methodologies.	The integration of concepts from Cybersecurity, afro-centric design and human-centred design domains makes this a significant contribution to the Security and awareness domains.
Research rigour	Design science research relies upon the application of rigorous methods in both the construction and evaluation of the design artefact.	Focus group of experts, informed by theories like Ubuntu and Uushiindaism.
Design as a search process	The search for an effective artefact requires utilising available means to reach desired ends while satisfying laws in the problem environment.	The iterative nature of co-design ensures that the artefact evolved and met utility.
Communication of research	Design science research must be presented effectively to both	Research papers were written for both Conferences and Journals.

	technology-oriented and management-oriented audiences.	Additionally, panel discussions and radio presentations were made.
--	--	--

Within DSR, artefacts can take various forms like. According to Hevner et al. (2004) these can be models, frameworks, constructs, methods, instantiations or better theories to understand the development, implementation, and use of IS (Vaishnavi & Kuechler, 2004).

3.5.1 Design science research models.

3.5.1.1 *Three cycle design science research method*

According to Hevner et al. (2004) the three cycles of design science research have an impact on the outcome of design artefacts. The three cycles are relevance, design, and rigour. The relevance cycle is a bridge between the contextual environment and design activities, the emphasis is on solving real-world problems within context. The rigor cycle marries the design activities to the existing body of knowledge, experiences, and expertise. Additionally, this cycle also ensures that there are theoretical frameworks that guide the development of models and the intended artefact. The design cycle forms the iterative nature of core activities involved in building artefacts and processes.

The environment encompasses the application domain which includes the people, culture, systems, opportunities, and challenges that exist within the context of application. The Knowledge base serves as the foundation from scientific and empirical literature that guides the various variables that demarcate the problem domain (Hevner, 2007). These could be methodologies for artefact evaluation, this too is one of the key areas that (Hevner et al.,2004) propose all DSR studies contribute to. The DSR itself is iterative and artefacts go through various instantiations through a design, build, and evaluate process.

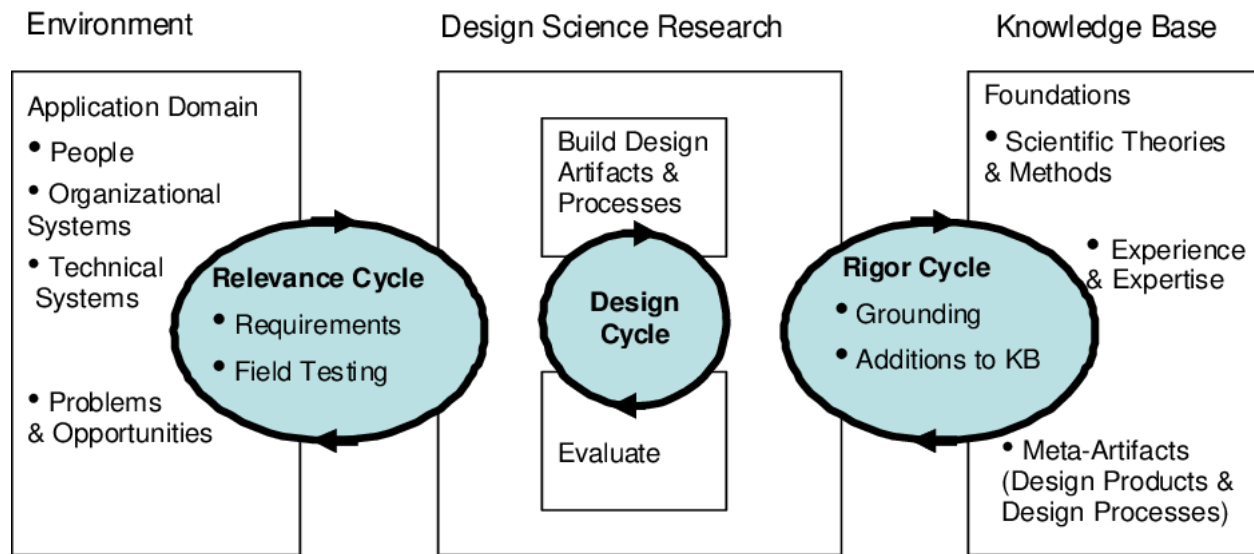


Figure 3.2: Three cycle Design Science research process

3.5.1.2 Design science research steps

Vaishnavi and Kuechler (2004) propose a procedure for DSR methodology utilising 5-steps, they argue that these steps are descriptive and bring to light the problem-solving nature of DSR.

Step 1, Problem awareness indicates the realisation of the existence of a problem, prompting further literature search and study to gain a better understanding of problem space.

Step 2, Suggestion states that once a preliminary understanding of the problem is existent, then an artefact as a possible design solution is “suggested”.

Step 3, Once the suggested solution is provided is it developed, in a form of a prototype.

Step 4, Evaluation is conducted on the prototype against some evaluation criteria or assessment.

Step 5, The building and evaluation process might lead to the refinement of the artefact, this is captured in this step.

Figure 3.3 Presents the generic steps as proposed by Vaishnavi and Kuechler (2007). Although they might appear sequential, some overlap may exist, and various iterations may occur as referred to for the development and evaluation of the artefact.

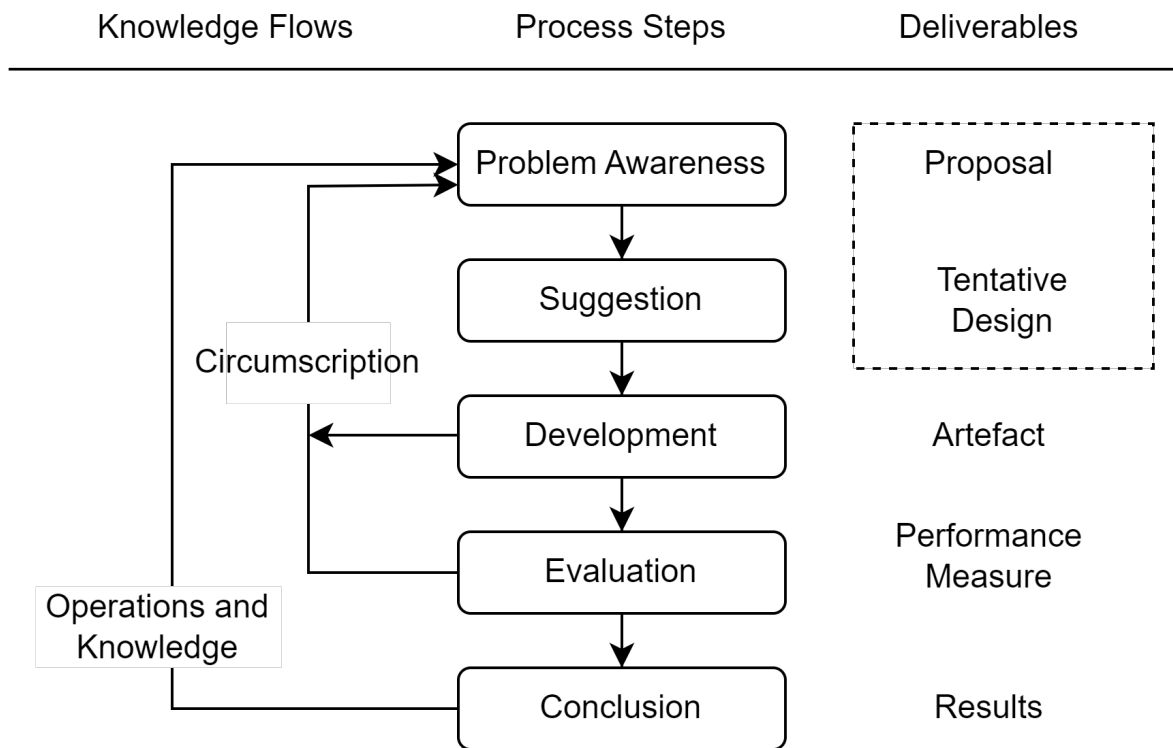


Figure 3.3: Design Science Research steps

3.5.1.3 Design Science Research Method (DSRM) process model

Design science research has come a long way. Peffers et al. (2007) introduced a modified version of the Hevner (2004) methodology. Arguing that although within Information Systems (IS) research the interpretive paradigm has been accepted. It still results in explanatory outputs that may not be applicable solutions to a problem, both in research and practice. The Design Science Research Method (DSRM) proposed by Peffers et al. (2007) provides four (4) entry point for research.

The key activities of this process model for DSRM are that there must be a clearly articulated problem that is motivated; this motivation according to Peffers et al. (2007) allows for the researcher to prove the relevance of the problem and allow acceptance of the end solution. Once the problem is defined, the objectives are then inferred from it. The objectives allow for the

development of the artefact, artefacts come in various forms as described in Table 3.3 in Design as an Artefact. The objectives must also clearly be elucidated.

Figure 3.4 provides an overview of the entire process model

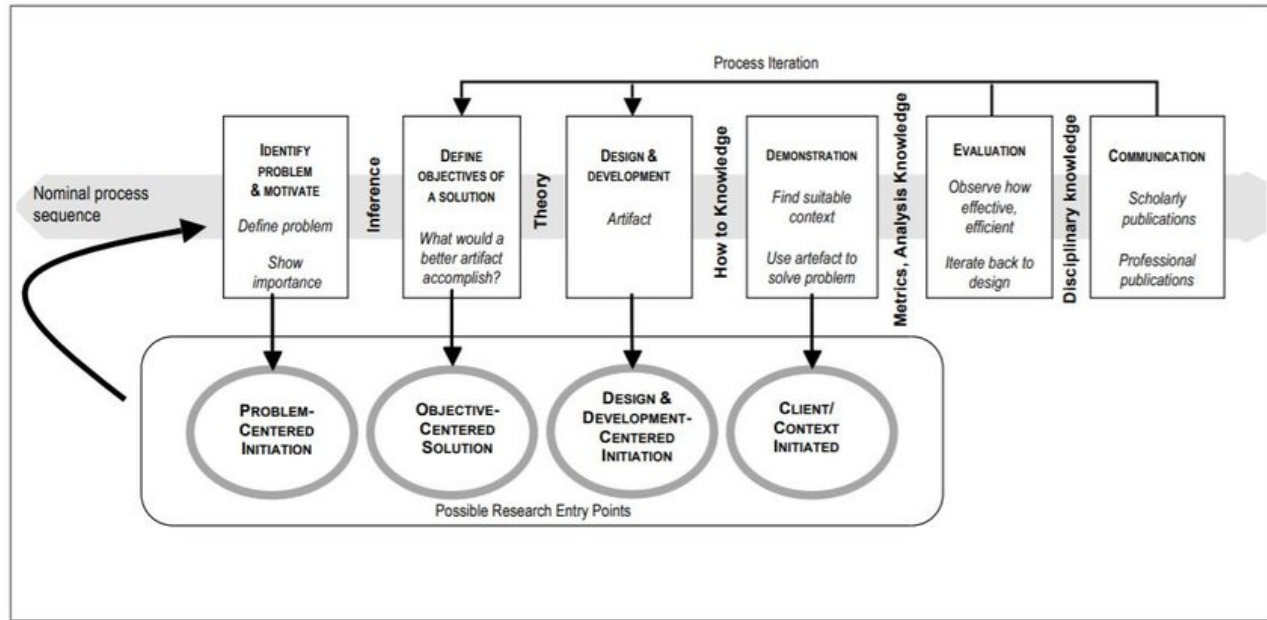


Figure 3.4: The DSRM Process Model

3.5.2 Methodology used in the present study

Studying rural communities can be complex, especially on the African continent, where existing research methodologies are not rooted within the community's epistemology (Kapuire, 2023). Therefore, for research within these communities to stand a better chance of success, there is a need to approach it differently. As such we developed, proposed, and adopted a new approach within this study, creating a pre-qualitative research approach as presented in Figure 3.5. This was created from literature synthesis and the researchers experience within rural African communities.

The approach as seen in Figure 3.5 has 4 major activities, namely, desktop research about the community, identification of community liaison, co-design of community engagement guidelines, and aligning the research to an existing qualitative research framework.

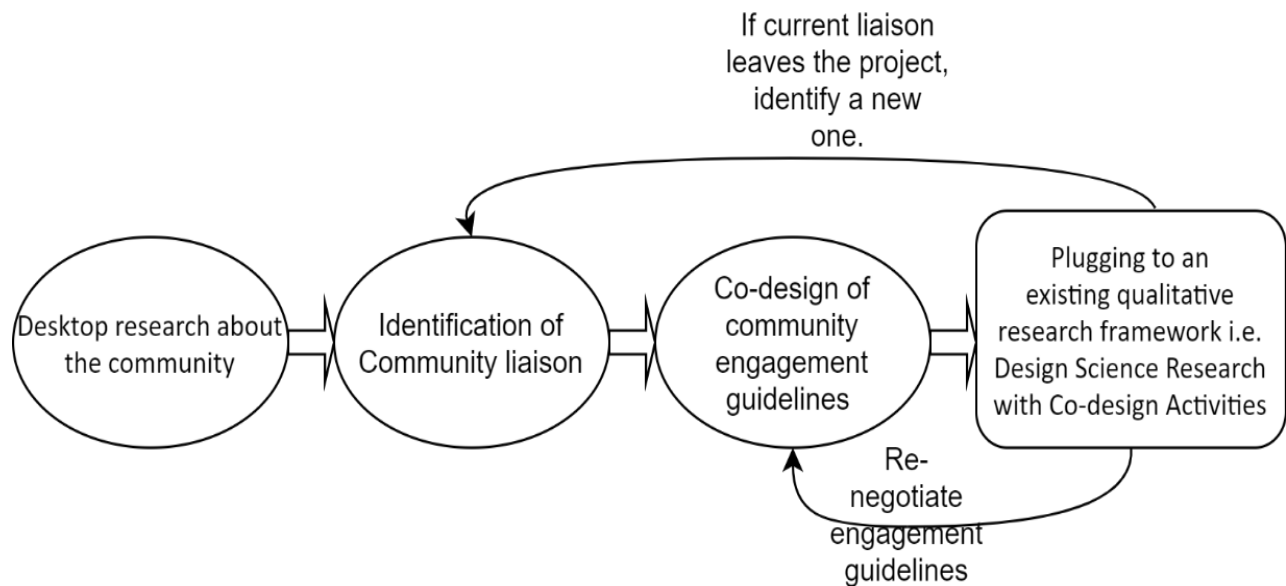


Figure 3.5: Participatory research approach for cybersecurity research in Africa

Desktop research about the community

Desktop research into the community or communities in which the researcher(s) intend to conduct their study is a crucial pre-planning activity. For rural African communities, this can be particularly challenging due to the limited availability of academic literature. However, cybersecurity researchers may find useful insights in other disciplines such as health, anthropology, and development studies. Newspaper articles are also likely to contain the most up-to-date and detailed information. Additionally, government archives can serve as valuable resources, helping researchers to understand the norms, culture, and traditions of these communities.

Identification of community liaison

Trust is often what many researchers assume terms like Ubuntu as explained in the previous chapter is inherent. However, with several information and community technology (ICT) for development projects failing, there might be a general distrust for aliens. This is further amplified if the researcher is not of African descent or from the local community (the community has no point of independent verification of who the researchers are) (Winschiers-Theophilus et al., 2015). Therefore, the identification of a community liaison is crucial to the community being

“open”, “honest” and “free” to engage. In Namibia, given our political historical context, there could still be many reeling from past traumas of the war, which could hinder research efforts before they even begin. Therefore, choosing a community liaison from pastors, existing organisations within the communities, and students from those communities to make introductions is the best solution. Ideally, the individual who serves as the liaison should have a good rapport within the communities and become part of the research team as they guide the researchers on protocols, norms, and traditions.

Co-design of community engagement guidelines

“Even though a community liaison and literature search were done in efforts to understand the community you intend to research with, it is imperative that engagement guidelines be established and co-created by researchers and the community. This will ensure that expectations are set and managed. Additionally, the research objectives can also be explained. This will also allow the community to decide if they wish to participate in the research or not. Here, caution needs to be taken by the researcher to allow the community to lead this stage, as any outcomes will impact the community. Issues of publications and ownership of outcomes also need to be discussed with the community. This also includes visits, duration, and frequency, and whether the researchers will not be embedded in the community.

This is a critical stage as it allows researchers the opportunity to build rapport with the community. Younger workers in community development agencies as community liaisons might move on from that community and if they are the only link with the community, this may result in the research activities halting or starting over.” (Nhinda & Bhunu Shava, 2021).

Aligning the research to an existing qualitative research framework

The approach stated here is not intended to replace existing methodologies that have been validated over the past few years. However, the intention is to extend and strengthen their ability to serve African communities better. These steps as indicated above are pre-cursors to the

research frameworks that would assist cybersecurity researchers in being effective in influencing end-user behaviour within African rural communities. Once they have been conducted, a move towards integrating them for instance with Design Science Research (DSR) methods might be made at this point. Although research frameworks like that of Hevner et al. (2004) include context environment and encourage iterative design, build, and evaluation cycles, how we get to engage with African communities remained a gap in literature, therefore this approach addresses that gap, especially for human security and technology research. Once we concluded the approach, we proceeded to a customised DSR model as described in the section 3.5.3. This approach resulted in a peer-reviewed conference publication, see Appendix D.3.

3.5.3 Design science research model used in this study

The present study makes use of the three cycles design science research method by Hevner et al., (2004). The customised cycles are illustrated in Figure 3.6. Of note, we customised this model by adding co-design as part of the design cycle and the relevance cycle. In both instances the communities for whom the secure practices framework (artifact) is being co-designed are partners within the creation and validation process. Thus, the relevance to the problem area is established and validated.

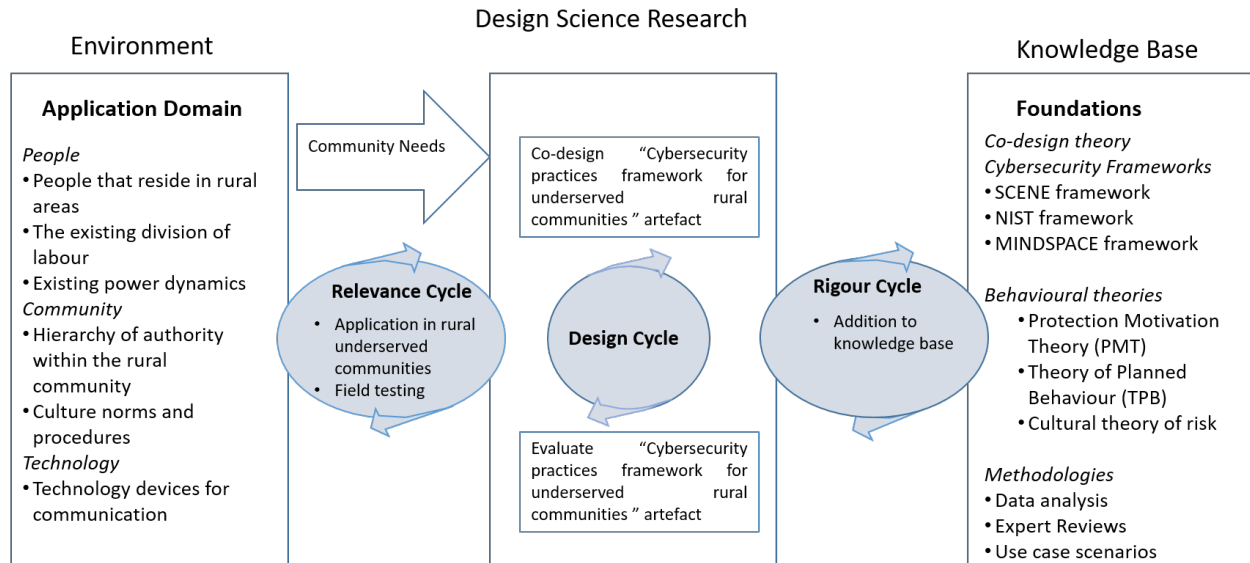


Figure 3.6: Adapted Design Science Research process model for this study

For the evaluation of the designed framework via the modified design science research model, this study used a two-pronged approach (see Figure 3.7) to evaluate the Co-designed cybersecurity best practices framework for rural underserved communities:

1. Evaluation by the community through the co-design feedback process.

Co-design as a process has an in-built feedback process that enables the evaluation of designed artefacts. In this study, this is used to evaluate the co-designed framework for ecological utility, effectiveness and completeness of the framework.

2. Focus group of experts knowledgeable in cybersecurity frameworks for efficacy.

Owing to the qualitative nature of this study, the focus group of experts evaluated the co-designed framework. Their focus was on the effectiveness, completeness, and possible utility of the co-designed framework. The process for conducting this focus group was done as listed below:

- a. Selection of the participants (a minimum of one participant must represent the communities from the Engela constituency)
- b. Sending a synopsis of the co-designed framework to the participants
- c. Presentation of the framework by the participants

- d. Discussion based on nudge questions to deal with the effectiveness, completeness, and utility of the co-designed framework.

This approach may garner criticism as possibly introducing bias. This is countered by ensuring objectivity in the presentation and only focusing on the main components of the framework. The objectives of the focus group of experts are already communicated to the participants as indicated in step b. therefore the presentation seeks to assist those who might not be very conversant in English or academic writing as a style. Step d. encourages diversity in the deliberations and evaluation of the framework.



Figure 3.7: Framework evaluation approach

Chapter 6 provides information on the evaluation results

3.6 CASE STUDY AND DATA COLLECTION METHODS

In this section the case study research design used in the present study is explained. Additionally, the data collection methods used are presented.

3.6.1 Case studies

Case studies are a form of qualitative and interpretive inductive research design, this design posits that the researcher is the primary data collection and analysis instrument (Merriam &

Tisdell, 2016). Yin (2016) defines a case study as a research design that is used to richly describe a phenomenon within its “real-life context” especially when the lines between the context and phenomenon might not be so vivid and to answer the how and why questions while delimiting the boundaries of the case study (Miles, Huberman, & Saldana, 2014). Creswell and Creswell (2018) define case studies as

A qualitative approach in which the investigator explores a bounded system (case) or multiple bounded cases (cases), over time, through detailed, in-depth data collection involving multiple sources of information (e.g. interviews, focus groups, documents, reports, and observations) and reports a case description and case-based themes.

Therefore, a case can be an individual person, group, or community (Merriam & Tisdell, 2016). Merriam and Tisdell (2016) caution that there is a need to avoid the conflation of the unit of study (case) and the process of conducting a case study.

Merriam and Tisdell (2016) postulate that for research to be considered a case study, the unit of analysis determines whether research is merely qualitative, or a case study needs to be bounded. This distinction they suggest can be determined by assessing the boundedness of the topic, looking at the population that would make the subject of inquiry.

As Yin (2016) advises that case studies can be single or multiple cases. Single case studies focus on one unit of analysis where multiple case studies (comparative case studies) can be used to present varying views and thus enhance the generalisability or external validity of the findings. Much like any qualitative method or design, case studies also have limitations, one such limitation is the lack of generalisability. Merriam (2009) indicates that, although this could be seen as a weakness, the onus lies on the reader to rely upon the vivid descriptions by the researcher and deduce what applies to their context. Another limitation is the possible bias of the researcher especially being the primary instrument of investigation. This can however be overcome by a rigorous description of the data collection and analysis within a case study (Merriam, 2009; Yin, 2016).

Therefore, this study followed an embedded single case study as the aim was to understand the existent security practices and co-design a cybersecurity framework from 4 villages (communities).

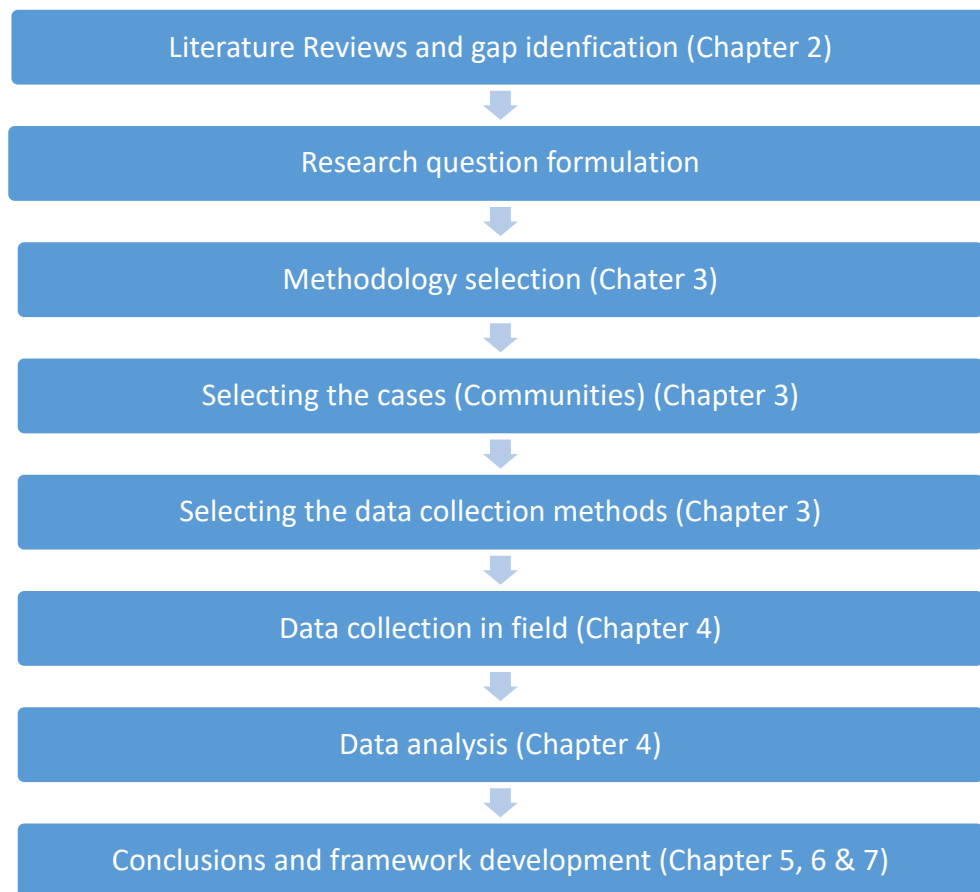


Figure 3.8: Case study process

3.6.2 Data collection methods

Data collection for the current study was done through interviews, focus groups, co-design sessions, field reviews and expert focus group for evaluation and literature review (Yin, 2009; Oates, 2016; Merriam and Tisdell, 2016).

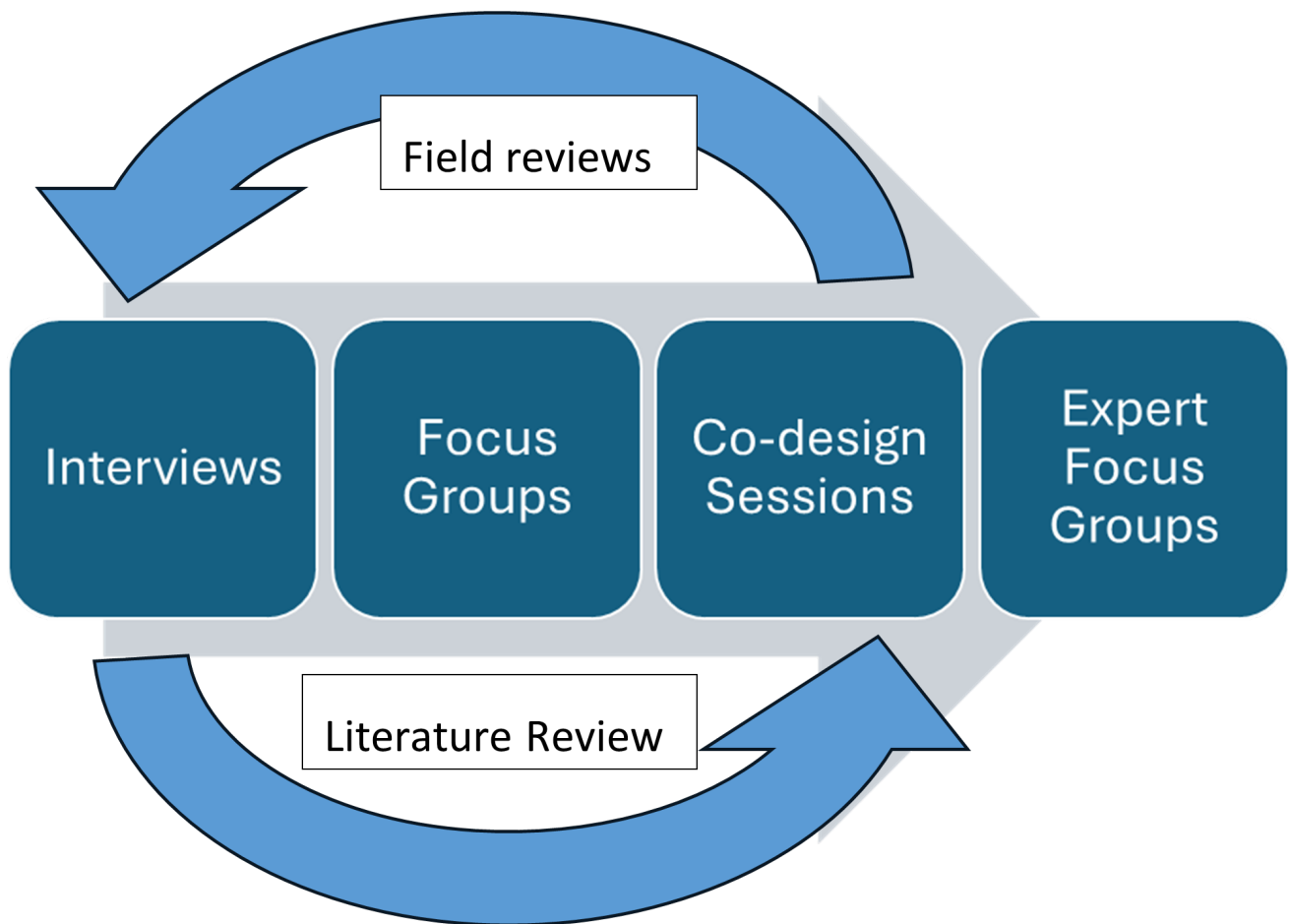


Figure 3.9: Data collection process

Figure 3.8 gives a visual representation of the data collection process followed in this study. Interviews can be structured or unstructured. Structured interviews are conducted using a preset list of questions. From an inductive approach, unstructured interviews allow free flow of dialogue with one participant, to get deeper meaning of what the participant means and tease out nuanced explanation that might explain positionality of the participant (Oates, 2016).

Focus groups allow a combined understanding of a phenomenon where participants from the same case study or as delineated by the researcher are placed in one space for discussion. This can be to understand existing engagement protocols, norms, security behaviours among other phenomena. Codesign sessions on the other hand allow creative collaboration in the creation of artefacts that might solve communal problems, usually addressing wicked problems (Yin, 2016). This data collection method enables participants to be constructors based on their understanding and introduces the aspect of democratization within data collection (David et al., 2013).

Expert focus group is what this study terms expert reviews, it allows the arrangement of experts within a particular domain or different domains to come together for the purpose of reviewing an artifact. Field reviews in the context of the present study are the reviews that community members conduct on the developed artefact.

Literature review presents the opportunity for primary and secondary data collection, through peer-reviewed publications and third-party reports.

Table 3.4 provides an overview of the research questions, the data collection techniques and the outcomes according to the thesis document

Table 3.4: Research questions and data collection methods with their respective outcomes

Questions		Data Collection Techniques	Outcomes
Main-RQ	How can a cybersecurity best practices framework be co-designed with rural underserved communities?	Literature review, Case study	• Co-designed cybersecurity practices framework for underserved rural communities. • Conceptual framework in Chapters 5 and 6
Sub-RQ1	What are the current security practices for rural underserved communities?	qualitative focus groups, interviews in a case study, observations	• Current cybersecurity practices • Research paper on existing cybersecurity practices in

			underserved rural communities (see Appendix D.2) • Presented in Chapter 4 Section 4.5.
Sub-RQ2	What risks exist for rural underserved communities as they interact with technology?	Participant observation, qualitative interviews within the case site	• Cybersecurity risks of rural underserved communities
Sub-RQ3	What are the best practices for a secure experience for rural underserved communities?	Participant observations, qualitative interviews within the case site	• Evaluation of best practices secure framework • This is presented in Chapter 5 Section 5.3.4
Sub-RQ4	Which components are required for the development of a cybersecurity best practice framework for underserved rural communities?	Literature review, qualitative focus groups, Interviews, Co-design sessions	• Components for designing the cybersecurity practices framework for underserved rural communities. • Presented in Chapter 5 Section 5.3

3.6.3 Data analysis

In qualitative studies, data analysis is not a linear step-by-step process, given that data collection and analysis do occur simultaneously. The analysis often begins with the first interaction of interview, focus group, or literature analysis, generating insights, and tentative themes, allowing the reformulation of data collection questions (Yin. 2009). This iterative process allows researchers to produce believable, trustworthy, and rigorous which are derived from the involvement of the researcher, triangulation of data from multiple sources, the rich description, and the interaction with the participants (Merriam and Tisdell, 2016 p. 191-192). There does not

appear to exist a uniform way of presenting qualitative write-ups, however, some scholars suggest that general guidelines on presenting enough evidence in support of the findings and elaborating the contributions to the body of knowledge and practice are recommended (Merriam & Tisdell, 2016).

Data analysis can be daunting when conducted after data collection as opposed to on a rolling basis. Within qualitative studies it is not always that the researcher knows the exact number of people to interview, however, the concept saturation should guide this boundedness (Miles, Huberman & Saldana, 2014).

Data analysis can be achieved in a structured manner. In this study, we utilise the five analytic phases approach as outlined by (Yin, 2016, pp. 184–245) see Figure 3.9. This is an iterative approach across the five phases. Phase 1 is the compilation and sorting of field notes (qualitative interviews, literature review, co-design sessions, and focus groups) a form of data triangulation of the data collected via the various data collection methods used in this study. Phase 2 is the disassembling of the compiled data into “codes”. All the data collected were coded independently of each other using open coding. Phase 3 is the reassembling of the coded data into different groupings and sequences. Phase 4 is the interpretation of the themes to create a new narrative. Phase 5 is the conclusion that is derived from phase 4 and the entire cycle (Yin, 2016).

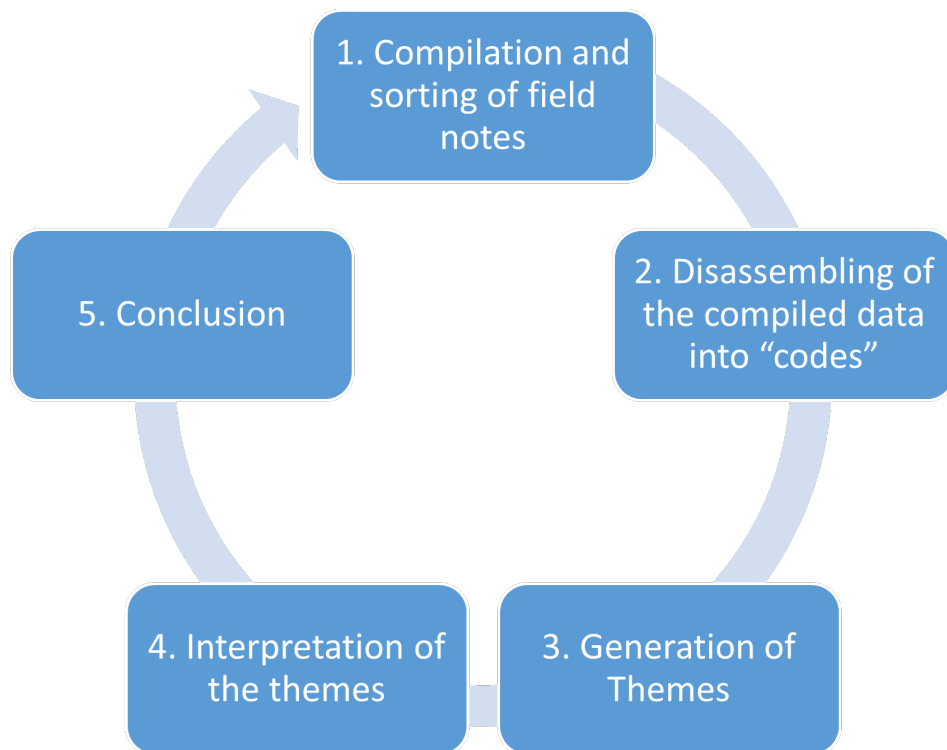


Figure 3.10: Five analytic phases approach

3.7 POPULATION

In qualitative case study research, the population represents the entire people that are eligible to participate in the study (Oates, 2016; Yin, 2016). Within qualitative case studies, the delineation of the case study is imperative to provide a vivid picture of the population (Merriam, 2009). The population for this study comprised of residents of underserved rural community. These are the residents of the 4 villages within which this study was conducted. The villages of Engela, Onghala, Ouhongo UaKondja and Omatunda Anghala.

Within these rural areas, communication is made through various means. Face-to-face communication is the most prevalent, and as such it was the main form of participant recruitment. Additionally, radio is also utilised, plus community meetings. Due to the COVID-19 pandemic, an accurate total number was not possible to provide a migration pattern within these

communities that has affected the population. These range from the loss of jobs in cities leading to temporal residents moving back to the village. Universities and schools also closed, leading to learners and students returning to the villages. However, all the adult residents of the communities made up the population of this study.

3.8 SAMPLING STRATEGY

Sampling involves the selection of representatives within a population for a specific purpose. In research studies convenience, snowball, random, and purposive are the most used (Yin, 2016). Convenience sampling is underpinned by the selection of data collection unit for their availability, this approach is criticised for potentially generating a degree of incompleteness. Snowball sampling deals with selecting new data collection units because of a branch of an existing one; precaution needs to be taken to ensure that the snowballing is purposive (Yin, 2016, p. 95). Random sampling deals with selecting a statistically defined sample from a known population, utilised more in quantitative studies, within qualitative studies, random sampling may yield a biased hand (Miles et al., 2014, p. 32). Purposive sampling deals with the selection of data collection units based on their potential to yield the most relevant and information-rich based on the topic of the study. Kuzel (1992) as cited in (Miles et al., 2014) advise that the selection of units should seek to obtain the broadest range of information, including maximum variation.

The current study made use of purposive sampling of persons “adults’ residents in the case site under investigation” as this allowed a small sample of people within their contexts allowing an in-depth study of the problem at hand.

Due to the relatively heterogeneous nature of the population, a sample size of 30 would be sufficient to reach theoretical saturation for qualitative interviews. According to Mason (2010) the minimum sample size range of 15 to 31 is required to achieve data saturation. Yin, (2016) postulates that the number of interviewees for qualitative studies ranges between 25 and 50. Saturation is the point at which little or new information is forthcoming from additional data collection instances (Mason, 2010; Yin, 2016, p. 98).

Qualitative data generated within a single case study requires careful analysis to ensure that the complexities of real-life are captured. This study used the five analytic phases approach as outlined by Yin, (2016, pp. 184–245). This is an iterative approach across the five phases. Phase 1 is the compilation and sorting of field notes (qualitative interviews, literature review, and focus groups), a form of data triangulation of the data collected via the various data collection methods that were used in this study. Phase 2 is the disassembling of the compiled data into “codes”. All the data collected were coded independently of each other using open coding. Phase 3 is the reassembling of the coded data into different groupings and sequences. Phase 4 is the interpretation of the themes to create a new narrative. Phase 5 is the conclusion that is derived from phase 4 and the entire cycle (Yin, 2016).

3.9 CASE SITE

The study is mainly located in the Engela constituency situated between Helao Nafidi Town and Ongenga Settlement. The constituency shares boundaries with Oshikango Constituency on the North-East, Endola Constituency on the South, Ohangwena Constituency on the East, Ongenga Constituency on the Western side, and the Angola-Namibia national border on the North-Western side. According to the 2011 National Census, Engela Constituency has most households within the Ohangwena region, making up 11.36% of the total households in the region with a population of 24 641 (NSA, 2011a). According to a 2020 electoral report, there were 13 743 registered voters in the constituency¹.

The Engela Constituency is headquartered in Oshimwaku village and is led by Honourable Councillor Erikan Hainghumbi an elected public official. It is comprised of several villages. For this study, Engela, Ouhongo UaKondja, Onghala, and Omatunda Anghala have been selected to participate in this study. These villages fall under the traditional leadership of the Senior village Headman albeit Onghala village being part of the political Ongenga Constituency.

¹ <https://www.ecn.na/wp-content/uploads/2022/01/Performance-Assessment-Post-Election-Report-2020-RCLA-Elections.pdf>

3.10 ETHICAL CONSIDERATIONS

Ethics forms part of academic scholarship. Therefore, in this study, ethical clearance was granted by the Faculty Research Ethics Committee (see Appendix A). All the participants in this study completed an Informed Consent form as their agreement to partake in this study (Appendices E and I). Permission was also granted by the Senior Village Headman (see Appendix B) wherein this study was conducted, additionally, due to the socio-political dynamics within the case study permission to conduct the study was also granted by the local constituency councilor (see Appendix C).

University ethics committees draft code of ethics guidelines, which have origins within the positivist utilitarian paradigm (Holliday, 2018), these guidelines bind researchers to aspects like informed consent, anonymity, and voluntary participation in research studies (Silverio et al., 2022). In this data collection experience, we came across an instance, where anonymity was waved by a participant. This occurrence is not unique to this study, other researchers like Wiles et al. (2012) Stanley (2020) and Wilkinson and Wilkinson (2017) faced similar requests from a participant or community wishing to waive anonymity. In their view, the participant was adamant about getting recognition for his participation in the study, they obliged and named the participant. Moosa (2013) posits that cultural sensitivities need to be taken into consideration, and the issue of anonymity should continuously be negotiated, from the inception of the research study to the communication of findings. An example of this position was experienced when a village elder was asked as part of the informed consent regarding anonymity “If I give you something, even information is it is yours and no longer for me to decide what you do with it”, statements like such require the researcher to then ask, “should we anonymize the data we collected here?” to which the elder indicated “I want people to know that I said this, so mention my name” – Senior Village Headman Djeimo Popyeinawa.

The above account allows us to interrogate our existing practices, especially as African universities. Are we diverse enough? Whose ethics are we referring to? Who should include who in their ethics? The communities? The university? The position of this study agrees with Silverio et al. (2022) who recommend that

we must ensure that participants' identities are protected by good research ethics, but participants are accurately and faithfully reflected in our outputs. We can achieve this through engagement with participant groups and ensuring they are included at all stages of research, whilst offering opportunities for representation, where possible and appropriate (p. 13)

The above is pointed to ponder and for scholars to reflect upon. Within this study, where anonymity was waived by the participant, the request was weighed in terms of its ability to harm the respondent and then granted accordingly (Moosa, 2013; Silverio et al., 2022; Wiles et al., 2012; Wilkinson & Wilkinson, 2017). In this study, participants selection was based on the village inhabitant's availability as such issues of fairness and equity are self-regulated.

3.11 CHAPTER SUMMARY

In this Chapter, various paradigms were explored, different research strategies and approaches were also discussed, and a decision was made to apply the interpretivism paradigm through a case study in this study. The case study design was chosen for this study as it allows in-depth exploration of a phenomenon (cybersecurity practices) in a bounded context. Within this case, study design the data collection, population, and sampling strategy are also presented in this Chapter. The case study is in the OuKwanyama kingdom specifically in the Engela constituency, this case site is also presented.

The design science research method was presented, and 3 modes presented, in this study, the 3-cycles process by Hevner (2004) is adopted. Although criticised for not providing a detailed and structured approach to conducting DSR-based research, it provided enough flexibility for the exploratory nature of this study. The 3-circles process posits that DSR research needs to be informed by the application domain, which makes up the environment of study, including the people, process, and culture. The IS research is made up of the build and evaluation processes in an iterative manner. The knowledge base where researchers get methods and theories and contribute to as presented in Chapter 7, section 7.3. The flexible nature of the 3-circles process allowed the development of a novel approach for research in rural African communities was

shared which serves as a precursor to traditional research methods for cybersecurity research in Africa as proposed in section 3.5.2 and published (see Appendix D.4)

This Chapter ended with ethical considerations wherein a call-to-action was posited by the researcher to introspect university ethics approval and processes to reflect African values. Although the existing ethics criteria suffice, it leaves elements of ownership and “participation-equity” open as it relates to intellectual property of research outputs.

The next Chapter provides the researcher's data collection experience and process as part of the descriptive nature of the qualitative case study research, and findings from the data analysis are presented. The analysis and findings are also presented in that Chapter.

CHAPTER 4: DATA COLLECTION AND ANALYSIS

4.1 INTRODUCTION

This Chapter presents the findings from the collected data from interviews, focus groups, and co-design sessions. The previous Chapter (Chapter 3) elucidated the methods used for data collection. This Chapter presents the case study of understanding the ICT use and cybersecurity practices of rural underserved communities in Northern Namibia. The demographic data, data from the interviews, focus groups, and co-design sessions are provided. The inductive thematic data analysis was also performed to create the indicated themes within this Chapter.

4.2 CONTEXTUALISATION OF CASE SITE

The case site is in the Northern part of Namibia, in the Oshana region, within the Oukwanyama Traditional Authority. The Engela constituency was the specific site. This constituency also borders Angola on the Northern site. The villages we conducted this study are located within this constituency. Oshikwanyama is the main language of the OvaKwanyama people with English being taught in schools as the official language and Portuguese spoken among youths. Oukwanyama as the area is known, is ruled by a Queen, Her Excellency Queen Martha Mwadinomho Christiaan. The Oukwanyama kingdom is organised in the form of advisors to the queen who also serve as senior leaders of vast areas which consist of cluster villages led by Senior village headmen who then control smaller clusters of villages led by junior head persons. The Junior headperson adjudicates matters within their village, like insults, stock theft, land issues, etc. However, should any party not be satisfied with the outcome, they can escalate the matter to the senior village headperson for further consideration to an avenue known as “Ediko”. If again there is no resolution, then the matter is referred to the kingdom tribunal. The queen also has appointing powers of all in the leadership hierarchy.

Homesteads within this area are located on fields that have been transformed into agroforestry. The original forests have been cleared leaving indigenous fruit trees in conjunction with cultivated crops, like pearl millet (*locally called Omahangu*). These cleared fields are referred to

as Omapya (Omahangu fields) which can range between 1 hectare to 5 hectares within communal land of the traditional authority. Homesteads tend to be in the middle of the Mahangu field and are constructed with palisades from the cleared forest in circular. Within the homestead are intricate passages and huts in rondavel fashion. Each rondavel serves a purpose and function within the homestead, from sleeping rooms segregated for male and female inhabitants, to storage rooms for specific items like hoes, ploughs, and other equipment to kitchen storage rooms for food and cooking ingredients. Similarly, the homestead is separated in areas with various functions, the most important being the traditional sitting room, which is the first point of entry, where visiting men may not go beyond unless instructed otherwise. Women tend to proceed to the kitchen area (*epata*) and are received there. If a woman has a quarrel or dispute, she remains at the Olupale, where there are chairs that communicate such to the inhabitants of the homestead. These chairs are located on the Southern side of the Olupale.

Neighbours tend to be located along the Omahangu fields, the proximity on neighbours to each other is based on the size of the Omahangu fields and other factors like grazing spaces between Omahangu fields, the socio-economic development of the area (village), water plans and underground water systems and population density. Figure 4.1 provides a pictorial representation of the case site.

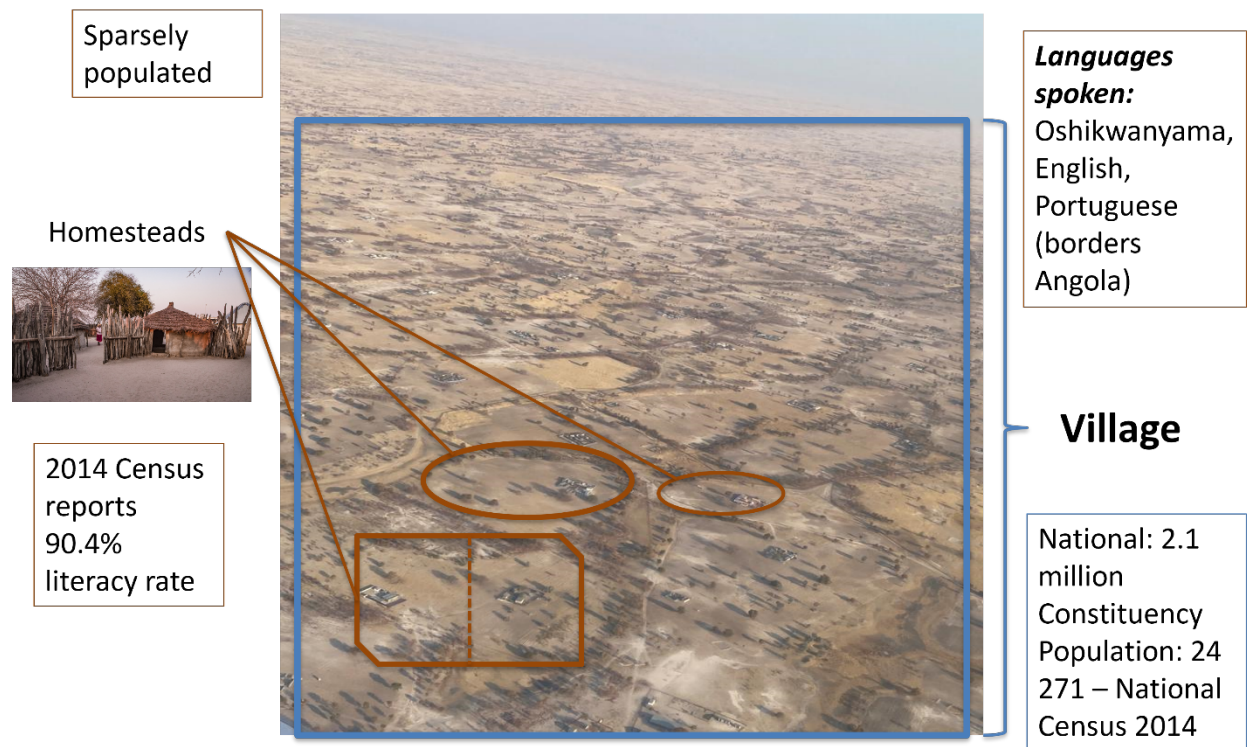


Figure 4.1: Case study setting

4.3 DATA COLLECTION PROCEDURE

The Data collection for this study was done through a case study of 4 sites. Case studies as a methodology have been in practice for over 40 years, but predominantly used within the social sciences, health, business, law, and education disciplines and finding footing within technology research (Yin, 2016). For the present study, we studied the current security practices of rural underserved communities, identified existing risks among community members when they interact with technology, understand their cybersecurity practices with the goal of co-designing a cybersecurity practices framework for these underserved rural communities in the 4 villages identified for this case study. A case study is the most appropriate qualitative methodology for the present study as it allows for in-depth understanding of the real-world phenomena (Yin, 2016). The details of the methodology used are presented in Chapter 2.

The process started with seeking Ethical Clearance (EC) from the Namibia University of Science and technology for data collection, when that was granted, the output is the EC certificate. The

next step was to engage the local constituency councillor and the cluster headman to seek permission to conduct this study; the outputs of these processes being the letters of permission from the Headman (see Appendix B) and another permission letter from the constituency councillor (see Appendix C). The next step involves the cluster headman informing the Kapatashu of the intended community meeting and to gather community members to attend. We held the community meetings on the dates we communicated to the cluster headman. Prior to the data collection during these community meetings, the purpose of the study was explained to the community members and any questions and concerns that arose were addressed. Once all the community members agreed to participate in the study, to audio record the sessions and take photographs throughout the study, they then signed the Informed Consent form (See Appendix E).

Data collection began with the focus groups, following the Focus groups' data collection instrument (See Appendix F). Once the participants were primed through the focus groups, the co-design sessions took place. During these co-design sessions, the community members identified various components that they would want to see in a framework that addressed cybersecurity for them. Here they indicated the importance of governmental involvement in helping them stay secure. Some community members added that they also would like to know how technology that was already developed elsewhere according to how the makers who created them can be contributed to them and that this should also come out clearly. They indicated using proverbs like *"shitunda nonghedi, shilongo nomukalo"*, to mean, each land has its own rules, regulations, values, norms, culture, and principles. Therefore, there is a need to respect the values of each person and community alike.

The interviews were the last to be conducted, with the researcher asking the group for those that would be interested in participating in an interview. Some participants indicated willingness to participate in the interviews but at a later stage, these participants were contacted, and arrangements were made to conduct these interviews.

The findings from the data collection were presented to some of the participants for validation and where errors occurred; they were corrected.

Figure 13 shows the data collection method utilised for this study and the relevant outputs at every step of the process

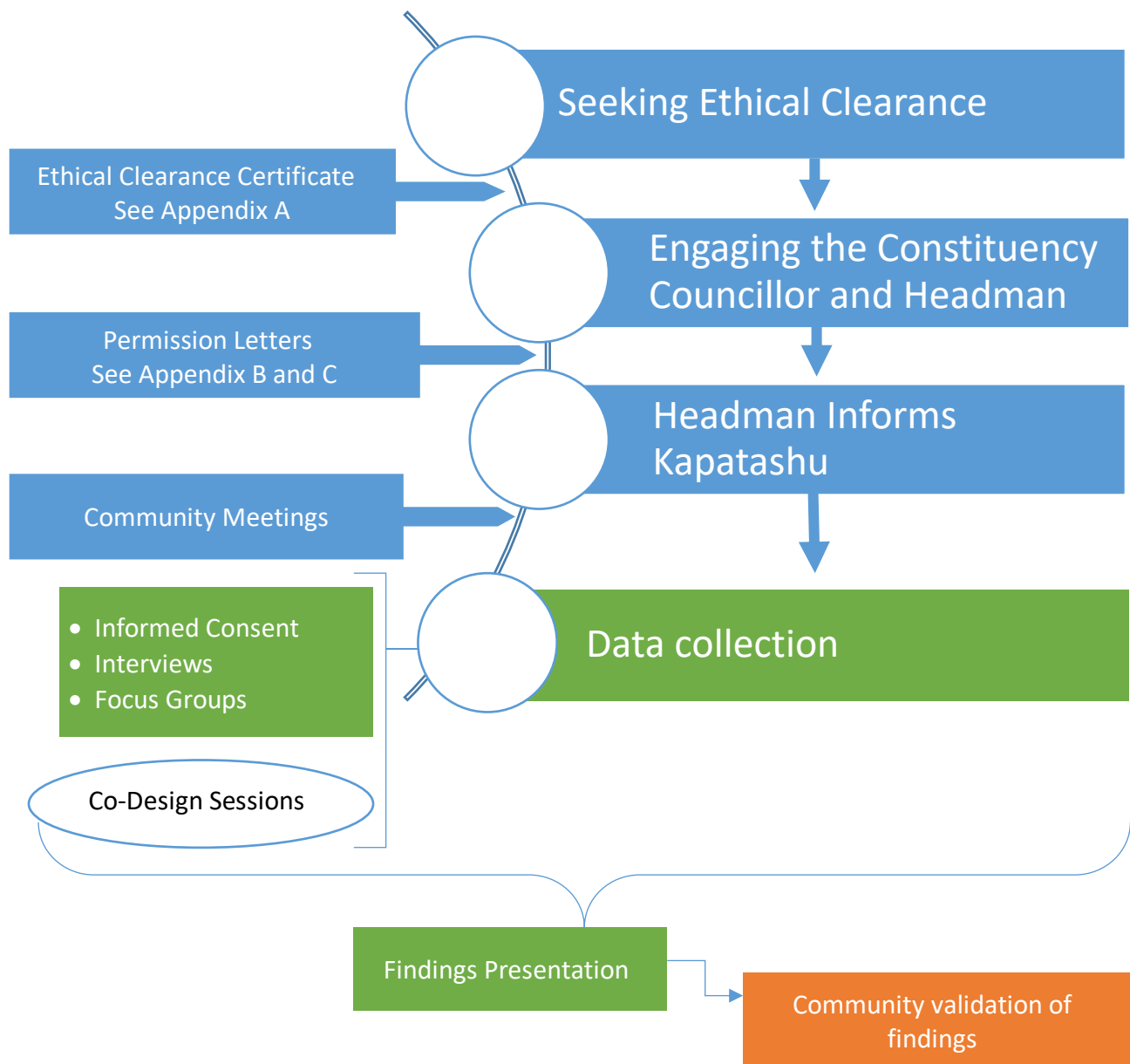


Figure 4.2: Data collection process

4.4 DATA COLLECTION EXPERIENCE

Our study was qualitative. Data were gathered using interviews, focus groups, and co-design sessions during 2021 after the second wave of COVID-19 had passed. Similarly, advice was sought to ensure that the researchers were not endangering the community and advice was given to isolate for 2 weeks prior to going into the field for data collection. This study targeted residents of villages in the Engela constituency, specifically looking at 4 villages: Engela, Onghala, Ouhongo UaKondja, and Omatunda Anghala and officials from the custodial Ministry of Information and Communication Technology.

Due to the nature of community-based research, we did not have a sample size or a target total number of participants. We were guided by the availability of village residents as per their norms for community meetings and guidance from the literature on data collection within qualitative studies, specifically data saturation (as indicated in the Research Methodology Chapter). Our community meetings in all 4 villages happened under a tree prepared by a Kapatashu or the village headman or a proxy of the village headman. These communal meeting places (matured indigenous trees) often were located near transit routes within the villages. Therefore, participants came and stayed only for the session that their availability permitted.

4.4.1 Interviews

A total of 14 interviews were conducted. Within the four villages that constituted the case study, 11 community members were interviewed. In addition, two individuals from the Ministry of Information and Communication Technology (MICT) were interviewed. These individuals were selected based on their involvement with cybersecurity at the national level.

Table 4.1 indicates a total of 12 interviews carried out across the four villages. These interviews lasted between 27 minutes and two hours and 24 minutes. Within the Oshikwanyama culture, when an elder speaks one may not interrupt or cut them off. The longest interview was with a village elder who also served as our research intermediary (EM-1).

Table 4.1: Interviewee profiles

Interviewee	Sex	Village/organisation	Code
1	M	Engela	EM-1
2	M	Engela	EM-2
3	M	Engela	EM-3
4	N	Engela	EM-4
5	F	Engela	EF-1
6	M	Onghala	OM-1
7	M	Onghala	OM-2
8	M	Onghala	OM-3
9	F	Onghala	OF-1
10	F	Onghala	OF-2
11	M	Ouhongo Uakondja	OKM-1
12	F	Ouhongo Uakondja	OKF-1
13	F	MICT	OMF-1

14	M	MICT	OMM-1
----	---	------	-------

The disparity between the durations of interviews was also elongated by the greeting culture where the elder spends time asking who you are, by your clan totems, family name, village of origin etc. Clan totems are required from the both the maternal and paternal lineage of the researchers. This process may seem repetitive with the elder greeting you as you arrive at the homestead “Mwa lele po?” “Opo muli?” “Omuli tuu nawa?” then proceeding to “Omweya po?”, “Opo ne muli?”. These are all greetings that serve multiple purposes, 1) to establish if you are okay, 2) to probe if you are a good visitor or one with a quarrel, 3) to try to determine the nature of your visit 4) to know if you are familiar with Oshikwanyama customs of greeting and understand oneself. This practice serves as a (scaffolding) trust building exercise and credibility evaluation of the researcher to determine dependability, credibility, and the seriousness of the researchers. Essentially living up to the Oshikwanyama proverbs of *“Omunhu e he ku lilile ke fi woye”*, which means one only seeks help from those they trust and that one must be trustworthy to get assistance. Additionally, a cautionary proverb that says - *“Loshipute olo hali lika”* - the weak one often does not enjoy trust. Therefore, it is imperative that researchers aiming to work in these communities needed to understand their cultural identity especially when coming from the Aawambo group. This also required that the researchers understand the culture they worked in, and understand their roots as well as who they are.

In addition to the above-stated interviews from the underserved rural communities, two participants from the Ministry of Information and Communication Technology (MICT), the custodian ministry, were interviewed. The MICT was founded in 1990 when Namibia gained Independence, tasked with telecommunications, broadcasting, television, crafting of relevant legislation, and issues of the Internet. Making the MICT the custodian of ICT in Namibia. The two individuals interviewed were responsible for cybersecurity legislation and policies and the implementation thereof.

The figures that follow show the interviews being conducted, with COVID-19 precautions being adhered to.



Figure 4.3: Interview in Onghala Village under a tree

Figure 4.3 shows an interview being conducted by the researcher in the Onghala village with participant OM-2. The tree under which the interview took place was prepared by OM-2 for this research study, it is located along the main route that links the village to other villages and enroute to the Namibia-Angola border. Behind the researcher and OM-2 in the picture, is a flood plain (locally known as Oshana) that floods during the rainy season, cutting off the village from neighbouring villages and the rest of the country, however, leaving a connection through land with nearby Angola.



Figure 4.4: Interview underway in the Ouhongo Uakondja village under a tree in the middle of an Omahangu field

Figure 4.4 shows an interview undertaken in the Ouhongo Uakondja village. Here the researcher and OKF-1. This interview was conducted under a tree prepared by the village headman's representatives' Omahangu field. Unlike in the Onghala village, this space was more secluded as it was not near any roads or recreational facilities.



Figure 4.5: Interview in Engela Village within the homestead of the Senior Village Headman

Figure 4.5 shows an interview at the Engela Village under a tree within the homestead of the Senior Village Headman (He indicated that he would like to be identified, thus voiding western-centric Ethical clearance requirements of anonymity and respecting local individual rights to identity and representation in mainstream literary works like a thesis). In the background is the traditional sitting room where the researcher had to wait to be assisted (greetings) when entering the homestead and in this picture is also another research participant EF-1.

4.4.2 Focus groups and co-design sessions

Focus groups and co-design sessions contained a varying number of participants per village. These focus groups and co-design sessions took place under a tree in each village as community meetings. Within these communities, all residents of a village were invited, as such all that were available showed up as their time permitted.

Engela Village

Per our itinerary, we were to begin in the Engela village, Engela village was chosen as the starting point because per local customs, as an outsider, you always start by paying your respects to the senior village headman of the village clusters. Additionally, we also identified the senior headman as our intermediary for this study. Upon entry into the homestead, we followed gender-specific protocols by sitting at the holy fire in the “olupale” the traditional sitting room. We sat on the northern wooden seats (which indicates that we are peaceful visitors); each seat is connotated to a meaning communicated through its position within the olupale. The southern part usually denotes bad news or a quarrel with the owner/ a resident of the homestead. According to culture, men visiting a homestead, do not proceed beyond this point within the homestead, unless otherwise directed. This applies to ALL homesteads within the OvaKwanyama culture and by extension Aawambo people.

Olupale, serves as the reception area for men. It is also used for night-time oral knowledge transfer through practices like “Omahepu” (storytelling) and “Eengano” (idiom-based games). Also, any news from the day tends to be presented here to the homestead residents.

Once we were greeted and received, we were moved to a shaded tree within the homestead, wherein we were to conduct our study. However, after waiting for over 2 hours only 2 participants showed up. We, however, interviewed with the headman (EM-1). EM-1 instructed us to come back 2 days later to allow him time to contact those he had previously arranged to participate in our study. We proceeded, the same day to Onghala and Ouhongo Uakondja villages to ensure that the village headmen were ready to receive us on the respective dates agreed upon. These visits also allowed us to customarily greet the village leaders, introduce ourselves and pre-brief them about the research project as well.

Onghala Village

On the day we conducted our study in Onghala, we found a clean tree with some chairs arranged by the village headman. He received us outside his homestead as he was on his way out. The tree was located near a main road and close to a cuca shop. On this day, as it turns out the state-run

child welfare and pensions were being distributed within this village. People joined us as they finished collecting their welfare and pension disbursements. As such, attendance was not always consistent for both the focus group and the co-design sessions. However, we had participants between 6-9 with 2-3 people coming and going.

Ouhongo Uakondja Village

In the Ouhongo Uakondja village, we received a similar welcome with a tree and chairs prepared. All participants arrived at the pre-arranged time and no additions were made throughout the focus group and co-design sessions. The tree was prepared by a retired teacher who served as the assistant to the elderly headman. The headman also joins the rest of the community members, although he excused himself mid-way to go attend to other community matters.

Omatunda Anghala Village

Omatunda Anghala we were received by kapatashu, who prepared the village meeting tree by cleaning it in preparation for the community meeting. Here the meeting tree was also close to a road, as much as all those who passed by joined and proceeded on their way. This tree was also located close to traditional wells that are used as drinking spots for animals in the village. As such, even those who led their animals to the drinking spot joined us once they were finished and then followed their animals after some time.

In the Engela and Ouhongo Uakondja villages, the attendance changed towards the end of the sessions. Some participants left, citing home obligations like “Ohandi ka kongelela” and “ohandi katyava” which translated to ‘I am going to look for the cattle to bring them home for the night’ and ‘I am going to look for firewood for cooking dinner’.

Table 4.2 below provides an overview of the participants of the focus group and co-design sessions for all four villages.

Table 4.2: Overall Focus group and co-design session participants.

Sex	Frequency	Percentage
Male	16	34.78%
Female	30	65.2%
Total	46	100%

4.5 FINDINGS PRESENTATION

Most interviews were conducted in Oshikwanyama others had aspects of Portuguese. In the underserved rural communities, two university students opted for interviews in English, while all MICT interviews were conducted in English. Both the focus groups and co-design sessions across all the villages were conducted in a code-switching mode of Oshikwanyama and English. The researcher is a native speaker of Oshikwanyama and equally proficient in English, with an intermediate command of Portuguese. The English mostly arouse when speaking of techno-centric terminology like “cybersecurity” and “cyber-hygiene” that do not have equivalents in African languages. The need to provide justification for language is central to future work to implement the co-designed cybersecurity practices framework for underserved rural communities.

The findings presented in this section are a result of data triangulation from the interviews conducted in the underserved rural communities, MICT, focus group and co-design sessions.

This data analysis resulted in eight major themes:

Theme 1: Co-designed Community Engagement protocol

For any research to be successful, there is a need to understand how best to engage the researched community. Not only for research purposes, but also for the outputs of that research to be communicated back to all stakeholders. This theme presents the co-designed community engagement protocol validated through co-design workshops in a sequential manner.

The co-designed community engagement protocol highlights the various processes that exist within the communities that make up the case study. The protocol was co-designed through co-design sessions at each village through a democratised process. These co-design sessions were in some instance led by the community members. Community members recognise the importance of the Village Headman who leads the village, the Kapatashu who is an administrative lead for a portion of a village reporting to the village headman, the Hamushanga, who serves as the secretary for village affairs and the custodian for village office matters and regalia. In addition, the communities also provided context on the interconnection and various outcomes of these interconnection between the identified entities and actors.

For each community, a co-designed community engagement protocol emerged, these were then validated in a sequential order, and by comparison by the researcher, including all the components that are common across the 4 villages and those that are unique within the protocol. Validation is key to ensuring that the developed artefact meets utility and solve real world problems (Vaishnavi & Kuechler, 2007). The outcome of this theme was published in the Journal of paper (see Appendix D.1)

Theme 2: Existing security practices

Communities exist within this world and not in a void, they too are full of contextual factors that guide everyday life, interaction within themselves and with external actors. Additionally, communities are shaped by communal practices, values, norms, customs, and ethics. Communal practices, include migration of homesteads and animal kraals (oludilu), funerals, weddings, childbirth, conflict resolution and adjudication practices, child rearing, (Mbenzi & Ashikuti, 2018) and traditional wedding ceremonies (olufuko). These practices often have an impact on the interaction of community members with foreign objects and technologies (i.e. Cell phones,

Internet). Therefore, community members transfer, adopt, adapt, and appropriate these foreign objects within their existing mental models of being, resulting in some practices that may be enabling and other deterring secure cybersecurity practices.

This theme specifically focuses on those facets and concepts that are related to security, from risk identification as enshrined within the communal norms existing of the communities that make up the case of this study. The communities have a process that they follow that forms part of risk identification, wherein they would engage in a practice called “okupopifa no kukunda”. These practices are intertwined with technology usage. These practices can sometimes be considered secure or insecure. However, these need to be evaluated within the Afrocentric lenses of Uushiindaism and Ubuntu advocated for by Afrocentric scholars (Pellerin 2012).

The outcome of this theme was published in the conference of paper (see Appendix D.2)

Theme 3: Technology device usage patterns and device ownership

Technology has become ubiquitous within societies, and underserved rural communities are no exception to this development. This theme provides insight into the device type ownership and technology device uses by community members.

Theme 4: Online security practices (cyber-hygiene)

Underserved, rural communities get sporadic Internet access, therefore, this theme presents the online security practices of these communities, looking at cyber-hygiene practices like logging-out of online websites and mobile applications.

Theme 5: Current cybersecurity practices

When engaging with cyberspace, whether for social media, banking, or education purposes, all Internet users have certain practices that they adhere to. This theme explores the cybersecurity practices of rural underserved communities. These are categorised as secure and insecure practices.

Theme 6: Legislation for cybersecurity

The ubiquitous nature of technology means that it has become an extension of oneself, from the physical world into cyberspace and back. When interacting within cyberspace, violations are bound to occur be it between individuals, with corporations or artificial intelligence. Cyber criminals are constantly on the look out to exploit unaware and unsuspecting victims for their gain. There are also other netizens hurling insults and engaging in defamation of character for whatever reasons and other forms of cyberbullying. This theme looked at existing and future legal recourse cyber-victims may utilise to seek justice offline.

Theme 7: Telecentres

In rural areas, although access to Internet enabled devices is prevalent, access to Internet and other commuting and peripheral devices is scant. This theme presents the various services available for community members to use for educational, religious, and business purposes through the Internet and access to affordable Internet related services.

Theme 8: Community peer education

Within communities' information flows through peer education. This theme sheds light on how these communities share knowledge. These practices of knowledge sharing are imperative for the successful implementation of the co-design cybersecurity practices framework.

4.6 PRESENTATION OF THE EIGHT THEMES

4.6.1 Theme 1: Co-designed Community Engagement protocol

From the co-design sessions, a community engagement protocol emerged. This community engagement protocol was validated by design comparison between the four village. This protocol sets out how engagement should occur, which should be contacted and how consent is sought within these communities. As presented in the Journal Paper (Appendix D.1), any engagement activities need to start with a researcher or a local informant contacting the senior village headman seeking permission to conduct research within that village (Stanley, 2020, p. 64).

However, there are instances where the researcher might not be known to the village headman, as such from our personal experience, there is need to send a trusted member of the community to represent the researcher. Researchers within the community-co-design space and decolonial scholars also assert that having a local person (local to the community) on the team as a co-researcher - a native researcher – has a great impact on project success (Kapuire, 2023). Additionally, this co-designed community engagement protocol speaks to Cultural tightness-looseness Theory, which to an extent deals with the sanctioning that can happen within a community due to deviant behaviour (Gelfand et al., 2006). These communities as observed during the co-design sessions, are tightly bonded, meaning there are shared norms that form part of the culture that guide aspects of daily life, e.g. greeting others, politeness, and hospitality (see the experience of data collection, where the meeting areas were prepared for us – section 4.4).

4.6.1.1 Leadership structure

The OuKwanyama Traditional Authority governs the villages where this study took place. These villages are led by Village Headmen, with a hierarchical structure, starting from Her Majesty the Queen all the way to Kapatashu who are responsible for smaller segments of a village, which is led by a junior village headman. The Junior Village headman reports to ‘ediko’ which is led by a senior village headman.

4.6.1.2 Power struggles

Traditional authorities exist within a democratically elected government which is made up of a political system. For effective governance, the country is demarcated into regions (governed by a Governor, who is appointed by the sitting president) and further into constituencies. A village from the political system standpoint falls within a constituency. These constituencies are governed by local councillors who are elected by the people through political parties.

The above description also then means that community members within a constituency are led by a councillor, therefore, permission needs to be sought from the councillor as well. For efficiency, these two processes of seeking support from the village headman and the councillor

should be done simultaneously. This arrangement of a traditional leadership and a political leadership presents from power struggles between the two institutional structures of governance. Given that they are disparate, some believe that they are independent of each other, others that they are under the other's leadership, one community leader lamented that

“Many village heads are left behind by developments that are occurring around them. For instance, when a councillor is elected and takes office, their first stop are the village heads, instructing them to rally the people. This now means that the village heads have no way to defend themselves, even when they say they are busy. The councillor will scold them, that they gave an instruction to rally their community member. Essentially, turning community leaders into errand boys. This has nothing to do with collaboration, collaboration is important and should be there. However, now it is just like you are in your fathers' house and you make your father you son. Now that you got married, you are instructing your father, 'dad go look for the cattle'; 'the olupale does not have firewood, let me find that you have collected firewood for the holy fire (okutyava)' (laughter). Additionally, the village heads in terms of national legislation are nowhere to be found, especially in terms of the” – EM-1

4.6.1.3 Anonymity in research

The concept of anonymity in research was also interrogated in line with the Oshikwanyama proverbs of “Omweenge mwenge tala kefo” and “Okaholameno kopondjila omanbodwe” whose sentiments were earlier reflected in section 3.10. A participant stated that the concept of anonymity is foreign and only valid if he was hiding something or lying stating;

“If you say it is the village headman, obviously, there should be a name attached to that title. Maybe there are those that do not wish to have their names identified, I would want to have my identity hidden if what I am saying is not true. I know that those are procedures that you need to follow by asking participants, however, for me you can identify me by name, this is to show you how open and truthful I am being”. – EM-1

4.6.1.4 Communication to the community

Once consent and permission to conduct the study has been given by the village headman and the local councillor. The village headman, and secretary “*Hamushanga*” to the village headman notified the affected community members of an impending community meeting. This is done in person, peer-to-peer through word of mouth, church, and various committees (water, health, community policing, etc.). The local councillor also informs the affected villages of any research meetings through official channels to schools, and via national radio stations. The communication should contain the date, time and abstract overview of the community meeting. Once the community members receive the communication, they inform the Kapatashu about their agreement and this is communicated through the leadership structures up until the village headman communicates to the researcher in the affirmative and any changes as may be necessary.

Figure 4.6 presents the co-designed community engagement protocol. This protocol is to be used in conjunction with the proposed approach for community-based research approach as applied in this study (see Section 3.5.2 Methodology Used in this study). Taking contextual factors like rains, field work (tilling, sowing, and cultivation periods), into consideration as part of the pre-planning stage in Figure 3.5 of the proposed approach.

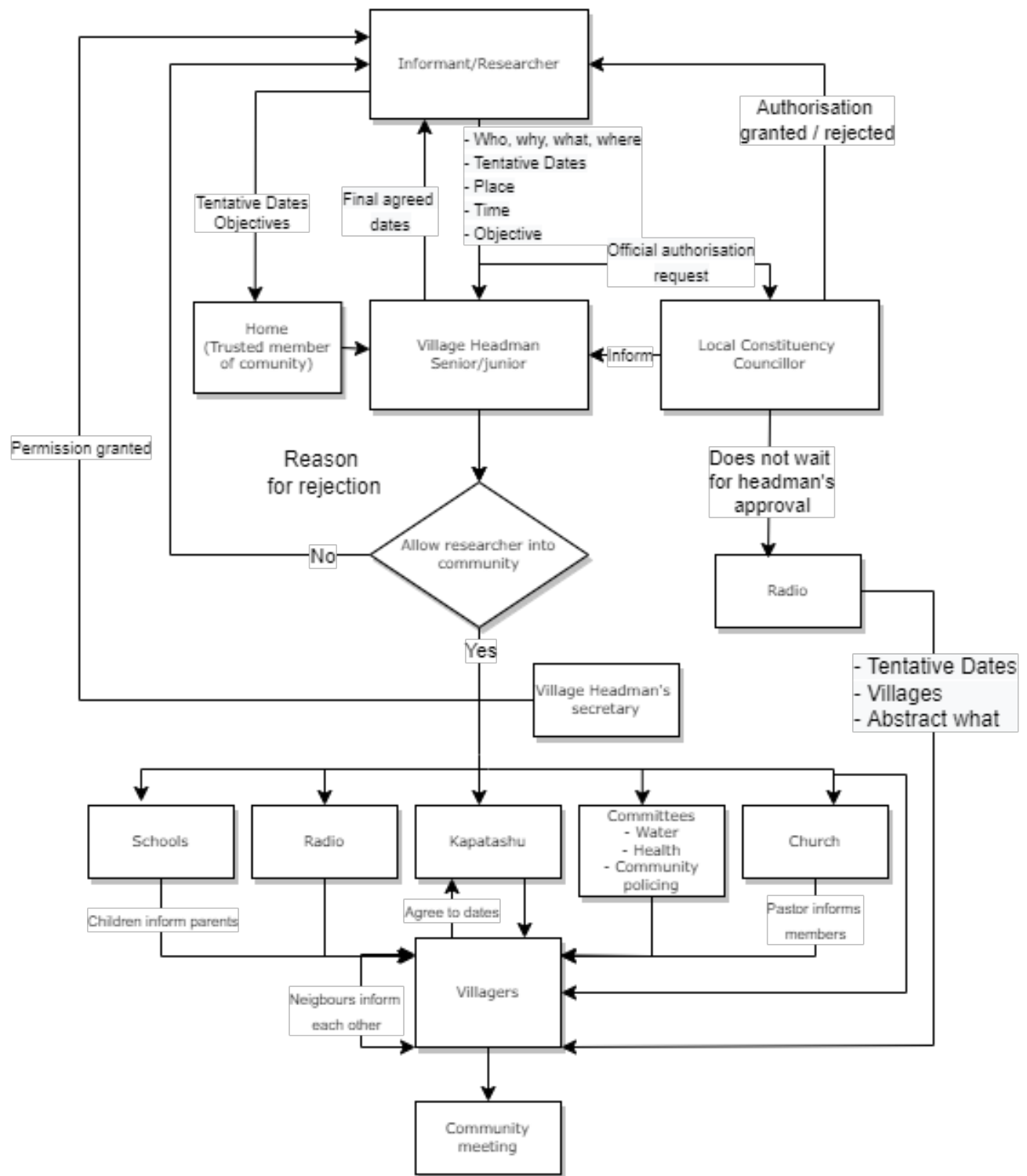


Figure 4.6: Co-designed Community Engagement Protocol (see Appendix D.1 for further reading)

4.6.2 Theme 2: Existing security practices

Within communities, there exists various aspects that are inherent to the people, these include, values, norms, practices, and ways of life which make up the culture of the people. These aspects of rural life within the villages wherein we conducted this study guide the way in which they exercise values such as trust and the levels to it, information sharing, and issues of community development. Existing security practices are majorly dependent on the trustworthiness of a person.

4.6.2.1 Trusted persons to render assistance.

Community members often face challenges, and when this occurs, they seek assistance. They seek this assistance through persons they trust. This trust sometimes is based on friendships, or a job title a person holds within the community; familial bonds, like a child assisting a parent with a device or a child trusting their parent with their banking information, cards, and pins. A participant narrated that,

“Yeah, the laptop. Yeah. I do contact some of my friends. Like maybe when I can't like really to figure it out. Like at first when I bought it, then I have to like to call up my friend and ask them how to operate some things on this laptop” – OKF-1

“There is something that is sent by a [mobile operator], sent from [common SMS number] I answered it, and it was eating my credit then I give it to [my daughter] to remove it.” – OM-4

Another participant further added

“I ask her because, she is my child, and she is the one who supposed to free me (assist me). I also ask the boys, but [my daughter] there is the one that is often near me in close to me – OM-4

“I ask my child for help, because they understand these technology things better” – Omatunda-Anghala focus group participant

However, with the advent of innovations within the telecommunications space, well intended to allow end-users to communicate even when not having the finances to afford credit (minutes) to make phone calls, this trust has been eroded. Some participants indicated that they now fear borrowing their phones to their children in fear that they will request taamba² and when they go recharge their credit, that credit will go pay the debt of taamba. A participant stated their views as follows:

“I sometimes share my phone with my children, but there was day that I recharge my airtime, and it was gone, then I realised the only reason this is happening is because somebody requested taamba on my phone and then deleted that SMS. Now I do not like them taking my phone to make phone call or even just to go watch videos because when I asked to request taamba on my phone, it was nobody” - Omatunda-Anghala focus group participant

Another focus group participant shared his view, stating that even though he went to school, he still struggles with English and the use of services like automated teller machines (ATM). To get assistance, he would rather ask a trusted neighbour to assist him, especially when having to get money from his mobile money wallets from the nearest town. However, he lamented that now he would have to take care of the needs of that person like transport, and food since the town is few kilometres from the village. He adds that sometimes the money he must withdraw from this mobile money wallet does not cater for additional expenses but is just enough to take care of a financial need. So, he is forced to go to town alone and seek assistance from a stranger that he deems trustworthy, like the security guard at the ATM or any other person he feels he can trust. He concludes by saying, sometimes he just hopes the person he finds does not rob him or swindle him.

² Taamba is an innovation that allows mobile subscribers to borrow minutes to make phone calls in lieu of a future recharge. Once a taamba has been taken for a particular value, the next recharge will replace value of the borrowed taamba minutes.

4.6.2.2 Trust of people (strangers)

In a community, house members often attend to strangers seeking assistance. The extent to which house members assist these strangers depends on the type of assistance required. Therefore, upon the stranger narrating their reason for visiting, the house member subjectively determines the authenticity and legitimacy of the stranger's request. In doing this, the house member is often guided by various factors such as manners, dress code, posture of the stranger, and the type of assistance needed based on the information presented. Based on the analysis of these various factors the house member makes a judgement whether the person's request is genuine or not. Primarily, the house member scrutinizes the stranger for potential risks or threats of exposure and accords the relevant assistance. A participant shared his views about assisting strangers as follow:

"I will get the visitor's intentions. Thereafter I will contact my parents and housemates if they are expecting any visitors and if none of them are expecting visitors, I will handle the situation my way." - OM-1

Others indicated that

"If it's something that I know, for example, something that is general does not involve like me giving away personal information, then I will help. But then if they may be asking about my personal issues or somebody's, then I will not answer." - OKF-1

"At least I will just assist the person with what he is asking but then not something which is inside the house. If I do not know that person maybe he's asking for help, but maybe he's lost or something like that, I will assist him or her. Okay. But then if he wants something and then I know that it's in the house, there's no way can assist with because I don't know him or her." – OKM-1

4.6.3 Theme 3: Technology usage patterns and device ownership

4.6.3.1 Technology Device ownership and type

Technology device ownership is prevalent in these rural areas. The type of device ownership ranges from basic feature phones (Katoshe), to smartphones, tablets, and laptops. This indicates that they use their devices for a variety of reason. One respondent indicated that they owned a tablet, smartphone, and a laptop.

“All of them they have Internet, except for the Katoshe. But then I just prefer my [smartphone] phone more.” - OKF-1

“I have a smartphone and a Katoshe” OF-2

“I only have this one phone (smartphone)” – EM-2

Another participant indicated that he owned multiple phones, however, one has a broken screen, and he will not fix it whilst he has his present smartphone.

“I have had two phones in my life, one is this one that I am using, and the other one has a broken screen, but I will not fix it while I have this one” EM-2

A participant indicated that she owned two smartphones, and a Katoshe, adding that the smartphone was entry-level and when broken she will not fix it. The ownership is just so that one has a means to communicate especially because she lives in the village, and she sees no need to have a fancy phone.

“I just keep this one to communicate, like now for some of us in the village, what do I really want to know. Imagine even if there is a meeting somewhere I would be the last to know.” – EF-2?

4.6.3.2 Technology device usage

Ownership of computing devices services multiple needs. For some community members, the usage between devices has varying levels of difficulty. Some use these devices for school

purposes, sending text messages, making phone calls, completing job application forms, social media, listening to music, etc.; however, some participants also noted that the advent of computing devices has caused a fracture in the social fabric of the community, where practices such as Oxungi³ are no longer practiced, as household members have become antisocial. This antisocial behaviour has also caused a level of aggression when prompted about it. The harmony that existed is slowly being lost.

“Uh, the laptop is for typing my assignments. The tab is for studying the phone is for Internet now and text messages, calls.” – OKF-1

“Mostly I use my phone just to get information on the Internet or perhaps like when I was at school, like, you can read something in the book, but then there is a word, and you just do not understand it. You have to take your phone, then you have to Google for you to give the answer or to get what you want. Okay. And also like to apply. Nowadays people, only used to apply vacancies through email. Yeah. Or through website?” – OKM-1

“Sometimes you see young people listening to music on their big phones. Even if you go visit them and you are sitting under a nicely shaded tree, forget about talking to that person, they will be listening to their music with heard phones or watching their videos. Even at home, some people especially those who are addicted to their phones, they will not even greet you. Now it is difficult to just go a look at what that person is doing on that phone, because sometimes they are also chatting to their friends, or on WhatsApp or on Facebook. So, they just sit there on their phone. It has even come to Oxungi not being practiced anymore, but at least those of us with Katoshe’s we will be laughing and talking our stories. Even if you ask why they are being anti-social just being on their phone, they will tell you that it is their phone. So sometimes a person doesn’t also know what to do because sometimes people are also filling in forms their phones” – EF – 2

³ Oxungi is a nighttime discussion practiced by the Aawambo people. These discussions range from the days’ activities, news and as well passing on of cultural knowledge and practices.

“My friends and I use our phones to write to each other, especially since we are from each other through Facebook.” – EM-2

Another participant indicated that he uses his phone to call community meetings with village residents for administrative purposes and to create a platform for community leaders to network. Additionally, the use of WhatsApp also allows for the sharing of traditional knowledge with the youth, to combat societal moral decay. One participant indicated that:

“I use my phone to call people but also to send SMSs for community meetings or when I have announcements to make. However, I am having a challenge with getting young people to come for community meetings. I heard that there are some youth groups on the likes of Facebook for Engela, however, I am not involved in those groups. Even now that you are here, it is my intention for you to help me establish a WhatsApp group for the village today. Just imagine, if we had that WhatsApp group, we could have had so many people attending to this meeting how, all at once and that could be effective communication. Now that we are struggling to get people here, is because of the lack of effective communication. So, for those who are coming today, we will create our WhatsApp group for the village, I have been longing for it for a while now. Like now, I have already created another WhatsApp group for all the village headmen not only for the Oukwanyama traditional authority, but for all the village headman throughout the country. I am trying to get you, the youth to come closer to the leadership so that we can teach you the traditions and customs. Because we can see that there is an erosion of manners which can be because you do not understand your values” – EM-1

These findings are like those of Shihomeka and Arora (2018) who found that youths in rural areas utilised mobile devices to communicate with others regarding issues of employment, and study opportunities. Additionally, he found that youths living in urban areas would call their fellows in rural areas when such opportunities arouse. Thus, cutting the long journey rural youths would have to travel to the nearest towns to access information.

4.6.3.3 Awareness of technology device security features

Some community members indicated that they utilise mobile device's in-built security features to secure information they consider private. Information such as SMSs and other applications are installed on the mobile device, and they enable application specific security setting. A community member indicated that

"No, I don't share with them, but then perhaps those people can be so clever. They can maybe behind you, like looking at you while you're putting in your password, then tomorrow, you find that person, like, like with your phone and then you be surprised how (GN (16:57): Yeah.) and from there, just to change your password." – OKM-1

4.6.3.4 Disposal of old devices

Community members indicated that their current technology devices are not their first devices. Some devices got lost, stolen, or they gifted to someone else. Some community members indicated that even though they have old devices they clean them first before giving them to the intended person. A participant indicated

"When my phones got old, some I gave away, one got lost. One was taken from me, but I got it back" – OM-4

This community member added that

"I have two phones that were taken from me. One cell phone, there was a young man that approached me in Oshikango and started touching my shoes in Oshikango. Why are you pulling on my shoes? He responded in Portuguese. I didn't understand him, then he came back and repeated it again. I almost beat him up. As we engage with the young man, my phone was in here (he points to his pants pocket). When he left, it seemed that he had just taken the phone with him. I didn't even think about the phone at that moment, I was just angry that someone was touching me and my shoes. When I got home, the phone was already gone. there was nothing! The other one was taken from me in this manner, I think a young man was just tailing me (okulifa omunhu). I was talking on the phone with

another person who was asking me about a Nissan Hardbody, I told him the Nissan's gearbox is broken, and I informed him that the car is not being scrapped, he was asking for spare parts. Then he said just tell me maybe when you get a gearbox, I might be able to afford the car. That was it, just when I walked a short distance like to that Omusati tree (a short distance from where we are seated) another Youngman stopped me, then approached me asking if I want to buy fuel. I said I don't want to buy fuel; he said his fuel is cheap and that he wants to go re-stock then I said even if it's cheap my car is already full, I don't want fuel. He then also proceeded to say he also sells many other things. I asked him, things like what.? then he said, even auto spare parts. Then I said I am looking for a Nissan gearbox, then he asked, what model Nissan? So, I said, a Nissan Hardbody gearbox. Then he said, there is a Hardbody at our neck of the woods (oshilongo shetu-to also include villages around where one lives) that is on stilts, but I am not sure if it is being scrapped. So maybe I can go and ask the owners, so maybe I can just show you where I stay, so that when you come tomorrow you can ask for me. I then asked him, where are he was going? he said, in the same direction as you, then he said, you can just take me with, and I will show you my ghetto where I stay. Then I gave him a ride in my car, then he said, what is best, let us exchange cell numbers. Then I agreed. Then he said, since you are driving, give me your phone so I enter my cell number. The moment I stopped he ran away with my phone!" – OM-4

4.6.3.5 Private information on technology device

During the focus group discussions, participants indicated that they do keep private information on their technology devices, indicating that there is some sensitivity to that information, and they would not want it to be seen by everybody. A participant indicated that, even though the information is not for all to consume, it does not mean that it is necessarily bad, just that sometimes it might cause harm to another person.

4.6.4 Theme 4: Online security practices (cyber-hygiene)

4.6.4.1 Computing device Internet access

Some of the participants indicated that the ownership of smartphones, which have Internet access capabilities. Another, a university student, indicated that they utilise a university issued Internet dongle to access the Internet, but lamented that it sometimes does not work in the village, but it worked when they were in the Windhoek (the Capital City of Namibia).

4.6.4.2 Frequency of Internet use

Participants indicated that they use the internet multiple days a week, adding that this sometimes is contingent on having access to mobile data, which in some instance they have to rely on friends and family to provide them with data bundles or with mobile credit.

“I use the Internet when I get data. So sometimes maybe like twice a month. Or if you are lucky, somebody can even send you like your cousin, or your uncle, can you even send you may be like credit. When your aweh finish then you just register another one.” – OKM-1

4.6.4.3 Internet usage

Most of the participants indicated that they use the internet, but mostly for communication, education, job seeking, and entertainment purposes. They indicated that they use the Internet to communicate with distant friends, which they achieve through platforms like WhatsApp or Facebook.

Other participants indicated they use the Internet for University studies, mostly to access electronic learning systems and research for concepts previously unknown to them. In addition, they also use it to apply for jobs, as most organisations prefer online applications. In addition to job applications, they cited sharing information they believe could benefit their peers and online friends or simply entertaining themselves.

“I mostly only use WhatsApp on Fridays is when there is a church announcements message that comes from the church.” – OM-4

“Mostly I use my phone just to get information on the internet or perhaps like when I was at school, like, um, you can read something in the book, but then there is a word, and you just do not understand it. You must take your phone, then you Google and Google for you, to give the answer or to get what you want. Okay. And like to apply. Cause nowadays the people, they only used to apply vacancies through email. Yeah. Or through website? Also, that one it already just depending on the, the data, if I have data and then yeah, that I can use it if I wanna do something. So especially on WhatsApp. On Facebook. Mm, yeah. May be even on Twitter also” – OKM-1

Some of the participants, however, did not connect Internet usage with WhatsApp and assumed that they are disparate.

4.6.4.4 Awareness of Internet advantages

Some participants noted that they are aware of the advantages of the Internet, how information is readily available as opposed to visiting libraries.

“Yeah. It's fast and simple. Like, and then also get information like fast instead of, um, maybe searching it on a book or you read somewhere then you're not comfortable with it. Just take, find it in your Google, get it just fast and simple and easy to use.” – OKM-1

“I mean like for now, for us that go to school, when you like have a difficult question that you cannot do on your own, you can always search for the answers. Yeah. And then maybe some, well, you know, when you don't go to school and you like cooking, you can always like search up for recipes to cook. Yeah” – OKF-1

4.6.4.5 Awareness of Internet disadvantages

Those that were and understood what the Internet is, also cited that the Internet provides a platform for societal degeneration. Adding that societal values sometimes are not adhered to by the youth, who end up insulting elders through social networking site. They also stated that another disadvantage of the Internet could be its addictive potential, leading to people not applying their minds to activities and simply thinking the Internet can solve their tasks. A more

worrying side effect of the addiction the participants indicated was the time-loss and neglect of their studies.

“I hear that sometimes people speak about things that should not be spoken about on WhatsApp. That there is no respect, and that the youth are really insulting the adults badly. That is what we hear.” – OM-4

“Maybe like, it can be addictive. Yeah. You depend on it like too much and then sometimes you cannot even think like, you would be, you, you rely too much on the Google thing instead of like, just thinking and then like maybe on the social media stuff can be too addictive. You Can even forget that you must study.” – OKF-1

4.6.4.6 Cyber-hygiene practices

Respondents have myriads of cybersecurity practices. Most of these practices are unconscious and often people do not understand what they are doing sometimes accepting to participate in competitions without understanding the terms and conditions, they also do not read the terms and conditions of applications when installing them. There is a sense of inherent trust for those that provide services like telecommunication providers, therefore, leaving themselves exposed to negative technological experiences. Actions like subscribing to games via SMS could have an impact on their access to services like cell phone banking. Additionally, due to societal expectations of modesty and truthfulness some respondents indicated that they do not share personal details of their lives online (social media). Adding that they also prefer to only share information that they are certain to be true. They however, in some instances did not vet the quality of information that they received from trusted persons, especially through messaging applications like WhatsApp that offer an intimate feel and expectation.

To the issue of being unaware of subscriptions effects on their ability to transact one respondent indicate that

“When I register like super-Aweh there was like remaining N\$20 and this happened maybe three days, when I want to check my balance on my bank account through cell phone

banking it is saying insufficient credit. So, I called MTC to ask what happened to the remaining N\$20 that I had on my phone after registering for super-aweh. I needed answers like how my money could disappear. Yeah. Then from there, they told me, like apparently, I used to like to play a lot of games, like those ones on 101. And then I never knew if they can maybe take credit then from there they say, if I want to (un)subscribe them, I should do it, I should just send the saying that something STOP then from there they (un)subscribe it. So, they told me that my credit used to go because of those games, even this Euro game that was in June still. I received that in SMS form 101. Like if I want to win a kind of money, I should say YES, then I ignore it.” – OKM-1

Additionally, they do not read the terms and conditions when installing mobile applications or documents from the internet, simply opting to receive the documents or seeking access to a particular application.

“Oh, sometimes those terms and conditions they used to belong, you just to scroll until it's written, download and then you download.” – OKM-1

Most respondents indicated that click on links send to them. They assessed the type of link but

“Uh, sometimes, uh, I used to [click on those links], especially on WhatsApp, I used to do it. And then from there, on WhatsApp, once you click it, there will be some information that says, congratulations you won something for you to continue, you must share those on WhatsApp, maybe 20 groups or five, or five people. But then it's not really true, it just kind of, uh, yeah, you can share there, but then they won't, they won't, they won't give you feedback after done sharing. It's like just of no use.” - OKM-1

“The threats do exist, except they are not aware of the existence of this threats, so they will click on any link that is shared on WhatsApp. They will click on anything that's shared via their Facebook profiles, so eventually that's a threat to them.” – MICT-1

Clicking on links especially those emanating from friends, neighbours, and church WhatsApp groups is often explained by the Cultural Theory of Risk. The Cultural Theory of Risk as presented

in Section 2.8.5 which argues that attitudes and judgements about risks are attributed to cultural relationships that guide the values and expectations for people belonging to a distinct group (Tansey, Tim, & Riordan, 1999). Within this community, there is an expectation that others only wish one good, because they can do no harm to them. Therefore, they are likely not to send malicious links, resulting in explicit trust and this is what cybercriminals exploit through malicious links.

In some instances, respondents indicated that they do protect their online profiles with unique passwords. This finding is like those of Golla et al. (2018) (as presented in Section 2.6) who found and advice that end-user create unique passwords for all their online accounts.

4.6.5 Theme 5: Current cybersecurity practices

Data analysis indicated that there were cybersecurity practices that residents in rural areas practiced. These practices were placed into two categories, secure security practices and Insecure security practices.

4.6.5.1 Obfuscating confidential information

Security breach incidents led to change in the way that some participants stored the data they considered private on their phones. This new practice is confidential information obfuscation, whereby only the person that created the “code” knows what that information represents. This was mostly in relation to how cell numbers are stored on the phone. Ideally, this is done by saving the first name and last name of the contact as prompted by the cell phones’ user interface. To this a participant indicated

“OK, firstly OK, what led me to put these codes in my phone stems from an incident that happened. We had cousins in our house, they are girls actually, I store their numbers in my mobile. Then these neighbours used to ask me about their numbers and then they told me that I must not give them their numbers. So, like this guy has to steal the numbers from my phone. Then the first thing I did is like this way of saving people numbers with let me say question marks, exclamation marks in it. Yeah well, codes just for you. You know which

person is which, so that others can have access to your contacts, but won't know which one is which.” - OM-1

This practice is similar to the findings to Szumski (2018) who found that users tend to create complex passwords in hope that no one else can get access to it. Obfuscation is not unique as a concept, for instance Gerber et al. (2021) found that if a need to deliver private information arises, end-users would use a foreign language or “code” to exchange sensitive information. However, the obfuscation of the names of contacts is unique to this study.

4.6.5.2 Change of shared passwords

Participants indicated that they do from time to time share their technological devices with others like friends, family, neighbours, or strangers that need assistance to make calls, send or check e-mails etc. However, since the prolonged use of the prevalent device which is the smartphone could lead to lock-screens they share the security passwords to log into those devices. Once the devices are returned, they change the passwords in fear of future unauthorised usage. A participant indicated that they started this practice after a neighbour who was persistently asking for the cell phone number of a female relative who came to visit for holiday, managed to access their phone and get the numbers themselves. This scenario caused some conflict between the participant and their family, thus prompting the change when the device and password has been shared, although they still do share their device with said neighbours if the need arises. Resulting in amended trust of the neighbour.

Scholars like Golla et al. (2018) and Szumski (2018) also advice that end-users change passwords that they believe to have been compromised. Golla et al. (2018) go a step further suggesting the use of password generators and subsequently password managers to avoid the leakages of these passwords.

4.6.5.3 Public Wi-Fi use

Some of the participants indicated that they make use of publicly available Wi-Fi connection when they make trips to the nearby town of Helao Nafidi. Making use of the Wi-Fi at fast-food

restaurants and the regional public library. In essence they did not indicate usage of tools like virtual private networks.

4.6.5.4 Limited cyber-risk identification

Risk identification in cyberspace was not indicated by some of the participants, with an Interviewee from the Ministry of ICT indicating, there are instance where a person might be compromised but they are not even aware, since they do not know the difference between normal internet access and compromised access.

“I'm sure the rural communities are equally not well informed or well learned to differentiate what a normal Access to Internet is and what is probably a cyber security threat because what we have observed is that we see in WhatsApp groups you'll see the rural community when they pick something from the WhatsApp groups. They will always forward it to you, maybe one of the well learned Cousins that they think he will be able to know what this is and explain, or if it's laughable then they will share these links. But definitely there are no reports coming directly to say I see this looks like a threat. So, what does that ministry think about this? No, don't get that.” – MICT-1

This was also confirmed by other participants from focus groups in the rural communities, who would click on links sent to them by friends or those that they found in WhatsApp groups. Especially, church groups, you find posts that come with links indicating that money or a prize is up for winning. This finding is no unique to rural underserved communities but rather has to do with the nature of humans.

In other instances, the participants indicated that loss of mobile credit due to games they signed up for was a common occurrence, this however, they cite not comprehending the messaging from the telecommunications providers who run these advertisements through SMS.

4.6.5.5 Cybersecurity knowledge and awareness

Cybersecurity in the country is taking centre stage, and the relevant line Ministry is taking steps towards getting the citizenry aware of it through the development of a cybersecurity awareness

strategy (Republic of Namibia, 2022b). They however, indicated that this strategy is not specifically targeted to rural areas and not in local languages for the meantime.

The knowledge and awareness of cybersecurity in the country, especially within rural communities is a matter of concern. With a respondent indicating that even though efforts are being made through existing platforms like the Information Communication Centre⁴⁴ to educate the nation on this crucial issue, there remains a mismatch between the message and the masses. This mismatch can be attributed to the language used to communicate cybersecurity awareness messages. This was also a finding by Quayyum and Freberg (2023) who found that participants in their study struggled to understand certain security-related concepts and words. Further adding that some participants did not relate to the idea or meaning of the concepts and words. These are like the findings in the present study.

Most respondents from the four villages indicated that they are not aware of the term cybersecurity. With only one participant indicating that they have heard of the term before in high school and in passing with a primary reading, another indicated that it was taught to them at university

“Hhmmm hmmm I never heard of that word” – EM-1

“In school that was like in high school. I think it was just like in a story that we were reading in a class if I'm not mistaken. At that time, I did not understand it, not really. Like I did today.” – OKF-1

Even though the knowledge of the term was low, instances and awareness of cybercrimes are evident. Some respondents indicated that they experienced through social engineering attacks, the attacks experienced can be categorised as forms of vishing and smishing.

⁴⁴ The Information Communication Centre served as a central platform to communicate COVID-19 news. This platform is both physical and streamed online through social media platforms and on national radio to reach the masses. This platform was created by the Ministry of Information and Communication Technology to avoid and curb Miscommunication and Disinformation. The platform has garnered authenticity and many still follow publications and communications that stem from this platform.

In other instances, respondents indicated that they heard of social engineering attacks through their church services where the pastor narrated their own ordeal and heeding caution to parishioners to be cautious. Other community leaders like the National Police also utilise the national radio to warn people of the existence of cybercriminal and share some of their tactics.

4.6.5.6 Password/pin sharing

From the focus groups, some participants indicated that they share their passwords and pins with loved ones and family members. The elder participants indicated that they trusted their children and believed that their children are their eyes and will have no bad intentions towards them, therefore, they implicitly trusted their children. Leaning towards the Oshikwanyama proverb of “*Ohonde okupona oi dule omeva.*”⁵ And “*Nekwa litoka oye ngoo nyoko.*”⁶ And “*Kaxuxwena hadela nyoko, nyoko onale e ku hadele.*”⁷

4.6.5.7 Unique password combinations

Some of the community members indicated that they have passwords on their devices that they crafted in such a manner that only they can understand and remember. They avoid using common facts and things that are known by other people.

4.6.5.8 Lack of passwords on electronic devices

Some of the community members indicated that they do not have passwords on their phones because they could forget the passwords and there is no valuable information in their devices. They did, however, narrate how sometimes they lose mobile credit or mobile wallets they receive because of this.

⁵ This proverb is translated to ‘Family members will favour each other over strangers’

⁶ This proverb is translated to ‘No matter the state of your parent, they are still your parent, and you should respect, honour and love them regardless’

⁷ This proverb translates to ‘It is the responsibility of children to care for their parents, for their parents too cared for them when they were young’

The lack of passwords on technological devices was also observed by researchers working with first nations (indigenous) communities in Canada, especially among the youth who also tended to share devices (Tanner et al., 2023). The sharing of devices is also similar to finding 4.6.5.9.

4.6.5.9 Electronic device sharing

Community members indicated that they share electronic devices with friends, family, and neighbours. Adding that this is a reciprocal relationship, this sometimes is because they too might not have mobile credit and need to make calls or SMS someone, or their devices are not charged, as device charging costs money. Others indicated that they share their siblings' feature phones because their smartphones simply do not get cell reception in the village.

4.6.6 Theme 6: Legislation for cybersecurity

In Namibia, cyber legislation is lagging and has been in development for a few years. However, there have been setbacks in the development of a cybercrime bill stemming from bottleneck failures in the legal drafting process and budgetary constraints. To this end, other pieces of legislation that address areas that as electronic transactions and digital signatures have been passed. A respondent indicated that the lengthy law-making process is causing these delays.

Therefore, for those that wish to take the legal route for any damages suffered within the cyberspace, the criminal and civil laws can assist in this manner. A respondent indicated that there has been high profile cases that have been successfully tried through this procedure.

4.6.7 Theme 7: Telecentres

Information and Communications Technology equipment is a scarce resource within rural communities, however, the MICT has availed projectors, monitors and PA systems for the community to rent at an affordable rate. Albeit these only being available at the closest towns to the rural community and not having internet capabilities. A respondent stated that

“Although it's not really technology oriented but then as a ministry there is PA systems for sound and meetings and conferences that is currently at the regional offices and then the

rural communities and surrounding towns are actually making use of that through hiring it at a very minimum fee of N\$350. So that's all that I know, but as far as telecommunications and other ICT services as a ministry, no, we're sitting at the helm of ICT policy development and the regulations mainly.” – MICT-1

As at 2021 the National Planning Commission reported that there were 24 Ministry of Information and Communication Technology (MICT) rural ICT centres which were all equipped with ICT equipment and Internet access. The MICT reports that there are 26 regional ICT centres in all 14 regions. In addition, there were 65 regional libraries of which 60 had access to Internet services. These libraries are mostly used by youths to access online education and online job application.

“Yes, the access to Internet is free of charge and the copy machines that are there are the ones that also have a small fine of N\$0.50 per copy” – MICT-1

4.6.8 Theme 8: Community peer education

A respondent indicated that he nearly fell victim to a social engineering attack. Adding that they use the names of reputable organisations coupled with the possibility of winning money in almost believable terms. He added that if it was not for his father that informed him to rather ask that he collect item he won physically from the respective organisation, he would've given them his entire banking details and by extension lost his money.

Within communities, people tend to trust those that are educated, or those they share a close relationship with. These relationships can be formed due to blood relations, clan relations, friendships, or due to the positions someone holds within the community structures or institutions that are perceived to be trustworthy, like teachers, nurses, and police officers. This notion of peer education within the community, is similar to what McAlaney and Benson (2019) refer to as the social influence, the perceptions that people within a group have of each other can impact their cybersecurity behaviour. In addition, Dolan et al. (2010) argue that for cybersecurity information to be impactful and have intended behavioural change, through the MINDSPACE framework, the messenger is a key component to that success, considering the

varying norms, contextualisation of salient way of doing things, and breaking the defaults or pre-set way life. A respondent indicated that these would be the best people to assist with community peer education. As part of community policing, the Namibia Police Force does from time to time patronise the Oshiwambo National Radio service, where community members indicated that they receive some information regarding the new scams unscrupulous individuals use to swindle funds through cell phones. A notorious scam that the communities narrated was that of someone that calls during times of bereavement.

Much like other Sub-Saharan communities, the OvaKwanyama belong to clans, however, due to a myriad (better work opportunities, school, medical care, etc.) of reasons, these clans have dispersed across the country. Therefore, family members' spokesperson would make a radio announcement about a bereavement, informing all clan and community members of the passing of a loved one. Criminals would then send an SMS formatted like a mobile wallet transaction from a banking service to the contact persons provided. Immediately, they would call that person indicating that they are a relative who send some money, however, they sent more money than they anticipated and would need some of it to travel. Under normal circumstances, the contact person would be able to vet the caller through the normal traditional system, however, due to the bereavement, and sensitive time, they are likely to believe the criminal and send money. At this time the contact person would've received many legitimate contributions towards the funeral costs, as such they sometimes are an easy target. The police warn of these scams, but they still work, for greater success, the scammers pretend to be elderly, relying on cultural values of respect for the elders to dispel any potential suspicion of their impending crime. The challenge of a trusted person to provide cybersecurity information was also identified by Szumski (2018) in the study on the cybersecurity practices of Polish students.

4.7 CHAPTER SUMMARY

In this Chapter, the results of the data analysis were presented. Data analysis followed a thematic analysis process, data were recorded, most were transcribed and then coded. These codes were synthesised into themes. The themes were then validated through discussion with the participants (Creswell & Creswell, 2018).

The Chapter began by contextualising the case site, giving a background of the 4 villages, the structure, governances, spirituality, and communication protocols, both spoken and unspoken. The analysis yielded 8 themes, namely, co-designed community engagement protocol; existing security practices; technology usage patterns and device ownership; online security practices (cyber-hygiene); current cybersecurity practices; legislation for cybersecurity; telecentres; and community peer education. These themes provide an understanding of the rural underserved communities that form the case study. Giving a glimpse into the mental model of how technology is adopted, assimilated to and how it also shapes the community over time, the Chapters' themes also provide alternatives to community members that have fallen prey to cybercriminal through legal route as seen in theme 6. The last theme (8) in essence gives a potential way forward towards utilising existing peer education to further the cybersecurity discourse and discover and identify new practices from the community over time, centring the African through the Afrocentric lens (Pellerin, 2012).

The next Chapter presents the co-designed cybersecurity practices framework for rural underserved communities.

CHAPTER 5: CO-DESIGNED CYBERSECURITY PRACTICES FRAMEWORK FOR UNDERSERVED RURAL COMMUNITIES (CCSPF-4-URC)

5.1 INTRODUCTION

The previous Chapters grounded the study in the existing body of literature and presented the key findings from the current research. In this Chapter, we present the Co-designed Cybersecurity Practices Framework for underserved rural communities (CCSPF-4-URC) design process. Elucidating the key components as guided by previous Chapters' outcomes.

5.2 CCSPF-4-URC FRAMEWORK DEVELOPMENT

A framework provides guidance to a researcher in identifying gaps and it is a foundation upon which research is built. Jabareen (2009) defines a framework as:

as a network, or "a plane," of interlinked concepts that together provide a comprehensive understanding of a phenomenon or phenomena. The concepts that constitute a conceptual framework support one another, articulate their respective phenomena, and establish a framework-specific philosophy. Conceptual frameworks possess ontological, epistemological, and methodological assumptions, and each concept within a conceptual framework plays an ontological or epistemological role (p. 51).

Here the ontological assumption refers to the real-world experience of the case site of how things are. The epistemological assumption refers to how things work, and methodological assumptions refers to how the framework is designed and evaluated for fit with the real world it aims to serve.

There are a variety of frameworks; theoretical and conceptual (Creswell & Creswell, 2018). Theoretical frameworks are developed when the unit of analysis is based on interdisciplinary concepts. A conceptual framework shows the interrelation of concepts that would result in an artefact that solves a given problem (phenomena) (Creswell & Creswell, 2018; Yin, 2016). To effectively design such an artefact, the adoption of an appropriate design methodology is imperative.

In addressing the development of the artefact (framework), this study employs an overarching methodology of Design Science Research (DSR), which, according to Hevner et al. (2004) considers the building of artefacts as “crucial”. However, they caution that artefact building needs be conducted within an iterative process of building and evaluating. This iterative process could look at aspects of utility and efficacy of the artefact. For this study, the objective was to co-design a cybersecurity best practices framework for underserved rural communities. This study borrows from a multidisciplinary body of knowledge to understand the sociotechnical phenomena at play since cybersecurity is not only a technical but also a complex social phenomenon (McAlaney & Benson, 2020). The multidisciplinary body of knowledge used to understand the phenomena of cybersecurity awareness, current security practices, perceptions of risk, and information flow processes within the affected communities, borrows from disciplines like social psychology, behavioural economics, communication theory, human computer interaction, and cybersecurity (Almansoori et al., 2023; McAlaney & Benson, 2020; Quayyum & Freberg, 2023).

Therefore, the design of this framework followed a co-design approach along the design science research methodology guided by the systematic procedure for component identification, integration, and validation.

From the Design Science Cycles the design of the framework falls within the Design Cycle

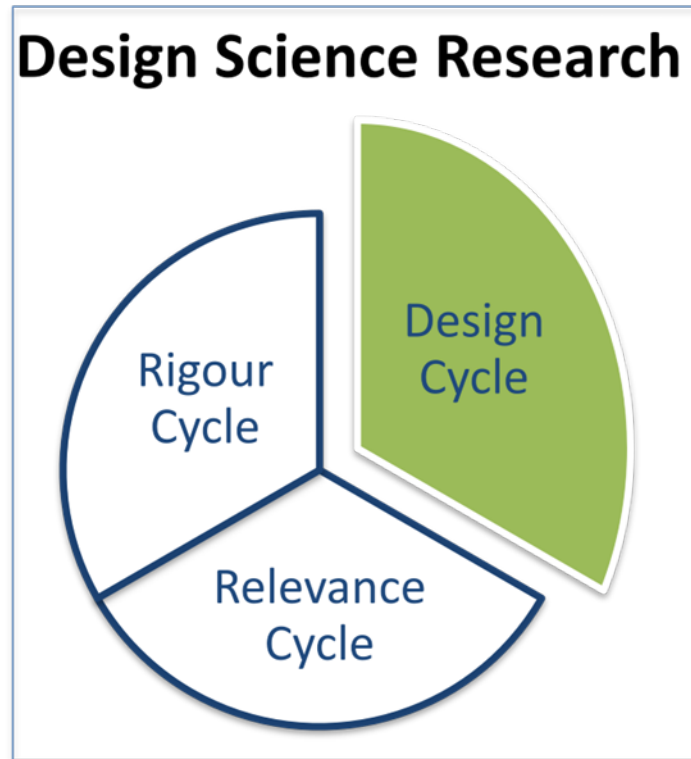


Figure 5.1: Adaptation of the Design Science Research Cycles

Jabareen (2009) proposed 8 steps that researchers can use to develop frameworks. Jabareen (2009) asserts that qualitative frameworks evolve overtime when new insights and knowledge come to the fore. Figure 5.2 provides a visual representation of the 8 steps.

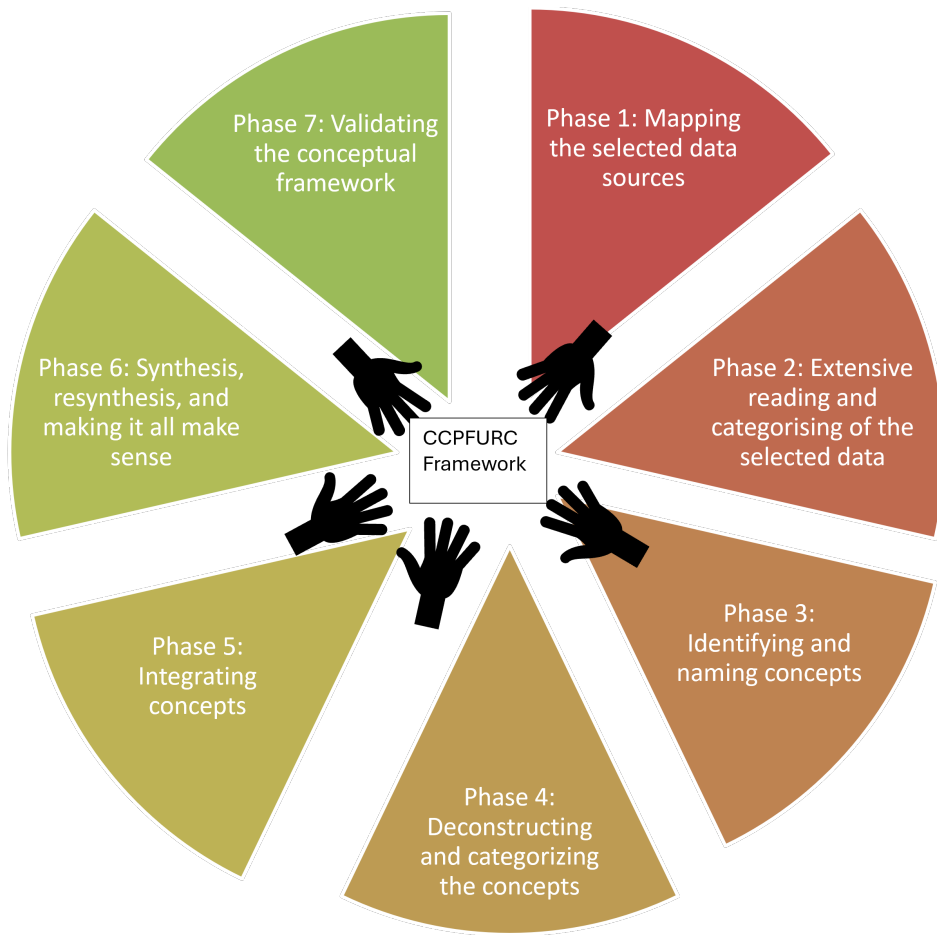


Figure 5.2: 8-Steps in building a conceptual framework.

To develop the framework this study utilised a simplified version of the 8-steps proposed by Jabareen (2009). The proposed CCSPF-4-URC framework was designed following the simplified version of Jabareen's 8-step approach for framework design steps of as illustrated in Figure 5.2. Even though the selected step seems sequential they are iterative. For the development of this framework, there was a need to utilise the steps indicated in Figure 5.3.

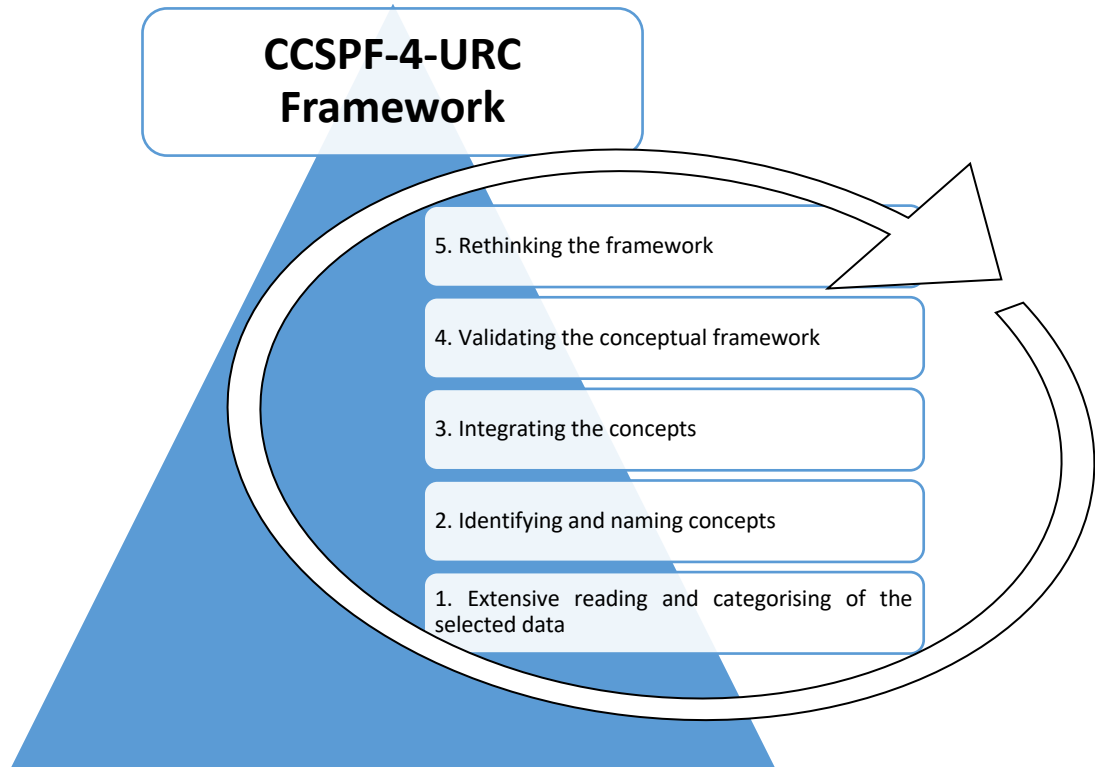


Figure 5.3: Framework design steps followed for CCSPF-4-URC

5.2.1 Step 1 – Extensive reading and categorising of selected data

Starting with extensive reading of and familiarisation with the existing body of knowledge around cybersecurity, indigenous philosophy and theories, existing cybersecurity frameworks and co-design as presented in Chapter 2. When the problem statement was fully formalised and research objectives were set and validated, the data were collected, analysed, and categorised as presented in Chapter 4.

The present study identified that there is a gap within the understanding of cybersecurity within rural and underserved communities. Even though many national states, Namibia included, have embarked on cybersecurity awareness programmes, there remains pockets of communities whose access to the Internet, experiences in cyberspace, and technology device use is not well understood. Specifically, those residing in rural areas and often underserved. Therefore, this study co-designed a cybersecurity practices framework for these underserved communities. Co-design was chosen as it has a greater potential to increase the chances of rural underserved

communities embodying secure practices when utilising technology and when accessing cyberspace.

The main objective of this study is to co-design a Cybersecurity Practices Framework for Underserved Rural Communities. The framework is intended to meet the following objectives:

- 1) To enable community members to resonate with the co-designed secure practices.
- 2) To empower community members to confidently apply the co-designed secure practices in their everyday technology use.
- 3) To reduce the potential susceptibility of community members to both online and technology-mediated attacks.
- 4) To iteratively create a living framework that evolves as the needs change.
- 5) To illuminate the relationship between the different framework components.

Co-design as a method for developing the framework that serves as an opportunity to iteratively develop the framework through the customised steps of Jabareen. This was done at each of the 4 communities that participated in this study. Overall, the framework seeks that residents of these communities can confidently apply the co-designed secure practices. Additionally, the framework seeks to reduce the potential susceptibility of community members to both online and technology mediated attacks.

5.2.2 Step 2 – Identifying and naming concepts

Four main concepts that would form the components of co-designed framework are identified from literature and from the presented data analysis presented in Chapter 4. These are further expounded in section 5.3.

- 1) People and Community
- 2) International Standards
- 3) Co-design Community Engagement Protocol
- 4) Co-designed Cybersecurity Practices

According to Jabareen (*ibid*) the concepts/components that make up the framework assume an ontological, epistemological, or methodological role. Table 5.1 places the four main components into these categories to provide clarity of their philosophical contribution to the framework.

Table 5.1: Assumed role of the main components of the proposed framework

Theme	Assumed role
People and Community	Ontological
International Standards	Epistemological
Co-design Community Engagement Protocol	Methodological
Co-designed Cybersecurity Practices	Ontological and Epistemological

The identified concepts make up the components of the CCSPF-4-URC framework. The resulting co-designed cybersecurity practices can be both ontological and epistemological in nature. The co-designed cybersecurity practices are a result of the on the existence of the practices along local trust models, existing security practices (ontology) and the engagement with the communities in the co-design process, thus bringing to light how the community knows (epistemology). Here the concepts are further elaborated upon.

5.2.2.1 Component 1: People and Community

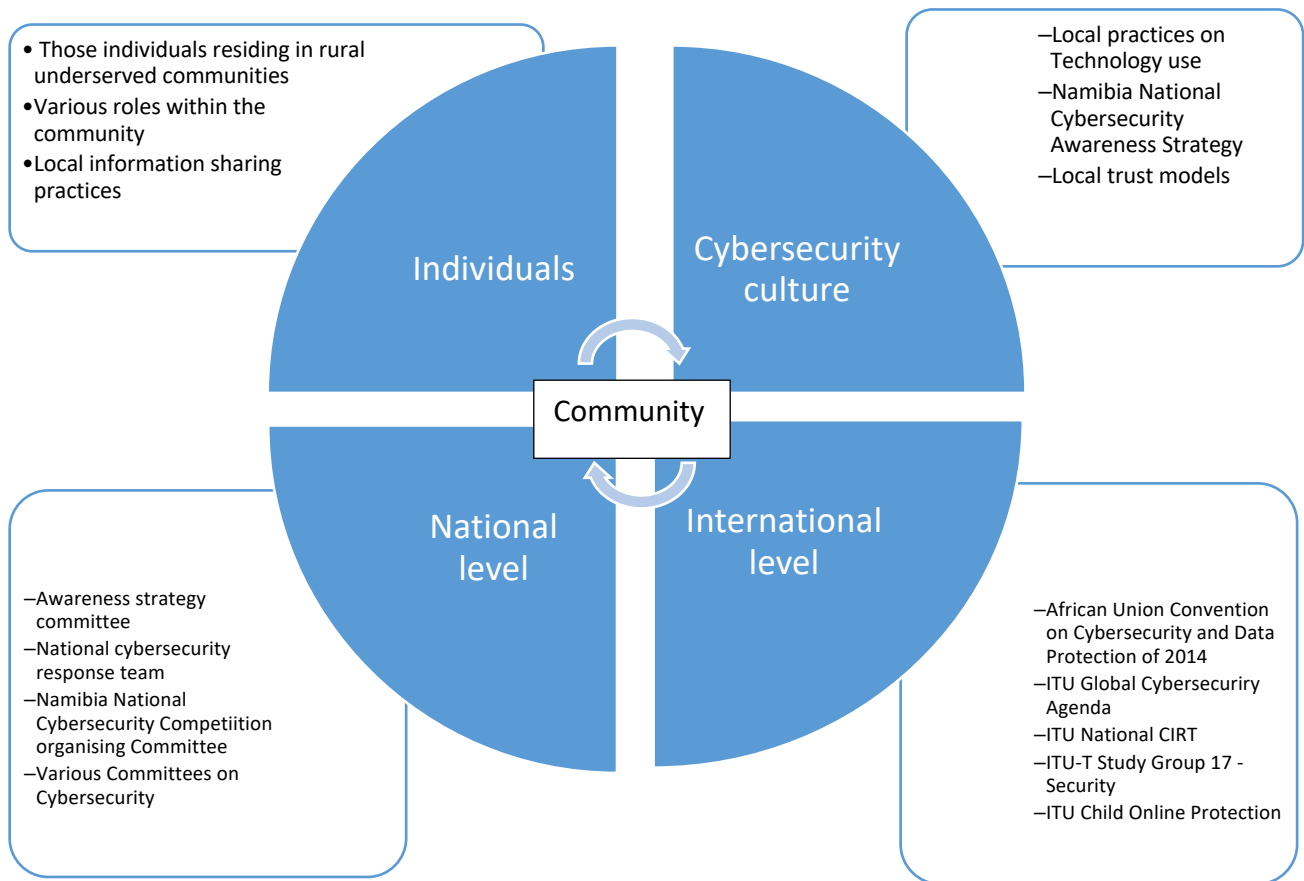


Figure 5.4: Individual and community component

- Individuals in the underserved rural community

Within Ubuntu based studies, there is an assumption that a homogeneity exists among African communities. However, within the present study, we identified that rural communities have an overarching cohesiveness, but individuals might be guided by additional sets of ethos. These individuals are usually foreigners that work for NGOs, university scholars that have had exposure to external ways of being and ascribe to both their ways with the newly learned ways. These could also be professionals that interact with peers from other parts of the world. Additionally, due to the proximity of the study site, there exists individuals from neighbouring Angola, who do not emanate from the OvaKwanyama kingdom, but from others like the Ovatjimba, Humbi, Tjimbundu, and

Mumwila tribes. Here various practices are like those of the OvaKwanyama, but differences exist, especially because of the structure of the village life. As indicated in Section 4.2, the structure of the villages tends to be comprised of compounds located in Omahangu fields. This design also means that various roles exist within the community, like those of trusted community leaders like Kapatashu, elders, youth group members, water committee members, and health committee members.

Within the community, the structure has an integrative nature and is consultative. The Kingdom of OuKwanyama is led by a Queen, who has Omalenga, the Omalenga are responsible for portions of the land area and have responsibilities for adjudicating disputes. Under the Omalenga are the Senior Village headman, these individuals are responsible for clusters of villages, and they are responsible for ediko. Ediko is responsible for attending to matters that affect each village and could not be resolved. The Junior village headmen are responsible for one village and may also temporarily lead another village in the absence of a leader (this can occur if a death occurs). The villages have Kapatashu who manage sub-sections of a village. The essential part is that the management of the kingdom has a quasi-bottom-up management style. Leadership of villages is inherited; the leadership is based on a trust by the community in the family responsible to lead fairly and equitably. Another occurrence of leadership is by appointment by the queen in the event a village does not have a headman. A community engagement protocol provides the trust-based engagement process in section 4.6.1.4. Here trust is dependent on the proxy and by association between the stranger and a known, respected member of the community. Deviation from this protocol might lead to mistrust of intentions. Due to Uushiindaism, community members are likely to trust their neighbours more because they believe they would not have ill-will for them. Additionally, the trust building process as outlined in section 4.4.1 also deals with how individuals introduce themselves, how they are introduced and who introduced them to the community.

- Community

Community plays a central role in rural communities' way of life, with shared values and norms that govern interpersonal relationships. These values prioritise respect, sociality, understanding, forgiveness, sharing, trust and reliability among village, neighbours, and people from the same homestead (Winschiers-Theophilus et al. (*ibid*)).

Community based practices, like assisting with ploughing of fields, sowing, cultivation, and group eating within homesteads continue to keep communities together (Shihomeka, 2019). Therefore, for cybersecurity practices to be shared they need to be rooted in these practices. Within the Ovakwanyama and the greater Aawambo people the use of Oxungi and through church services could assist in the evolution of co-designed cybersecurity practices and the framework emanating from this study alike. In support of what Jabareen (2009) terms the re-thinking of the framework as the last step in framework design.

- National level community

At the national level various committees exist that aim to address different aspects within the digital economy. These committees are often constituted of different players within the space of technology often constituted by Acts of Parliament, in anticipation of legislation (being that the law-making process is long), civil society committees, and international best practices. These committees range from the Cybersecurity awareness strategy development committee, to the preservation of indigenous knowledge committee through ICT, and cybersecurity incident response teams (Republic of Namibia, 2017, 2019b).

The other stakeholders identified here are the banking institutions, the various governmental ministries, and agencies responsible for citizen education on cybersecurity:

- Ministry of Higher Education,
- Ministry of Youth, Sports and Culture,
- Ministry of Basic Education,
- National Police Force,

- Telecommunications service providers, and
- Communications Regulatory Authority of Namibia.
- International Community

At the international level, efforts to guard against cybercriminals exist. These start at the regional level within economic trade communities like the Southern African Customs Union (SACU) to which Namibia is a signatory. These communities are also existent at a continental level, with the AU having a convention on data protection and cybersecurity (African Union, 2014). Past the African continent, communities such as the International Telecommunications Union committee on data protection work to assist countries with country wide maturity assessments for cybersecurity, looking at areas like the cybersecurity and data protection laws. Partner regional organisations like the European Union further assist with capacity building in the areas of cyber-law drafting, and awareness strategy building.

- Cybersecurity culture

Cybersecurity culture refers to the lived practices of a community, ranging from a microcosm like an organisation to communities in underserved rural areas. These practices often reflect the underlying values and norms that govern peoples' way of being (Nhinda & Shava, 2023b). Within rural areas these practices include the appropriation of technology to fit contextual needs, like sharing of mobile devices. Cybersecurity culture also includes national imperatives like the National cybersecurity awareness strategy which aims to ensure a cyber-secure citizenry through awareness of cyber-hygiene and practices (Staff reporter, 2023), albeit it not focusing on underserved rural communities explicitly, there is an implicit impact on these underserved rural communities due to the channels sometimes used to pass this awareness to target groups like Television, radio and social media platform to which underserved rural communities might have access to.

5.2.2.2 Component 2: International Standards

International standards regulate and tend to offer a common way to develop technologies be it software or devices. Within cybersecurity, there are a myriad of standards, that are not legal nor binding but serve as best practices for implementation (Coventry, Briggs, Jeske, et al., 2014; Dolan et al., 2010; NIST, 2023; Shen, 2014). However, none focus on underserved rural communities. Therefore, the literature in Chapter 2 brings to the fore 3 significant standards and frameworks that could be beneficial for the development of the co-designed framework as indicated in Figure 5.5.

- National Institute of Standards and Technology Cybersecurity Framework
- MINSPEACE Framework
- SCENE Framework

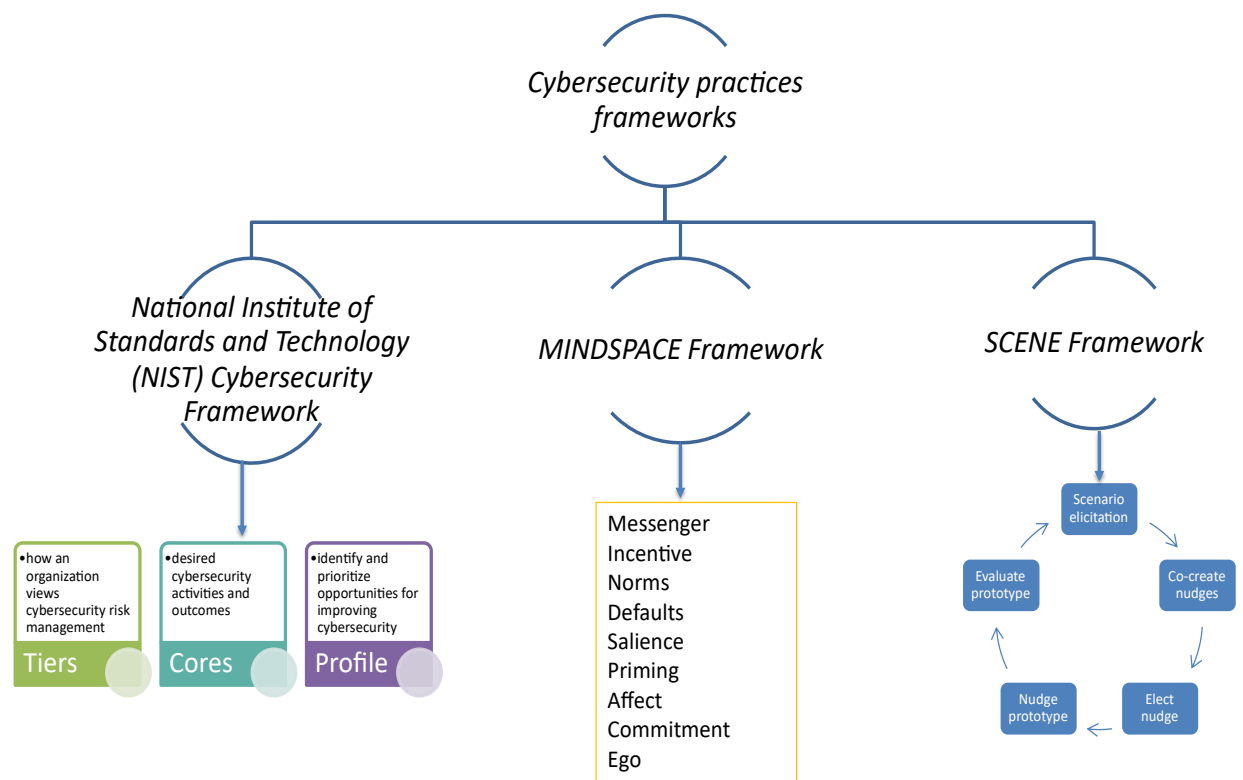


Figure 5.5: Existing frameworks in cybersecurity.

5.2.2.3 Component 3: Co-design Community Engagement Protocol

For any practices to take hold a community engagement protocol needs to be adhered to. However, for non-residents including native researchers to an extent, there is a need to elucidate this protocol collaboratively. This component provides both an information flow of how to approach the communities within the norms and values as indicated in Component 1. The communities that formed the focus of this study belong to a robust and dynamic system of governance, which is forgiving of faux pas, however as Winschiers-Theophilus et al. (2013b) there might be instances where the trust might be broken, which may present a challenge for any further community-based research activities.

Using the inform flow provided in Figure 5.6 is the most effective way to work with the OvaKwanyama people, not only for research projects but also for engagement and creation of cybersecurity practices. Co-creation as utilised in this essence also served as an opportunity to

educate the community on cyber hygiene and as well learn about technology utilisation and various opportunities present for socio-economic purposes. This rings true of the vision of National policies like the National Broadband policy of 2019 as mentioned in Chapter 2 of this thesis.

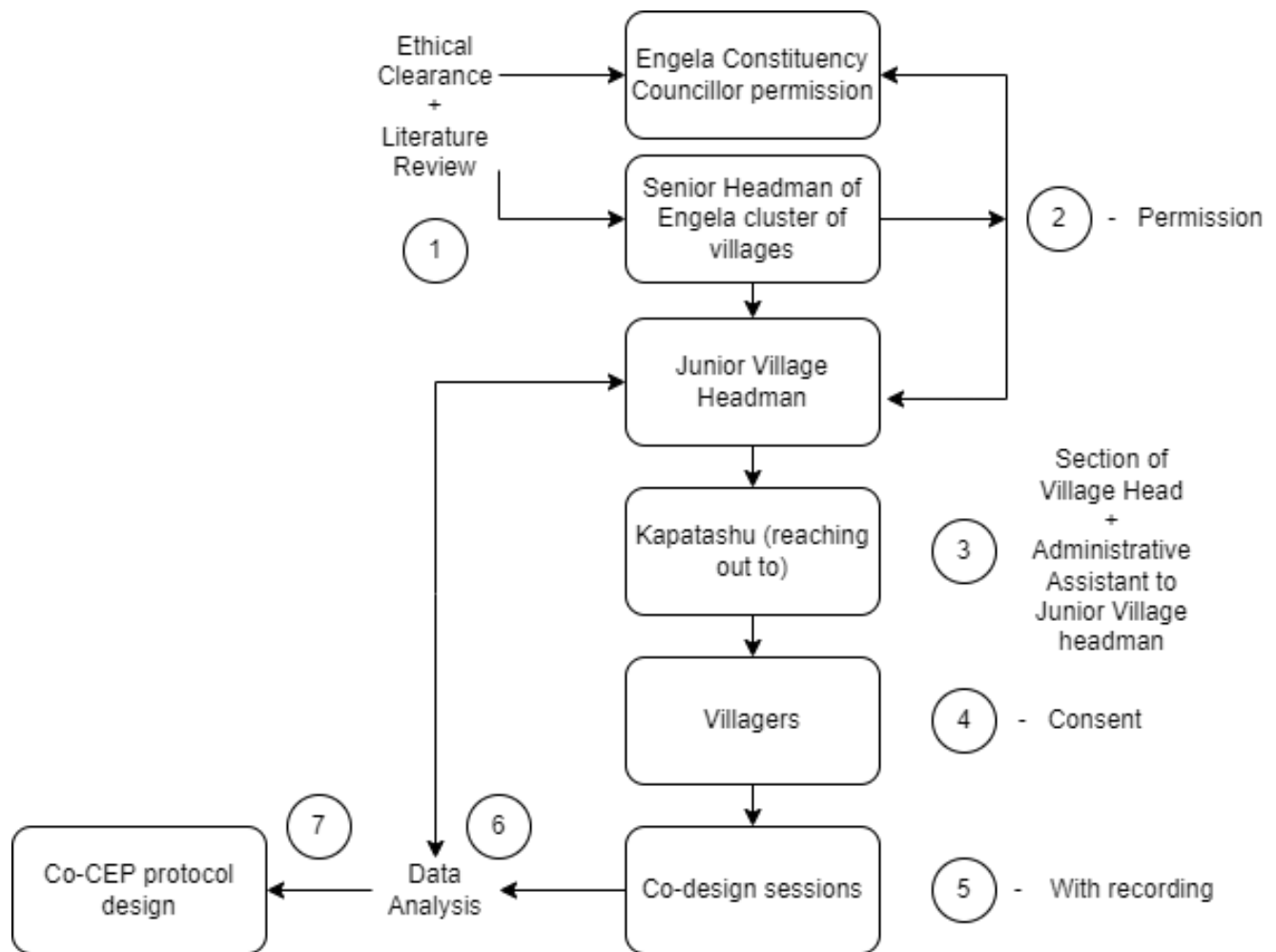


Figure 5.6: Information Flow within communities for cybersecurity research

The information flow presented in Figure 5.6 informs the co-designed community engagement protocol. This protocol was developed and validated by the communities at each community meeting. Firstly, in the Onghala Village, the design was led by the community, and they took the role of design leads. The researcher stepped aside and participated as an assistant giving prompts where needed. Only once consensus was reached by all in the meeting then a component of the community engagement protocol was added to the flip chart that we used to diagram and

represent the protocol. The community in this village self-selected to draw boxes with arrows to indicate direction. In the initial sketches, overlapping lines did not seem to matter as the community members understood the direction and would use a mixture of directions like North, South, West and East in combination with Up, Down, Left, and Right; to explain where exactly wanted a particular concept added or needed to provide clarity.

An example of a direction would be, I would like to know why the schools as listed on the paper are not coming out, the schools on the Eastern side, down.

The Ouhongo Uakondja Village took a similar approach with diagramming but added written explanations of what they meant when discussing the relationship between leadership structures within the village and how the information should flow. In the Engela village diagramming with verbal explanations was the chosen method and the Omatunda Anghala community opted for the researcher to lead the session. It is worth noting that that except for the Onghala and Ouhongo UaKondja communities, the other two only consisted of youths (school going and out of school youths). This observation was enquired upon and the response from the village headman indicated that technology related matters are often associated with the youth and not the elderly.

The use of diagrams and directions could also serve as a method of cybersecurity education through the creation and adaptation of traditional game play among other aspects to emphasise the importance of certain attributes like signing out of online accounts on shared devices (Sultan, 2020).

The information flow diagram is key to providing direction to technology developer that wish to engage rural underserved communities like those that formed part of this study. Developing inclusive technologies often does not always investigate user factors. Some reasons this researcher postulates are the lack of inroads to meeting “edge cases” in taking care of scenarios of technology use. However, this information flow only provides an overview, researchers are encouraged to study the co-designed community engagement protocol as presented in Figure 5.7.

The co-designed community engagement protocol identifies various key actors that enable or could constrain successful cybersecurity knowledge transfer and awareness. Most importantly, it also elucidates the possible power imbalances between traditional leaders and politically appointed councilors. A burning point of contention that cybersecurity researchers need to keep in mind is “who reports to who”. A misstep on this point could lead to possible rapport damage and project failure.

Engagement with these communities takes a similar approach to the information flow presented earlier. Where knowledge is passed from the senior village headman who controls a cluster of villages. This senior village headman is referred to as “ediko”. The senior village headman is then responsible for informing the junior village headman, who then inform the kapatashu, and the kapatashu to the village folk. However, this is not a strict information flow, since the senior village headman can also inform the inhabitants of villages if they meet while rendezvousing or at events (weddings, funerals, or church).

Before permission to engage a community could be granted, the team responsible for cybersecurity awareness (which includes a trusted local liaison) needs to contact both the local constituency councilor and the senior village headman. There should be sufficient details to explain the background, objectives and intended duration of the activities to be completed. Once permission is granted, various means of communication are utilised to spread the message of people in the community, radio, schools to inform children, churches, etc. Within these communities there is a sayings “te ku lombwele, keshi woye” meaning, the one who cares will warn you, and “Momtwe womutumwa iha muyi mbole” to mean, the messenger is not to blame for the message. Therefore, villagers tend to inform each other of the happenings within the village.

This co-designed community engagement protocol was published as a Journal paper (see Appendix D.1)

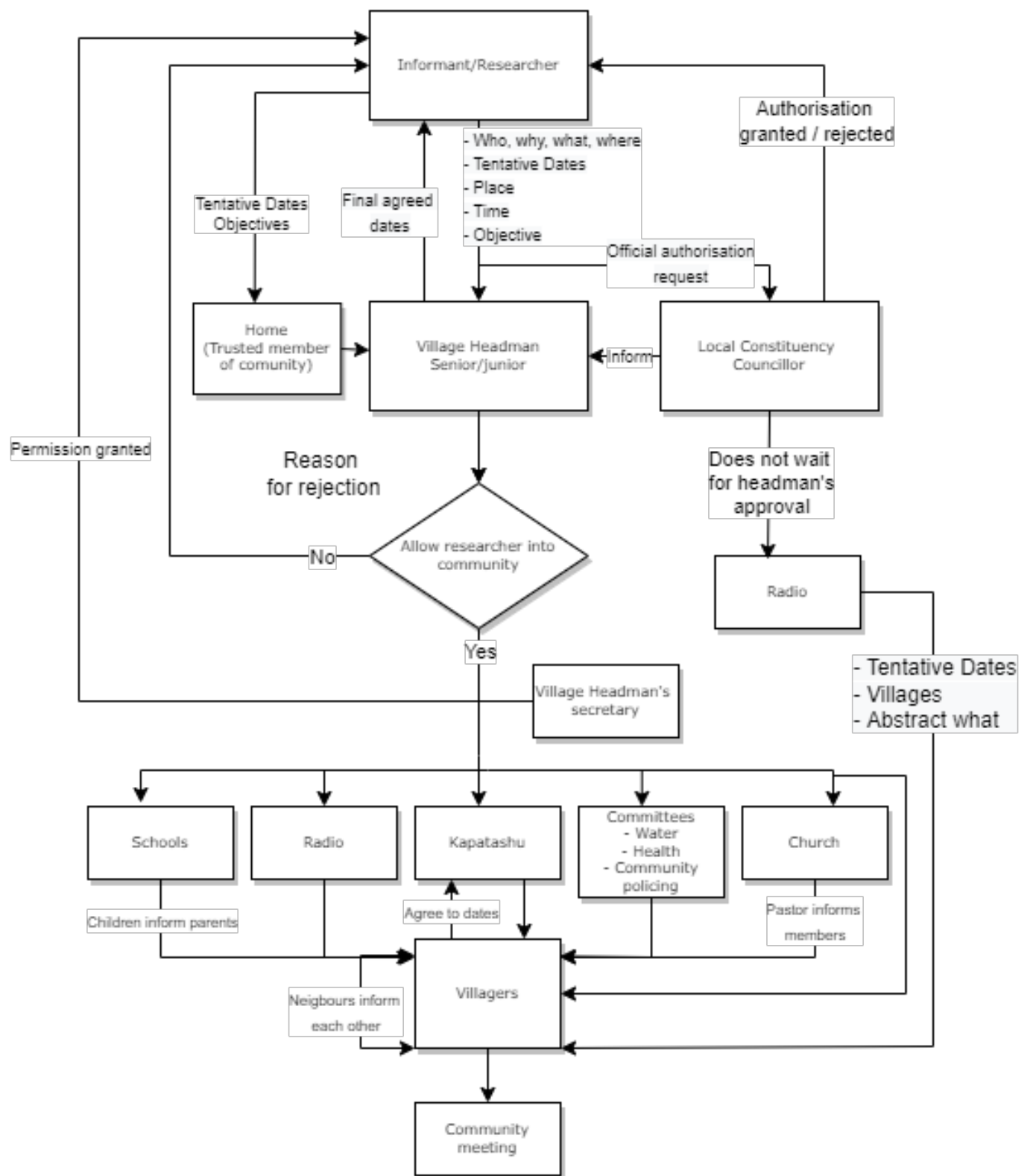


Figure 5.7: Co-designed Community Engagement protocol

5.2.2.4 Component 4: Co-designed Cybersecurity Practices

The above-identified components holistically combine to address community-specific challenges and result in better cyber hygiene. As part of the current study, a decolonial stance was taken to understand what conventional research methods would consider secure and insecure cybersecurity practices, these are provided in Table 5.2. However, as a critical grounding of this study, an Afrocentric lens is used to study these practices, cantering the African phenomenon through the values ascribed by the community and how a bridge can be made with conventional Western understandings of secure and insecure.

Table 5.2: Cybersecurity practices themes in underserved rural communities

CATEGORY	SECURITY PRACTICE	
	THEME	QUOTE
Secure practices	Use of In-device security features	"I decided to put phone lock and smartphone app locks whereby you cannot go in any app without putting in the code."
	Not sharing passwords	"My cell phone banking, for example, I want to check my balance, I am the only one who knows that password, that one I will never share with nobody"
	Logging out of online platforms	"When I am done using my insta or FB I log out because sometimes it is not my phone I am using"
	Change of potentially compromised passwords	"If I share my phone with someone, that means, once the phone is back, I'll change the password." as soon as it comes. Because I am not sure if they did not share it with someone else"
	Codes for the Creation of security passwords	"I can only come up with a password that contains something that will remind me that only I know"

	Use of different passwords	"On my banking, I have a different password than my phone, I don't know why, it's just like that"
	Obscuring sensitive information	"There was a guy that wanted some girls' numbers, I did not share them with him. So, he took my phone and took the numbers. From there, I have people's numbers with question marks and exclamation marks. Codes, just so I know who the person is."
Insecure practices	Clicking links from friends	"If I get a link that says I won, I use to click on it, but it does not go anywhere, it just says I must forward it to"
	No passwords on some devices	"I put my private information on my laptop since I am the only one who uses it. No need for a password since someone cannot just come and start using my laptop. Thank is private"
	Sharing of cell phones	"Sometimes I use my fathers' phone to access the Internet because I don't have data"
	Sharing of pin	"If I am stuck, I ask my daughter over there to assist me, she is the one who is supposed to free me. She knows my pin to the phone and bank card"
	Trusting strangers	"I got a call saying I won money from the mobile operator because I recharged a lot, they asked me to give them my bank card number, so I receive the money. My father said no, and we need to know more or go to the offices of the mobile operator, but I wanted to collect my winnings"

	Use of common words/phrases for Passwords	"I tried using sentences, but the sentences can be a little bit long, so I have words instead that I can remember." "I just put passwords and mostly book titles because I read many books."
--	---	--

From the tenets of Ubuntu and Uushiindaism as explained in Chapter 2 Section 2.2.; sharing, trust, reciprocity, hospitality, kindness, respect, compassion, and solidarity are the core tenets of the humanistic philosophies. However, as Mokobane and Botha (2020) put it, these very values that make for a utopian existence within a community may also leave said community susceptibility to cybersecurity exploits through social engineering, vishing, and phishing attacks. However, relooking at the above stated practices, four co-created practices emerge that both enable a community to be secure and safe with utilising technology and while using the Internet. It is also worth noting that these practices, especially those that are conventionally considered secure existing within the community.

- Practice 1: Trusted sharing
- Practice 2: Unique codes for security access controls (pins and passwords)
- Practice 3: Use of in-device security features
- Practice 4: Obscuring sensitive information in devices
- Practice 5: Change of potentially compromised access controls

The existing cybersecurity practices have been published in a peer-reviewed conference as Paper 2 in this thesis (see Appendix D.2).

5.2.3 Step 3 – Integrating the concepts

Step 2 identified the major concepts which formed the main components that are required for the design of the CCSPF-4-URC. In this step the relationship between these components is

clarified. These concepts were integrated into a conceptual framework, interrogating the interrelations of the various concepts.

All the above components form part of the CCSPF-4-URC which is a living framework. As communities engage with technology and educational information regarding technology, it is the expectation that the community practices, and the way they engage technology and cyberspaces change as well. These changes cannot be anticipated nor predicted. A study of that nature which is rooted in Ubuntu and Uushiindaism will need to be performed.

Component 1: People and Community

Component 2: International Standards

Component 3: Co-designed Community Engagement Protocol

Component 4: Co-designed Cybersecurity Practices

Components 1 and 2 have a direct relationship. Component 2 provides the various international standards upon which most technology that the community utilises is based upon, i.e. NIST. These frameworks provide guidance to the development of the cyber-physical devices around how to handle cybersecurity and device security. Component 1 utilises these technologies.

Components 1 and 2 do not interact in a vacuum, therefore an iterative symbiotic relationship exists with the community practices, Ubuntu, and Uushiindaism. This interaction leads to co-designed cybersecurity practices as component 4. These co-designed practices are influenced by the various tenets that govern rural life, such as sharing, trust, reciprocity, and hospitality. Component 4 is the major outcome of the relationship between all the various components that make up this framework. Component 4 also feeds back into the relationship that people and communities (Component 1) have with technology as cyber-physical systems. Similarly, there are educational efforts by government institutions and agencies, telecommunications providers, banking institutions, and other non-governmental organisations to create cybersecurity awareness. However, none of these initiatives are specifically geared toward rural underserved

communities. Therefore, any efforts that seek to engage these communities need to utilise Component 3, which is the co-designed community engagement protocol.

As a living artefact, the integration of the 4 components provides for a flexible framework that seeks active participation of rural underserved communities in providing an understanding of how appropriate technology and their way of life impacts the way they interact with technology and any materials that aim to assist them in understanding technology and cyber-physical systems.

5.2.4 Step 4 – Validating the conceptual framework

The validation of the framework was done in two steps. Firstly, as part of the co-design process, each village (community) validated the initial design of the framework. The co-design process has a feedback loop that is built into it, which allows for in-situ validation of design artefacts.

Secondly, the validation was done through an expert focus group. This group looked at aspects of completeness, and ecological utility. The expert group comprised experts from the community who were knowledgeable about their lived experience, cybersecurity, and indigenous knowledge. Details about the validation of the framework and additional reflections are presented in Chapter 6.

5.2.5 Step 5 - Rethinking the Framework

This step is done after the evaluation of the framework. The framework was evaluated in the field through the co-design sessions and by expert focus group. The feedback received at each interval, allowed for the iterative evolution of the framework as it seeks to meet the objectives identified in section 5.2.1. This step saw the culmination of all the validation and evaluations resulting in the final CCSPF-4-URC as presented in Chapter 6, section 6.8.

5.3 PROPOSED FRAMEWORK

The proposed framework comprises four main components that lead to the co-designed cybersecurity practices. The people and the community are the most important aspects of the

framework, whose lived experiences and way of thinking about the world and life, interactions with technology, and the Internet have and are influenced by international standards. The international standards and frameworks on cybersecurity practices are used as best practices for the development of technology (both software applications, artificially intelligent systems, and physical devices). These are utilised and regulated by the people and community and other technical committees at the national and international levels.

The usage of the technology exists through the lenses of Ubuntu and Uushiindaism by the people in the rural and underserved communities. However, for any cybersecurity awareness to reach the communities it needs to be through the co-design community engagement protocol. These engagements, interactions between the varying components of the framework, result in the co-designed cybersecurity practices.

Technology pervasiveness inadvertently leads to some experiences not being positive, while others border on criminals. Therefore, the national legislation would then be the grounds upon which cybercrimes can be reported, investigated and adjudicated. Similarly, the amendment of these laws and policies that make provision, not only in criminal justice but also in civil matters, is provided for. The iterative and ever evolving threat landscape also means that the co-design cybersecurity practices evolve over time.

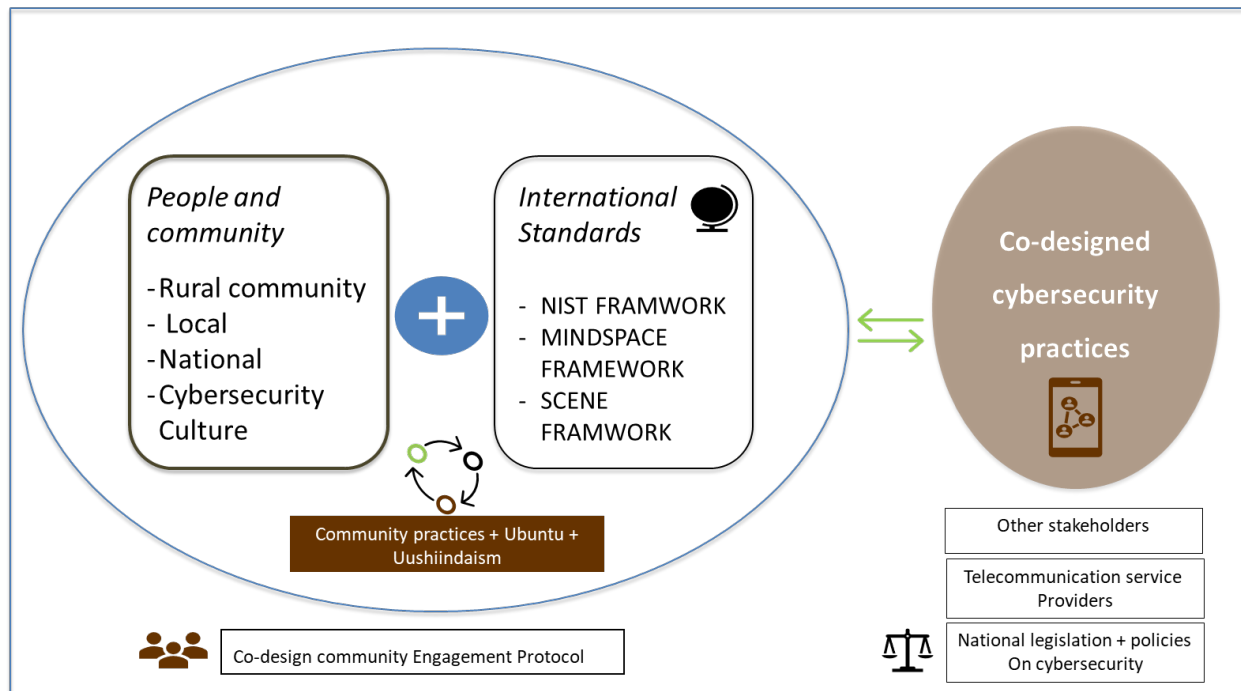


Figure 5.8: Co-designed Cybersecurity Practices Framework for underserved rural communities- CCSPF-4-URC

5.4 CHAPTER SUMMARY

In this Chapter, the co-designed cybersecurity practices framework for underserved rural communities is presented. The Chapter started by defining a conceptual framework and its grounding in the various uses of the concepts; namely ontological, epistemological, and methodological. The proposed framework was designed using a simplified 5-step process inspired by Jabareen's 8-step process for conceptual framework design. The objectives of the framework were: to enable community members to resonate with the co-designed secure practices; to empower community members to confidently apply the co-designed secure practices in their everyday technology use; to reduce the potential susceptibility of community members to both online and technology-mediated attacks; to iteratively create a living framework that evolves as the needs change; and to illuminate the relationship between the different framework components.

The proposed framework comprised 4 abstract components: the people and community; the international standards; the co-designed community engagement protocol; and the co-designed cybersecurity practices. These components are explained and linked to other chapters in the

thesis. The Chapter ends with a visual presentation of the proposed framework and an explanation of the interrelationship among the various concepts mentioned above.

The next Chapter presents the evaluation of the proposed co-designed cybersecurity practices framework for underserved rural communities.

CHAPTER 6: EVALUATION OF THE CCSPF-4-URC

6.1 INTRODUCTION

The previous Chapter presented the proposed co-design cybersecurity practices framework according to the simplified 5-step framework development process used in this study. In this Chapter, the evaluation of the proposed framework is presented as per step 4 of the 5-step framework development process. The Chapter also presents the evaluation results, the refined framework, and the Chapter summary.

6.2 CCSPF-4-URC FRAMEWORK EVALUATION

In design science research (DSR), evaluation alongside the build of artifact is central to ensuring rigour (March & Smith, 1995). Kuechler and Vaishnavi (2011) state that evaluation of artefacts cements the outcomes and findings of a study, moving it past “preliminary findings” status. Evaluation in DSR may occur ex-ante (before the construction of the artefact) and ex-post (after the construction of the artefact). The choice of time to evaluate the outcomes of DSR remains a debate within Information Systems (IS) research. With scholars like Pries-Heje et al. (2008) arguing that most DSR researchers still choose their evaluations as though they are performing empirical studies (ex-post). However, design research is iterative (see Chapter 2 and 3), necessitating evaluations to be conducted as the design of the outcomes is ongoing. Hevner et al. (2004, p. 78) postulate that “the evaluation of the artefact provides feedback information and a better understanding of the problem to improve both the quality of the product and the design process.” Therefore, it is imperative for the DSR researcher to intentionally evolve the design process and the design artefact as key parts of the research. Hence, a combination of ex-ante and ex-post evaluations improves the rigour of the outcome of DSR.

Hevner et al. (2004) urge DSR researchers to choose evaluations “guidelines” or strategies to aid in showing the efficacy, utility, and quality of the designed artefacts through rigorous evaluation methods and strategies. The choice of evaluation strategies depends on factors such as the evaluation objectives, contextual constraints like time, resources available, the characteristics of

the design artefact, research subject availability, and the level of abstraction of the artefact (Venable et al., 2012).

Evaluation of artefacts depends on the type of artefact that has been designed. However, all evaluations within DSR attempt to answer two fundamental questions 1) "Does the artefact work?" and 2) "How useful is the artefact in addressing the problem?".

The benefits of evaluation are three-fold (Hevner et al., 2004; Vaishnavi & Kuechler, 2007);

1. Evaluation indicates the feasibility of the artefact and how it improves on existing practice.
2. Evaluation allows the researcher to determine if they understood the problem, the quality of the design process utilised to design the artefact, and identify missing components to refine the artefact.
3. Evaluation allows further research as part of theory building using social science methods.

The above is paradigm-specific, within positivist and pragmatic studies, evaluations tend to be statistic-laden and conducted through questionnaires. However, for the current study, which is qualitative and interpretivist in paradigm we utilise an expert focus group and in field evaluation of the artefact. In this study, we follow the seven (7) guidelines of Hevner et al. (2004) who note that an artefact must meet its utility and efficacy. These guidelines are elucidated in Table 6.1.

Table 6.1: Design Science Research Guidelines

#	Guidelines	Description
1	Design as an artefact	Design-science research must produce a viable artifact in the form of a construct, a model, a method, or an instantiation. For this study, a co-designed framework is the artefact.
2	Problem relevance	The objective of design-science research is to develop technology-based solutions to important and relevant business problems.

		The framework presents relevance to the objective of the study and the reality of the communities that are the main beneficiaries of the framework.
3	Design evaluation	The utility, quality, and efficacy of a design artifact must be rigorously demonstrated via well-executed evaluation methods. Section 6.3 details the evaluation approach, tool, and procedures used to evaluate the framework.
4	Research contributions	Effective design-science research must provide clear and verifiable contributions in the areas of the design artifact, design foundations, and/or design methodologies. Contribution to the body of knowledge in the space of co-design with underserved rural communities. Additionally, an understanding of the current cybersecurity practices of these communities and overall, the framework presented makes the greatest contribution to safeguard the communities in focus as they interact with cyberspace from the various cyberattacks that exist and allow them to evolve over time within their ethos.
5	Research rigour	Design-science research relies upon the application of rigorous methods in both the construction and evaluation of the design artifact. Co-design as a research method has been applied in various areas, including community-based research. The processes followed in this study have been tested over time. However, the contribution and extension to methodology regarding

		research ethics, and methodological relevance is presented in Chapter 3 Section 3.3 and Chapter 4 Section 4.3.
6	Design as a search process	The search for an effective artifact requires utilising available means to reach desired ends while satisfying laws in the problem environment. Within this study, the local customs and protocols have been observed as presented in Chapter 3 Section 3.5.2.
7	Communication of research	Design-science research must be presented effectively both to technology-oriented as well as management-oriented audiences. As part of this study, peer-reviewed publications in journals and conferences are made.

Hevner et al. (2004) argue that the guidelines they propose need to be met for the designed artefact to solve a unique problem or a known problem innovatively. The choice of evaluation methodologies and strategies emanates from the knowledge base within the design science research methodology. In its early days, DSR evaluation methods were limited to analytical experiments, case studies, simulations, and field studies (Hevner et al., 2004). However, with the emergence of participatory methods, like co-design qualitative methods like focus group

discussions can be used. The evaluation also falls within the rigour and relevance circle of the chosen DSR model as indicated in Section 3.5.3, and in Figure 6.1.

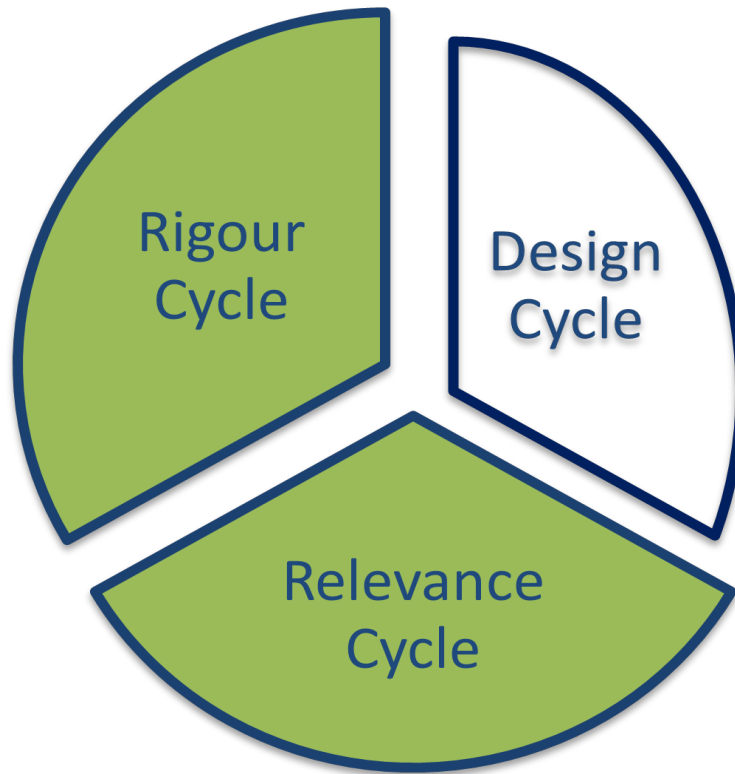


Figure 6.1: Framework evaluation falls within the rigour and relevance cycles of DSR

Within the present study, the evaluation was done both ex-ante and ex-post to feed creating an iterative evaluation process. The ex-ante evaluation also included a validation aspect through co-design sessions, where the communities that formed the case study of this study, identified, and validated various components they wished to be part of the framework as presented in Section 6.3 of this Chapter. The validation was completed following the process as highlighted in Chapter 4 Section 4.5. The ex-post evaluation was done through expert focus group discussions.

Quality of the Framework

In qualitative research, validity is a key that needs to be considered by researchers. In this study, careful attention to the design of the framework was taken to ensure that the artefact which is the design of the DSR process has internal and external validity, and that the artefact is reliable

and objective. Internal validity here refers to the causal relationship between concepts and that their relation is triangulated.

External validity refers to the generalisability of findings with a single case study as applied to other contexts, with greater external validity being reached as the findings are replicated across more contexts. Reliability refers to the accuracy of the documented procedure to guide others to replicate the study and arrive at the same conclusion. According to Hevner et al. (2004) social phenomena are not static and evolve with the interaction of external influences i.e. the researcher explaining the purpose of the study and its objectives. Therefore, a clear research process with a recorded data collection method would allow others to study and come to similar conclusions. However, newer data collections from the same contexts will yield different results, while objectivity refers to the absence of researcher bias (Oates, 2012; Yin, 2016). In our case, objectivity cannot be demonstrated as the researcher through the co-design process as proposed in Chapter 2 becomes part of the research and data collection, essentially marrying what Yin (2016) terms an object within the research process. To ensure that bias is reduced, this study presents detailed descriptions of analysis. In Chapter 4 Section 4.3 the data collection process was elucidated for this purpose and in Chapters 1 and 3 wherein the research background is presented, the limitations are indicated, objectives are stated, and Chapter 3 makes clear the methodology used in this study in section 3.5.

According to Yin (2016) for qualitative studies rooted in interpretivist paradigm trustworthiness and not validity is considered as it related to the methods to design and evaluate the framework and its components. Therefore, for qualitative studies issues of generalisability are only valid when the contexts are similar as such to aid this process, documentation of the tools used for design and evaluation of this frameworks addresses this challenge.

Given the complexity of political, social, economic, and diversity of cybersecurity within rural underserved communities, this results in a social phenomenon that is not comparable to other settings. Therefore, the alignment of the research process allows issues of credibility to be addressed.

The evaluation of the framework was conducted to identify the following

- Ecological utility
- Completeness
- Effectiveness

The protocol used for ex-ante evaluations is shared in Appendix F. The approach for ex-post evaluation is given in section 6.3.2 and Figure 6.2.

6.3 EVALUATION RESULTS

6.3.1 Ex-ante Framework component evaluation and validation through co-design sessions

As part of the co-design process, validation occurs during the feedback steps. Identification and validation of Components 1, 3, and 4 were done in the 4 communities where this study was undertaken during the co-design sessions.

Component 1: People and community emanate from the co-design sessions and all 4 communities identified these as key for creating secure practices. They also co-designed Component 3: community engagement protocol, which was also validated through literature and studies like those of Kapuire (2023). In addition, they identified the role of the government and its various agencies in creating a secure digital environment through laws and regulations. Component 4 was also evaluated through the co-design process where the community members indicated the identified co-design practices resonate with their existing practices of sharing. They, however, acknowledged that sharing in this day and age needs to be done with trusted persons.

The second component is derived from literature, which argues that there is a need to provide a link to existing frameworks and standards on cybersecurity. These international standards do not only feed into the community; however, the iterative nature of the framework also means that the community's practices can influence international standards to incorporate Afrocentric tenets as espoused in the underlying theories of Ubuntu and Uushiindaism that guide interaction within the community. Therefore, the community did not have opinions on this component.

6.3.2 Ex-post framework evaluation through expert focus group discussions

The evaluation of the framework was done in a 2-pronged approach through a focus group (see section 3.5.2). This approach is presented in Figure 6.2. First, the focus group participants were identified and selected, initially, they were supposed to be 8 however, only 5 were available to participate. The criteria were that they needed to represent the various knowledge areas that make up the theoretical framework for this study as identified in Chapter 2. Secondly, a synopsis of the focus group, including the research background, research objectives, and evaluation objectives was shared with the participants to serve as a primer for the focus group discussion. Thirdly, although the participants received the synopsis, the researcher presented the framework and its various components to the participants. This session was recorded with the permission of the participants. Lastly, the participants were guided by the researcher in the discussion of the framework, using a discussion guide with nudges to encourage dialogue and critical engagement.

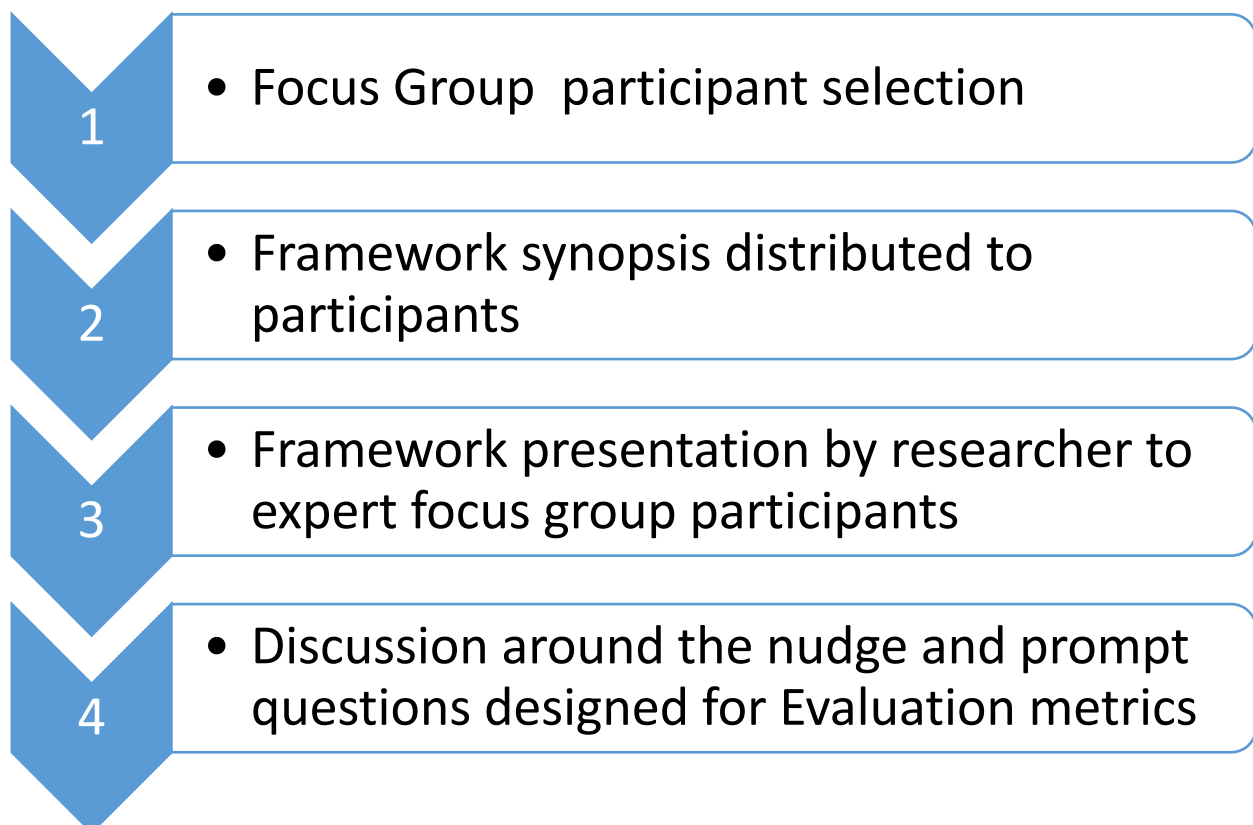


Figure 6.2: Framework evaluation approach

The focus group discussion was composed of various experts from cybersecurity, indigenous Knowledge Management, and human-computer interaction, and community members from the Engela constituency. The cybersecurity expert serves to ensure that the cybersecurity practices are sound and grounded within the domain. The indigenous knowledge expert is responsible for ensuring that the research methods and representation of the indigenous communities are centered, and that the language use is in line with decolonial practice as postulated by Afrocentricity. Additionally, this human-computer interaction and behavioural sciences expert serves to ensure that relevant theories that are appropriate for rural underserved communities are part the study. Additionally, this expert also looks at the framework from the perspective of how it may influence the behaviour of the communities to ensure that the communities resonate with the co-designed cybersecurity practices. The community member represented the communities from the Engela constituency to ensure that their voice resonated throughout the final framework. This community member was selected because she was actively involved in assisting the senior headman in arranging community meetings, the member is also involved in the administration of community affairs like the drought relief programme. Additionally, the community member has taken a keen interest in technology related matters and showed concern regarding cultural preservation and the erosion of cultural practices mediated by technology. The member also noted that there are benefits to technology and recognised the need for protecting other members of the community from cybercriminal. Table 6.2 gives the profiles of the focus group evaluands.

Table 6.2: Focus group framework evaluation demographics

Participant	Field of expertise	Qualification	Gender	Code
1	Community member	Grade 10	Female	FG1

2	Indigenous Knowledge Management and Afrocentricity	PhD	Male	FG2
3	Human Computer Interaction and Behavioural Sciences	MSc	Female	FG3
4	Cybersecurity	MSc, Ethical hacker	Male	FG4
5	Human Computer Interaction and Networking	MSc	Female	FG5

Before the focus groups, the identification process of experts to serve on this evaluation played a major role. Due to the interdisciplinary nature of this study, it was imperative that representatives from each of the main knowledge areas of this study critiqued and provided feedback on the proposed framework. Additionally, from the community, the identification of a representative meant someone who was actively participating and contributing during the fieldwork and someone outspoken and passionate about the problem at hand.

6.3.2.1 Ecological utility of the framework

Ecological utility deals with the ability of the framework to solve a particular problem for a given community of users. In this study, the evaluation of the framework by experts including the community members allows this utility to be demonstrated. Some of the participants like FG1 remained relatively silent during the evaluation discussions. However, FG1 indicated that the

framework seemed complete, however, culture was rather confusing as how can one have two cultures, theirs, and a cybersecurity culture? Relating it to, how do the Queen and the Headman understand this? FG1 Further added that she knows that the senior village headman knows more about the cybersecurity culture because of his background because of his job, only returning to take the helm of the headman when his father passed away.

FG1 indicated that *"The Ubuntu values are not coming out clearly in the current framework as it is designed, maybe some presentation of that could help, I am not a graphic designer so I cannot make suggestions but the values being represented would add value to the framework and make it complete."*

"From the topic of the study, how does the framework bring out the concept of underserved rural communities" - FG4

Framework Improvement

The framework makes use of symbols to clearly indicate the influence of culture within the framework.

As a key takeaway from the evaluation results, there is a need to clarify the relationship between the cybersecurity culture and the existing culture within the community. This key takeaway is important to note as the Ubuntu values are not prominently highlighted within the framework. Another takeaway is the representation of these cultures within the framework. The representation of Ubuntu values was not indicated clearly within the framework.

The above takeaways and framework improvements are implemented within the framework as indicated in section 6.4.

6.3.2.2 Completeness of the framework

Completeness in this sense can be measured in the overall coverage of the key components of the framework in addressing the problem at hand. Another metric is the alignment of the framework to the objectives of the framework as indicated in section 5.2.1. Another metric is the flexibility and adaptability of the framework to change. Lastly, the consideration of stakeholders needs to be provided for as a key metric.

For instance, the relationship between the communities and the national environment and national strategies on cybersecurity. This relationship at present is uni-directional, however, within the framework, it is multi-directional as it allows for an iterative process where communication between the various stakeholders can be initiated at any given time.

The often-uncertain definition of what is meant by rural underserved communities was discussed and the need to properly indicate the definition used within the study to provide context to the reader. The experts felt that many times the phrase rural underserved communities is mentioned but never explained leaving it to the readers to interpret their meaning.

“According to the framework, how is underserved community defined? It is not coming out clearly. During the development of the national digital transformation strategy, the word underserved came up, in relation to how the strategy might be rolled out to the various underserved communities in the country. The workshop attendees also indicated that underserved might look different in different communities. So, I was just interested in how you defined underserved communities in this study. The workshop did not provide a definition but rather an example of how the infrastructure is present in the communities, however, for the digital transformation to occur. So, the lack of resources to complete the digitalisation process, network towers might exist but there is no on-gride electricity available” – FG4

“That keyword underserved caught my eye, does this mean all the underserved rural communities, or just those that you work with?” – FG2

“The link between the problem statement, the communities, and the solution is not clear to me. Maybe it needs to come out clearly” - FG2

“I really like the co-designed cybersecurity practices as you represented them. This is significant for understanding how communities operate.” – FG5

Given the nature of the study being grounded in Afrocentric philosophy, terms like Ubuntu and Uushiindaism, were discussed, and a clarification was sought indicating how those chosen research methods are represented in the framework as it relates to the problem statement.

“You indicated that there are Western frameworks that were used, why? When people who come from community research hear ‘Western’ they assume something bad. So, what aspect did you get from the frameworks you indicated?” – FG2

“Which tenets from the Afrocentric methods you used are used in the framework? They are not coming out strongly. Indicating them will help with assisting the readability of the framework.” – FG2

The relationship between the various components was also discussed to explain how they relate to the framework and in assisting the framework to meet its objectives.

“It was a very insightful presentation, and I would’ve appreciated the clarification on the lower half of the framework, the relationship between community practices, Ubuntu, and Uushiindaism.” – FG4

“The People aspect is not clear, as to which people you are referring to, you are from the community, so when you are in the field, you are a native researcher. I am struggling to understand who. You also mentioned that they are not the same, but Ubuntu does not individualise people.” – FG4

The co-designed community engagement protocol was interrogated for its design and flow, adding that it looked more like an information flow than an artefact that was co-designed.

“The Co-designed protocol looks like a process because when you present the co-design, I am looking forward to seeing what was co-designed and not the flow you used to meeting the various stakeholders to get to the community” – FG3

Framework Improvement

The framework uses symbols to clearly indicate the influence of underserved and clarification is done by creating a clearer interaction for Components 1 and 3.

The national environment needs to be clearly indicated. The components from other frameworks are added to the framework. The tenets of Ubuntu like trust, hospitality, sharing, trust, reciprocity, hospitality, and kindness are represented in the framework.

The framework explanation was provided to indicate the clarity required. There are two instantiations that need to be clarified. The information flow and the co-designed community engagement protocol.

6.3.2.3 Effectiveness of the framework

FG1 indicated that she understands how the framework works especially pointing out that the youth especially those below the age of 18, already understand the risks and benefits of technology as compared to the older generation. Therefore, the framework will be much easier for the youth to understand. FG1 further added that the framework that was presented is what was designed in the village (Engela Village). Thus, showing the representation of the community in the co-design.

“The framework has relevance for other communities in Africa as well. Let me refer to the communities that I work with, I can take this framework and inform them that my colleague has done research with other rural communities and found that there are issues that need to be

addressed regarding community members' internet use. Therefore, the need value is there.” – FG2

“I think the framework is well structured and I really learned a lot from this presentation” – FG4

“I do not really have any comments on the framework because this is the one that we designed.” – FG1

Framework Improvement

There are no improvements that need to be made in this metric, the expert focus group indicate that they see the value for other communities, even though there is no generalisability in qualitative research.

Some key takeaways are that the evaluation of the framework indicates that it is effective in addressing the problem of the study. The objectives of the framework are intended for the community members to be able to acquire cybersecurity practices while also adapting according to their existing cultural practices, underpinned by Afrocentric theories of Ubuntu and Uushiindaism. The evaluation results show that the co-design process enabled ownership of the final framework, as indicated by FG1, who stated that during the co-design sessions, she learned how to secure herself when using digital technology. This also means that there is a need to create a living framework that is constantly fed through cybersecurity awareness training. The trust factor is key to cybersecurity and the effective functioning of the local community according to their own customs and engagement protocols.

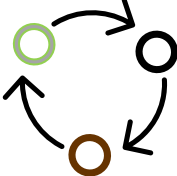
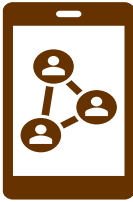
6.4 REFINED CCSPF-4-URC FRAMEWORK

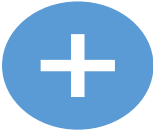
The critical feedback provided by the group of experts as provided in section 1.7 yielded some improvements which led to what Jabareen refers to as rethinking the conceptual framework and a refinement of the framework. Figure 6.3 presents the refined framework. There are some

comments by the evaluators like that of FG4 who indicated that the concept of underserved did not come out clearly on the framework. This has been addressed in Chapter 2 section 2.3.3.

The refined framework provides two additional components and the clarification of the relationship between the various components. Table 6.3 provides an explanation of the framework components.

Table 6.3: Explanation of framework symbols

	This icon represents the community engaging with external individuals/researchers
	This icon represents the community
	This icon represents the iterative interaction of the community, with technology designed using international standards. All this happens within the community and through their various Ubuntu and Uushiindaism tenets.
	This represents the international standards.
	This represents the community's appropriation of technology which results in their technology and cyber use according to their co-designed cybersecurity practices.

	This icon represents the cybersecurity awareness training that is influenced by other stakeholders (manufacturers of devices) and the community's use of technology and cyberspace.
	This icon represents an intertwined relationship where the community utilises technology.

The CCSPF-4-URC framework was designed and evaluated to meet the following objectives as presented in section 5.2.1:

- 1) To enable community members to resonate with the co-designed secure practices.
- 2) To empower community members to confidently apply the co-designed secure practices in their everyday technology use.
- 3) To reduce the potential susceptibility of community members to both online and technology-mediated attacks.
- 4) To iteratively create a living framework that evolves as the needs change.
- 5) To illuminate the relationship between the different framework components.

The evaluation results as presented in section 6.3 indicated that all the objectives have been met.

The next section presents the limitations of the CCSPF-4-URC framework.

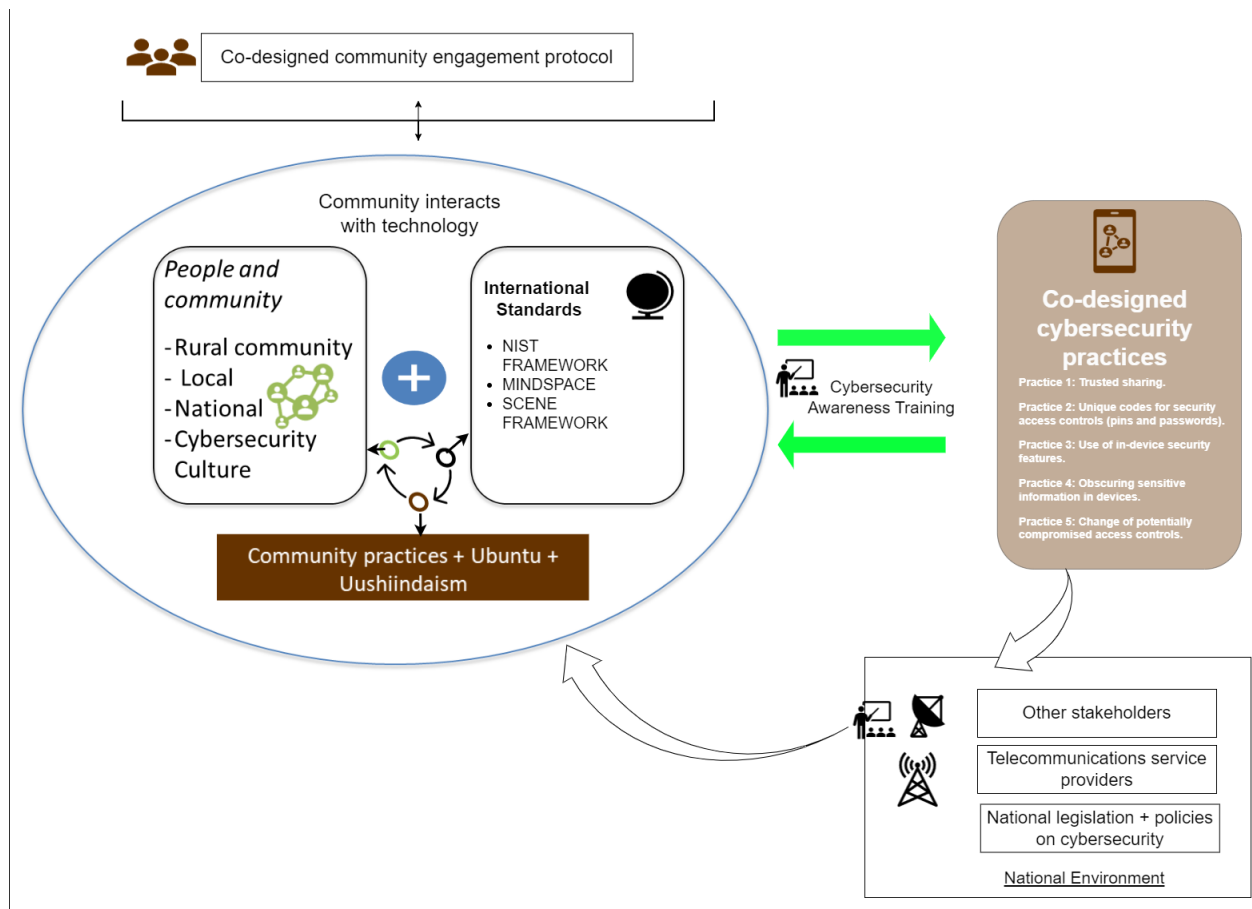
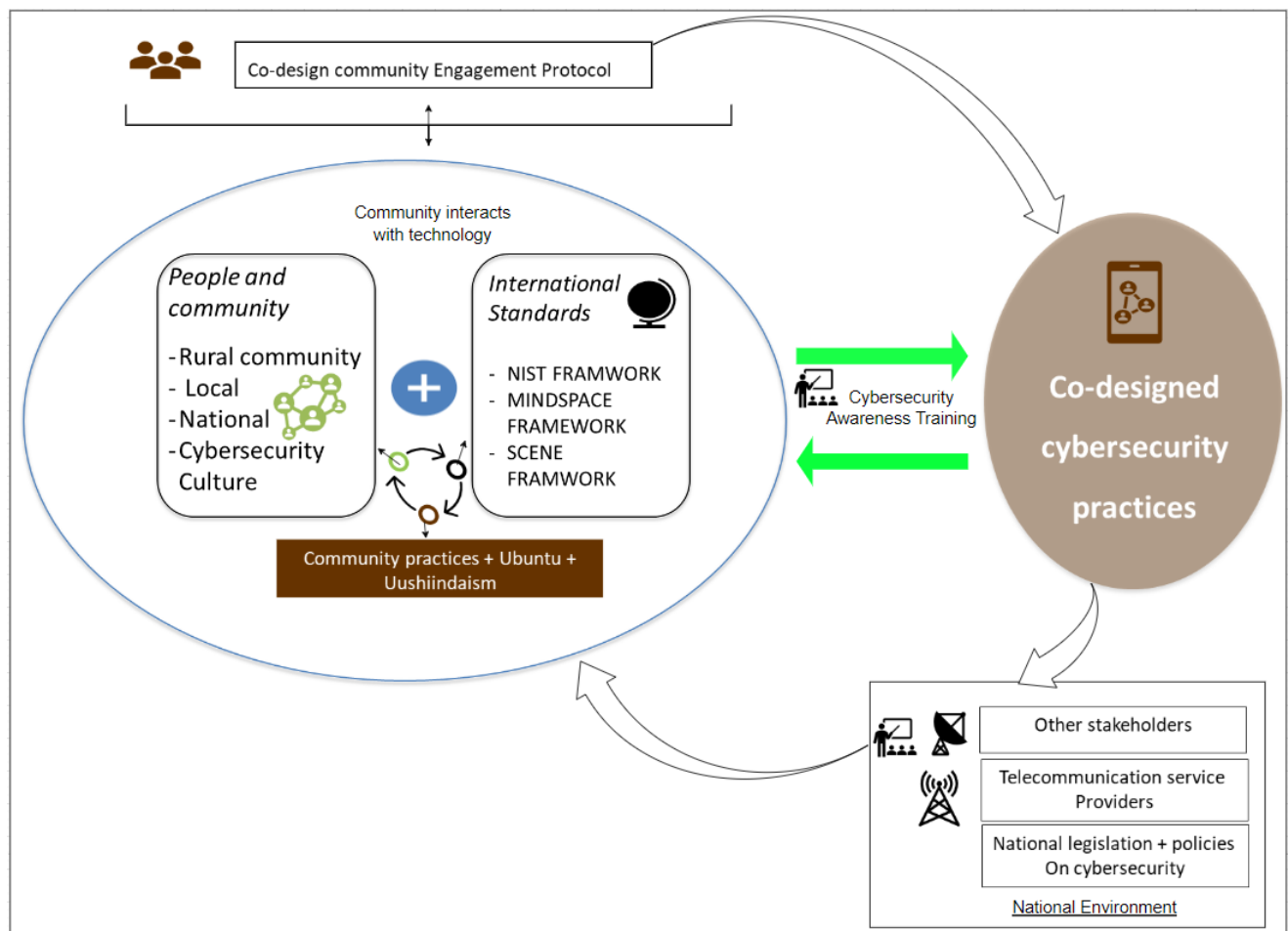


Figure 6.3: CCSPF-4-URC Framework



6.5 FRAMEWORK LIMITATIONS

The co-designed framework encompasses five components: people and community; international standards; co-designed community practices; and the national environment, which exhibits several limitations that warrant consideration. The conceptualisation of key concepts like cybersecurity, cybersecurity culture, and digital security may be abstract and ambiguous to communities and may need further clarification to enhance comprehension. The framework's adaptability and scalability to different cultural contexts are untested, which may not be applicable beyond the setting of this study. The reliance on international standards poses possible challenges in localisation, cultural fit, and the language barrier, for which no words currently exist. Additionally, although the interaction between the community and their own cybersecurity culture is influenced by international standards and cybersecurity awareness

training, the feedback to influence these standards will be challenging. These limitations underscore the need for the framework's effectiveness in addressing the problem at hand.

6.6 CHAPTER SUMMARY

This Chapter presented the tool that was used to evaluate the co-designed framework (CCSPF-4-URC). The evaluation results from the focus group of experts from diverse backgrounds provided insightful suggestions that led to the refinement of the framework in section 1.8. Through focus group of experts' discussions, 2 additional components of National environment and cybersecurity awareness training were added to the framework. Additionally, as part of rethinking the framework further relationships were provided in the refined framework.

CHAPTER 7: RESEARCH CONCLUSION

7.1 INTRODUCTION

This is the final Chapter which reflects the identified problem, key findings, objectives, and the knowledge attained and disseminated. The various key findings are illustrated as part of the research overview. The main objective of this study was to co-design a cybersecurity practices framework with rural underserved communities through a case study of 4 villages within the Engela constituency located in the Oukwanyama Kingdom along an Afrocentric epistemology. This Chapter forms part of the last step of the DSR method used in this study, as a reflection which is presented in section 7.5.

7.2 RESEARCH OVERVIEW

This study aimed to “co-design a cybersecurity practices framework for rural underserved communities”. This section presents how the objectives of this study have been met by indicating how each Chapter of this thesis contributed to the attainment of said objectives. Chapter 1, section 1.5 presents the overarching objectives of this study based on the problem statement in section 1.4.

The main research objective of this study was “To co-design a cybersecurity best practices framework for underserved rural communities.”

The sub-research objectives below allowed for the attainment of the main research objective.

1. To determine current security practices of underserved rural communities.
2. To investigate possible risks that exist in current technology use of underserved rural communities.
3. To evaluate online security best practices for underserved rural communities.
4. To identify components required for the development of a cybersecurity best practice framework for underserved rural communities.

Below an exposition of how the research objectives were met is provided.

Sub-research objective 1: To determine current security practices of underserved rural communities

Technology has permeated throughout most corners of the world and rural communities are included in this occurrence. This proliferation of technology throughout society has also meant that there is a need to understand how underserved rural communities practice security. The concept of underserved rural communities within computing is underrepresented in literature. Therefore, there was a need to understand the security practices of the communities that formed the case study. Interviews were conducted to determine these practices.

The presentation of the findings on the current security practices is provided in Chapter 4 Section 4.6.2. These findings centre around the notion of trust as a key determinant of security. The trust deals with how communities handle trust for strangers and those known to them. It is interesting to note that the level of trust accorded to strangers sometimes also depends on the individual approached for any type of assistance, the role within the community of the approached individual, who referred the person, and how that person presents themselves. These findings on trust complement findings by other scholars who also note that trusted persons can also be responsible for creating community links, delivering education, or aiding with sensitive tasks (Bada et al., 2015; McAlaney & Benson, 2020; Szumski, 2018; Winschiers-Theophilus et al., 2015).

This objective has been met.

Sub-research objective 2: To investigate possible risks that exist in current technology use of underserved rural communities.

Community members indicated that they own various types of devices – feature phones, smartphones, tablets, wireless dongles, and laptops. This finding is congruent with the findings built on those of Stork et al. (2013) who found the majority of Namibian in rural areas only possessed feature phones, with only calling and SMS capabilities. However, Stork and Calandro,

(2014) only a year later found that the Internet has gone mobile in Namibia, with more and newer users gaining access to the Internet through mobile devices.

The risks associated with technology use are captured in Chapter 4 Section 4.6.3. They look at sharing devices among community members and even those from the same homestead. Additionally, issues of the lack of passwords and pins to unlock technological devices in older participants as they trust their children, and how they dispose their devices pose risks in the usage of technology devices are presented. Tanner et al. (2023) their study on indigenous communities in remote areas in Canada also found that device sharing and password sharing to access devices are common among the communities they studied. In addition, Markert et al. (2021) share that password choice is dependent on a device and account users' strategy, this is also a finding that is like in this study.

This objective has been met.

Sub-research objective 3: To evaluate online security best practices for underserved rural communities.

The previous sub-research objective 2 looked at the types of devices that are owned by community members in underserved rural communities. Therein technology devices like smartphones, tablets, and laptops were found to have the capability of internet access. Therefore, this study also looked at the practices that community members espoused while online when the opportunity arose. It is worth noting as discussed in Chapter 2, section 2.9.2 that the cost of Internet in Namibia is rather expensive, especially for those rural communities, therefore as Chapter 4, section 4.6.4.2 shows that community members tend to only access the Internet when assisted by other (friends or relatives).

The online security practices identified in this study under Chapter 4, section 4.6.5 is categorised into two, secure and insecure practices. These practices range from authentication practices like pins and passwords, re-use of passwords across multiple online accounts, and logging out of social media accounts especially when sharing a mobile device as indicated under Sub-objective 2. However, as presented in the peer-reviewed publication of the findings of this sub-objective

(see appendix D.2), these practices need to be interpreted from an Afrocentric lens, they the use, appropriation, and adoption of technology within rural communities are affected by their culture, norms and values. From the perspective of a community member whose being is governed by Ubuntu and Uushiindaism ontology, is sharing bad? When the tenets of those two espouse sharing and reciprocity? (Nhinda & Shava, 2023b)

This objective has been met.

Sub-research objective 4: To identify components required for the development of a cybersecurity best practice framework for underserved rural communities

Addressing and meeting the first 3 sub-research objectives as presented earlier allowed the identification of components for this study. The refined framework was presented in Chapter 6, section 6.4 was constructed from 5 major components. The components are presented in Chapter 5, section 5.3, and Chapter 6, section 6.4. Section 5.3 presents 4 components, the first components is people and community, the third is the co-designed community engagement protocol and the fourth is the co-designed cybersecurity practices. These components were identified through the inductive approach as stated in Chapter 3, this approach suggests that through qualitative data collection methods like interviews, focus groups, and co-design sessions outcomes can be determined. The second component was identified through literature synthesis as presented in Chapter 2 section 2.5. The remaining fifth component, the national environment was identified through the expert focus groups as a missing component of the framework as part of the Evaluation of the framework presented in Chapter 6, section 6.3. Although the National environment component was not identified through the co-design sessions with the communities, it does provide for the completeness of the framework, especially considering the constitution of the expert focus group that suggested the improvement.

This objective has been met.

Sub-research objective 5: To evaluate the cybersecurity best practices framework for underserved rural communities

As with all DSR based research, the key components are the design and evaluation of the artefact developed. In the design of the artefact as presented in Chapter 5, the framework was preliminary designed and presented to the community members who validated the identified components. The design was then improved as suggested by the 5-simplified framework design steps presented in Chapter 5, section 5.2.

The evaluation was done as the design evolved. The first was the co-design of the some of the framework components (Component 1 and 3) which were also validated by the community members. The proposed CCSPF-4-URC was evaluated through an expert focus group, which comprised of experts from the community, cybersecurity, indigenous knowledge management, and human-computer interaction. The results of the evaluation are presented in Chapter 6.

The sub-objectives led to the co-design of the refined CCSPF-4URC framework, this co-design process ensured that for most parts of the study, the community was always involved. Leading to the attainment of the main research objective which is *“To co-design a cybersecurity best practices framework for underserved rural communities.”*. This study made various types of contributions to the body of knowledge; they are presented in the next section.

This objective has been met.

The main objective of this study has been achieved through the achievement of the sub-research objectives. This has led to the contributions to the body of knowledge in section 7.3 and in line with the Design Science Research framework adopted (Hevner et al., 2004) within this study, the feeding back into the knowledgebase was achieved through the publication of conference and journal articles as evidenced in Appendices D.1 – D.4.

7.3 CONTRIBUTION OF THE BODY OF KNOWLEDGE

This study contributed to the body of knowledge in multiple ways.

The most important contribution is bringing awareness to an area of knowledge that is underrepresented within literature and deserves more attention if the Internet and cyberspace are truly to emancipate all global citizens and create a true global village. These contributions are in line with the DSR methodology followed in this study as it relates to the relevance, rigor cycles, and the communication of research outcomes guidelines by Hevner et al. (2004).

1. Proposing a new methodological approach to cybersecurity research in rural underserved communities

This study proposed a new methodological approach to conducting research in rural underserved communities. The approach builds on the existing body of knowledge in community-based co-design activities, however, it makes room for the co-design of engagement guidelines and plugs into existing research methodologies. From a methodological standpoint, it ensures that the relevance and rigor of research projects meet the needs of the community through participatory methods.

This contribution was published in Nhinda and Bhunu Shava, (2021) as a peer-reviewed conference paper suggesting the use of participatory methods as an approach for cybersecurity research (see Appendix D.4). This proposed approach was also implemented as part of the methodology used in this study. The preliminary findings using this approach were presented at a peer-reviewed conference as an extended abstract (see Appendix D.4).

2. Cybersecurity practices of rural underserved communities

Cybersecurity practices of rural underserved communities were relatively unknown prior to this study. Therefore, this study contributes to the body of knowledge by bring these practices to the fore, not only through vanilla cybersecurity practices but also through categorising them as either secure or insecure practices. Though the study did not find some exotic "in the wild" practices, these practices are interpreted through the Afrocentric lenses of Ubuntu and Uushiindaism, which advocate for community, unity, sharing, reciprocity, and hospitality. The practices were also published in a peer-reviewed conference (Nhinda & Shava, 2023b) and are available in Appendix D.2 of the current study.

3. Co-designed community engagement protocol

This engagement protocol was collaboratively designed with the case study communities and validated by the communities. It entails the flow of information from the instance the researcher contacts the community to collaborate in research activities, the various key stakeholders that enable research, the ethical considerations within the community that need to be adhered to, and the best instances to get hold of the community. Another key is to share the research outputs with the community. This engagement protocol was published in a Journal (Nhinda & Shava, 2023a) and can be seen in Appendix D.1

4. Integration of Afrocentric methods for data analysis

For any research to postulate that it follows an Afrocentric lens in any shape, there is a need for alignment from research design, data collection, data analysis, and findings presentation. The language used also needs to be decolonial, in that it does not disparage Africans but situates them as the main protagonists within the research project. In this study, a contribution is made to look at cybersecurity data from this lens, to be cognizant of what the data means and from whose perspective it is being interpreted. Some might argue that conventional wisdom or knowledge alleges that there is a right way to conduct data analysis and the opposite of that too. However, a burning question is according to whose frames of reference?

This reflection by researchers might see a better understanding and better adherence to designed awareness campaigns. In addition, this has the potential to also impact existent behavioural models like the MINSCAPE, SCENE, and theories around technology acceptance like UTAUT and TAM. As such this is also a key contribution of this study to the body of knowledge.

5. Co-designed cybersecurity practices framework for rural underserved communities (CCSPF-4-URC)

The main objective of this study was to investigate how best to co-design a cybersecurity practice framework for rural underserved communities. This framework is a major contribution as it is novel and the first of its kind to the best of the researcher's knowledge. The five components

that make up this framework, 1) people and community, 2) international standards, 3) co-designed community engagement protocols, 4) national environment and 5) co-designed cybersecurity practices. This framework is presented in Chapter 6.

6. Two-pronged Qualitative framework evaluation in DSR based research studies

Within this study, a two-pronged approach for framework evaluation was utilised (Section 6.3.1 and 6.3.2). First ex-ante evaluation through co-design sessions was conducted. Here the communities within the case study identified, validated, and evaluated the components that they desired to be in a framework that aims to serve their needs. Additionally, ex-post qualitative expert focus group discussions about the framework were applied uniquely, the composition of the "experts" redefined what it means to be an expert as it relates to epistemological alignment within research projects. In this study, experts are knowledgeable in their areas of expertise, here, cybersecurity, human-computer interaction, indigenous knowledge management experts were joined by a community member who is an expert in her lived experience comprised the ex-post evaluation of the framework.

The idea of ex-ante and ex-post evaluations is not new to DSR research as scholars like Baskerville et al. (2009) proposed this approach as part of "soft design science methodology". However, the configuration of a qualitative "expert" group is a provocative contribution for researchers within, for, and with Africans in mind.

7.4 LIMITATIONS OF THE STUDY

- The duration of the study was limited to the duration of the academic study programme, therefore, prolonged interaction within this community might yield different results due to the fast-paced socio-technology evolution.
- There is a scarcity of existing literature about rural underserved communities and their technology use. When examining the cybersecurity culture, practices, and risk perceptions, this gap becomes agape. This scarcity of studies within this area limits the ability to contextualise our findings through comparative studies. This scarcity of studies

necessitates further investigation within this area of study to provide a comprehensive understanding of the problem domain and better situate the findings within this study.

- When working with the communities, different terminologies with reference to cybersecurity emerged. This resulted in challenges when translating terms from English to Navaho for people to comprehend what the study was all about. This language barrier may have impacted the community's understanding, leading to a possibly affected accuracy and depth in their responses.
- The framework was exclusively evaluated by communities from the Oukwanyama kingdom during the co-design sessions. Evaluating the framework with other communities might yield improvements to the framework on its robustness.

The next section reflects the study at a scientific, methodological, and personal level.

7.5 REFLECTIONS ON THE STUDY

In this section, scientific, methodological, and personal reflection are provided. The scientific reflection deals with situates the contributions of this study to the research community. The methodological reflection allows the researchers to show their stance and approach to conducting this multidisciplinary study. Personal reflection shows the growth through the research process.

7.5.1 Scientific reflection

The Internet is purported to present many economic, social, educational, and political benefits for all. However, some concerns need to be addressed when accessing the Internet. Within organisations and ministries, cybersecurity awareness campaigns are rife, but sadly, employees still fall victim to cybercriminals and sophisticated cyberattacks. These employees, organisations, and ministries, fortunately, employ dedicated staff to help deal with the "weakest link" within the cybersecurity programme of any organisation - the human. However, for the ordinary citizen, access to these protections is not always available, as such they are forced to rely on cybersecurity awareness campaigns from governments. A subset of these citizens resides in rural

areas that are in most cases, underserved. Underserved in this context refers to the lack of inadequacy of telecommunications infrastructure to allow them to access the Internet affordably.

Studying the challenges of rural communities in Africa is a multi-faceted challenge, that incorporates various disciplines. From behavioural science to philosophy and technology. This aims to bring out the socio-technical dimension of how communities evaluate, engage, and appropriate technology. Therefore, securing this sub-set "weakest link" from their perspective allows them to also enjoy the benefits of the Internet securely.

The fact that most of the Internet users in rural communities are mobile first, presents a challenge around design requirements for their cybersecurity awareness campaigns. As such, co-designing emerges as the most appropriate methodology as it aligns with existing practices of decision-making within communities. This aligns with Namibia's slogan "No Namibian but be left out", this contribution to the discourse on safer internet for all also builds on the inclusivity aspect and mission of international bodies like the Internet Society and African Union Commission on Cybersecurity.

7.5.2 Methodological reflection

A researcher can never divorce themselves from the research they conduct, as such, bias is always a challenge and risk they must manage. I am an OmuKwanyama, born in the Engela State hospital, I came from the community that formed the case study. As such, that is my first point of departure, therefore, I cannot distance myself from the research. As an African, I have experience and ideas about the challenges this community faces, especially as a technology expert who is referred to for all things technology. This experiential knowledge assisted with connecting with the community as a native researcher to allow the construction of the co-design process, in the codesigned community engagement protocol and the resultant, co-design framework

As Afrocentric and decolonial researchers, there is a need to correct the narrative of Africans within research discourse, therefore researchers need to be mindful of research methodology

choice. In this study the Design Science Research methodology, coupled with the Afrocentric interpretivist paradigm answers the question "Was the appropriate methodology chosen for the identified problem?". The focus remains on the problem of understanding the risks of technology use, and cybersecurity practices and co-designing a framework that addresses the needs of Africans, thereby centering the African. The data were collected through interviews, focus groups, co-design sessions and literature, and expert focus groups. The thematic data analysis from the lenses of Ubuntu and Uushiindaism, which resulted in the framework components was employed, providing an understanding of the challenges and opportunities that exist within cybersecurity research within these communities.

7.5.3 Personal reflection

Research offers the opportunity to study an identified problem to find a solution that is fit for purpose. However, another facet of research that I have come to embrace is the concept of unlearning and relearning. I started this journey motivated by a passion for people, human-computer interaction, and cybersecurity, looking at how to possibly design better solutions for humans as they interact with technology. The area case study site came naturally as I often found myself as a sort of IT support for my community in the village. I came to realise that there is a disconnect between what we understand as best practices and what the community members I engaged with practiced.

As the study progressed, I came to understand and embrace that knowledge is an evolving concept, whereby we learn from each other, this was a key takeaway from the communities that I engaged with in this study. Additionally, validity of knowledge is not just based on it being codified in written form but orality-based cultures such as the one that I engaged with during this study are equally just valid and needs to be preserved and embraced as we tackle the cybersecurity challenge, in unity.

7.6 FUTURE WORK

Scholars like Hevner et al. (2004) and Jabareen (2009) have acknowledged that artefacts that are developed as an outcome of research are constantly evolving and require reflection and further refinement. For this reason, this study serves as a starting point for future research work, both from an academic and practitioner perspective. Cybersecurity in rural areas in Namibia and most African countries is an understudied area that holds much potential.

- Therefore, further longitudinal studies could provide empirical evidence on how this space evolves and further exposure to external influence; especially now as the connectivity infrastructure becomes gradually available in many rural areas.
- From a methodological perspective, this study was qualitative, although qualitative case studies allow for in-depth understanding, a combination with quantitative aspects might help to study the case and effects of communal behaviour as it relates to cybersecurity.
- Operationalisation of the CCSPF-4-URC framework while addressing the shortcomings identified in Chapter 6 could also prove valuable to the national efforts to ensure that the cybersecurity posture of the nation is ironclad.
- Co-development of cybersecurity awareness messaging and training in the local languages from an Afrocentric perspective could also be an interesting area of research.
- Co-designing mobile interfaces with communities often on the fringes of society for security could also provide new insights into how the rest of the world perceives security and help provide edge cases for technology developers globally.
- Lastly, a nationwide quantitative study of cybersecurity practices and possible awareness would be fundamental to the success of any future research in this area.
- Testing the framework with other communities to confirm its ability to solve the identified problem and test its environmental utility.
- Community-based co-co-design to deepen community involvement in the development of framework implementation with other communities.

7.7 CONCLUDING REMARKS

This Chapter concludes this research. The main objective of this study was to co-design a cybersecurity best practices framework for underserved rural communities. This objective was further subdivided into five sub-research objectives (Chapter 1, section 1.4), which were achieved in this research. Data collection and analysis and the final artefact are presented in Chapter 6.

Cybersecurity research in Namibia, especially in underserved communities is still in its infancy stages. This observation which was also noted in Chapter 2 leaves room for further investigation. Rural communities are often still intact in terms of their cultural practices, albeit somewhat influenced by the socio-political history of the country. There needs to be a reflection in the research methods that researchers choose to use in these communities, reflecting also on their positionality as it relates to their philosophical assumptions. In this study, the research philosophy stands on the Afrocentric position, looking to right the wrongs of the past by centering Africans at the heart of their reality. It is for this reason that data collection methods like co-design were employed to ensure that the end-artefact that was developed in this study – the CCSPF-4-URC framework – truly is centric to the communities and meets their needs as presented in Chapters 3, 4, 5, and 6.

Finally, in this study, my reflections on growth through the research process and the reciprocal learning from the community are given, befitting the conclusion of a journey as the OvaKwanyama proverbs provided teaching and guidance during this time:

"Tashi ya ihashi londelwa, tashi i osho hashi talwa."

(Only the past can be seen and studied, what is to come cannot be rushed into nor anticipated, because one does not know when it will come, but the exercise of patience is wise.)

"Ihadi wanene omutwe umwe."

(Knowledge does not reside with one but rather a collective, therefore, consult when needed.)

REFERENCES

- African Union. (2014). *African Union convention on cybersecurity and personal data protection*.
- Ajzen, I. (1991). The theory of planned behavior. *Organizational behavior and human decision processes*, 50(2), 179–211. [https://doi.org/https://doi.org/10.1016/0749-5978\(91\)90020-T](https://doi.org/https://doi.org/10.1016/0749-5978(91)90020-T)
- Ajzen, I. (2002). Perceived behavioral control, self-efficacy, locus of control, and the theory of planned behavior. *Journal of Applied Social Psychology*, 32(4), 665–683.
- Akama, Y., Faily, S., Coles-Kemp, L., Dunphy, P., Just, M., & De Luca, A. (2013). Designing interactive secure systems: CHI 2013 special interest group. *CHI'13 Extended Abstracts on Human Factors in Computing Systems, 2013-April* 2469–2472. <https://doi.org/10.1145/2468356.2468807>
- Almansoori, A., Al-Emran, M., & Shaalan, K. (2023). Exploring the frontiers of cybersecurity behavior: A systematic review of studies and theories. *Applied Sciences*, 13(9), 5700. <https://doi.org/10.3390/app13095700>
- Alsheri, T., Abokhodair, N., & Olivier, P. (2019). *Understanding culture with a transnational population: A value-sensitive approach*. <https://doi.org/10.31235/osf.io/kpz2r>
- Aludhilu, H. N., & Bidwell, N. J. (2018). Home is not Egumbo: Language, identity and web design. *2nd Second African Conference for Human Computer Interaction Proceedings*, 1–11. <https://doi.org/10.1145/3283458.3283460>
- Asante, M. K. (2017a). Afrocentricity: Notes on a disciplinary position. In M. K. Asante & M. Karenga (Eds.), *Handbook of black studies* (pp. 152–164). Sage Publications.
- Asante, M. K. (2017b). The philosophy of afrocentricity. In A. Afolayan & T. Falola (Eds.), *The Palgrave handbook of African philosophy* (pp. 231–244). Palgrave Macmillan. https://doi.org/https://doi.org/10.1057/978-1-137-59291-0_16

- Atkins, D. E., Droegemeier, K. K., Feldman, S. I., Garcia-Molina, H., Klein, M. L., Messerschmitt, D. G., Messina, P., Ostriker, J. P., & Wright, M. H. (2003). *Revolutionizing science and engineering through cyberinfrastructure: Report of the national science foundation blue-ribbon advisory panel on cyberinfrastructure*.
- Aurigemma, S., & Panko, R. (2012). A composite framework for behavioural compliance with information security policies. *Proceedings of the Annual Hawaii International Conference on System Sciences*, 3248–3257. <https://doi.org/10.1109/HICSS.2012.49>
- Bada, M., Sasse, A., & Nurse, J. (2015). Cyber security awareness campaigns: Why they fail to change behaviour. *International Conference on Cyber Security for Sustainable Society*, 11. <http://www.cs.ox.ac.uk/publications/publication9343-abstract.html%0Ahttp://discovery.ucl.ac.uk/1468954/1/AwarenessCampaignsDraftWorkingPaper.pdf>
- Baskerville, R., Pries-Heje, J., & Venable, J. (2009). Soft design science methodology. *Proceedings of the 4th International Conference on Design Science Research in Information Systems and Technology, DESRIST '09*. <https://doi.org/10.1145/1555619.1555631>
- Bhunu Shava, F., & Van Greunen, D. (2014). Designing user security metrics for security awareness at higher and tertiary institutions. *Proceedings of the 8th International Development Informatics Association Conference*, 281–296.
- Bidwell, N., & Hardy, D. (2008). Dilemmas in situating participation in rural ways of saying. *Proceedings of the 21st Annual Conference of the Australian Computer-Human Interaction Special Interest Group: Design: Open 24/7*, 145–152.
- Bidwell, N. J. (2009). Anchoring design in rural customs of doing and saying. *Human-Computer Interaction—INTERACT 2009: 12th IFIP TC 13 International Conference*, 686–699.
- Bidwell, N. J. (2020). Women and the sustainability of rural community networks in the global south. *ACM International Conference Proceeding Series*, 1–13. <https://doi.org/10.1145/3392561.3394649>

- Bidwell, N. J., Winschiers-Theophilus, H., Koch Kapuire, G., & Rehm, M. (2011). Pushing personhood into place: Situating media in rural knowledge in Africa. *International Journal of Human Computer Studies*, 69(10), 618–631. <https://doi.org/10.1016/j.ijhcs.2011.02.002>
- Bodunrin, P. O. (1981). The question of African philosophy. *Philosophy*, 56(216), 161–179. <https://about.jstor.org/terms>
- Bourke, D., Boland, S., Bourke, P., & Gilligan, J. (2018, October 30). A co-design partnership to develop universally designed ict applications for people with intellectual disability. *Universal Design & Higher Education in Transformation Congress*.
- Briggs, P., Jeske, D., & Coventry, L. (2017). Behaviour change interventions for cybersecurity. In *behaviour change research and theory: Psychological and technological perspectives*. Elsevier Inc. <https://doi.org/10.1016/B978-0-12-802690-8.00004-9>
- Busumtwi-Sam, J. (2019). Remittances, regulation, and financial development in Sub-Saharan Africa. In A. Hira, N. Gaillard, & T. Cohn (Eds.), *The failure of financial regulation* (pp. 153–190). Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-030-05680-3_5
- Chawane, M. (2000). The development of Afrocentricity: A historical survey. *The Western Journal of Black Studies*, 24(4), 223–238. <https://doi.org/10.17159/2223-0386/2016/n16a5>
- Clark, K. (2005). Serving underserved communities with instructional technologies giving them what they need, not what you want. *Urban Education*, 40(4), 430–445. <https://doi.org/10.1177/0042085905276388>
- Cleven, A., Gubler, P., & Hüner, K. M. (2009). Design alternatives for the evaluation of design science research artifacts. *Proceedings of the 4th International Conference on Design Science Research in Information Systems and Technology - DESRIST '09*, 1–8. <https://doi.org/https://doi.org/10.1145/1555619.1555645>
- Communications Regulatory Authority of Namibia. (2019). *2019 Annual report*.

- Cousineau, T. (2004). *Narrowing the Divide*.
<https://www.itu.int/osg/spu/youngminds/2006/essays/essay-travis-cousineau.pdf>.
- Coventry, L., Briggs, P., Blythe, J., & Tran, M. (2014). Using behavioural insights to improve the public's use of cyber security best practices. In *Project Report. Government Office for Science*.
- Coventry, L., Briggs, P., Jeske, D., & van Moorsel, A. (2014). SCENE: A structured means for creating and evaluating behavioural nudges in a cyber security environment. In Aaron Marcus and Associates (Ed.), *Design, user experience, and usability. Theories, methods, and tools for designing the user experience: Third international conference, DUXU 2014, Held as Part of HCI International 2014* (Vol. 8517, Issue PART 1, pp. 229–239). Springer International Publishing. https://doi.org/10.1007/978-3-319-07668-3_23
- Craigien, D., Diakun-Thibault, N., & Purse, R. (2014). Defining Cybersecurity. *Technology Innovation Management Review*, 4(10), 13–21. <https://doi.org/10.22215/timreview/835>
- Creswell, J. W., & Creswell, D. J. (2018). *Research design: Qualitative, quantitative, and mixed methods approaches* (Fifth edition). SAGE Publications, Inc.
- Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioural information security research. *Computers & Security*, 32, 90–101. <https://doi.org/10.1016/j.cose.2012.09.010>
- Da Veiga, A., & Martins, N. (2014). Information security culture: A comparative analysis of four assessments. In J. Devos & S. De Haes (Eds.), *Proceedings of the 8th European conference on IS management and evaluation* (pp. 49–57). Academic Conferences and Publishing International Limited.
- David, S., Sabiescu, A. G., & Cantoni, L. (2013). Co-design with communities. A reflection on the literature. *Proceedings of the 7th International Development Informatics Association Conference*, 152–166.

- De Paula, R. (2013). Designing for the 'emerged' markets. *Interactions*, 20(2), 12–14.
<https://doi.org/10.1145/2427076.2427080>
- Dearden, A., & Kleine, D. (2018). Minimum ethical standards in ICTD / ICT4D research: A co-produced document. *Published Standards. University of Sheffield*, 1–13.
<https://ictdethics.wordpress.com/minimum-ethical-standards-in-ictd-ict4d-research-a-co-produced-document/>
- Deckert, C., & Schomaker, R. M. (2022). Cultural tightness–looseness and national innovativeness: impacts of tolerance and diversity of opinion. *Journal of Innovation and Entrepreneurship*, 11(1), 29. <https://doi.org/10.1186/s13731-022-00219-2>
- Dlamini, Z. I., Olivier, M. S., & Grobler, M. M. (2016, March 17). the smartphone evidence awareness framework for the users. *ICCWS 2016 11th International Conference on Cyber Warfare and Security: ICCWS2016*.
- Dlodlo, N., & Hamunyela, S. (2017). The status of integration of health information systems in Namibia. *The Electronic Journal Information Systems Evaluation*, 20(2), 61–75.
www.ejise.com
- Dolan, P., Hallsworth, M., Halpern, D., King, D., Metcalfe, R., & Vlaev, I. (2012). Influencing behaviour: The mindspace way. *Journal of Economic Psychology*, 33(1), 264–277.
<https://doi.org/10.1016/j.joep.2011.10.009>
- Dolan, P., Hallsworth, M., Halpern, D., King, D., & Vlaev, I. (2010). *MINSPACE Influencing behaviour through public policy*. Institute of Government.
<http://eprints.lse.ac.uk/id/eprint/35792>
- Dugdale, A., Daly, A., Papandrea, F., & Maley, M. (2005). Accessing e-government: Challenges for citizens and organizations. *International Review of Administrative Sciences*, 71(1), 109–118.
<https://doi.org/10.1177/0020852305051687>

- Dutta, U., & Das, S. (2016). The digital divide at the margins. *Communication Design Quarterly*, 4(1), 36–48. <https://doi.org/10.1145/2875501.2875504>
- Dutton, W. H. (2017). Fostering a cyber security mindset. *Internet Policy Review*, 6(1), 1–14. <https://doi.org/10.14763/2017.1.443>
- Ekandjo, T. A. T., Jazri, H., & Peters, A. (2018). Online social networks risk to organisations. *Proceedings of the Second African Conference for Human Computer Interaction: Thriving Communities*, 1–4. <https://doi.org/10.1145/3283458.3283465>
- El Hajal, G., Abi Zeid Daou, R., & Ducq, Y. (2021). Human firewall: Cyber awareness using WhatsApp AI Chatbot. *2021 IEEE 3rd International Multidisciplinary Conference on Engineering Technology (IMCET)*, 66–70. <https://doi.org/10.1109/IMCET53404.2021.9665642>
- Enayaty-Ahangar, F., Albert, L. A., & DuBois, E. (2021). A survey of optimization models and methods for cyberinfrastructure security. *IIE Transactions*, 53(2), 182–198. <https://doi.org/10.1080/24725854.2020.1781306>
- Frohlich, K. (2017). Evaluating the effects of e-government initiatives on citizen-centric goals at selected Namibian Government Ministry. *2017 IST-Africa Week Conference (IST-Africa)*, 1–9. <https://doi.org/10.23919/ISTAFRICA.2017.8102361>
- Fröhlich, K., Jain, K., Pinomaa, A., & Nieminen, M. (2021). Empowering communities in marginalized surroundings: Opportunities from collaborative community-managed electrification and advanced ICT. *CHI Greece 2021: 1st International Conference of the ACM Greek SIGCHI Chapter*, 1–7. <https://doi.org/10.1145/3489410.3489437>
- Fröhlich, K., Nieminen, M., Peters, A., & Pinomaa, A. (2018). Considerations for co-designing e-government services in under-served rural communities. *Proceedings of the Second African Conference for Human Computer Interaction: Thriving Communities*, 1–4. <https://doi.org/10.1145/3283458.3283476>

- Fröhlich, K., & Peters, A. (2017). E-government social exclusion and satisfaction among Namibian citizens: A case of a Namibian government ministry. *Proceedings of the South African Institute of Computer Scientists and Information Technologists*, 1–6. <https://doi.org/10.1145/3129416.3129435>
- Furuholt, B., & Sæbø, Ø. (2018). The role telecentres play in providing e-government services in rural areas. *Electronic Journal of Information Systems in Developing Countries*, 84(1), 1–14. <https://doi.org/10.1002/isd2.12006>
- Gcaza, N., & von Solms, R. (2017). Cybersecurity culture: An ill-defined problem. In *10th IFIP World Conference on Information Security Education (WISE)* (Issue May 2017, pp. 98–109). https://doi.org/10.1007/978-3-319-58553-6_9
- Gelfand, M. J., Nishii, L. H., & Raver, J. L. (2006). On the nature and importance of cultural tightness-looseness. *Journal of Applied Psychology*, 91(6), 1225–1244. <https://doi.org/10.1037/0021-9010.91.6.1225>
- Golla, M., Wei, M., Hainline, J., Filipe, L., Dürmuth, M., Redmiles, E., & Ur, B. (2018). What was that site doing with my Facebook password? *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, 1549–1566. <https://doi.org/10.1145/3243734.3243767>
- Gregg, D. G., Kulkarni, U. R., & Vinze', A. S. (2001). Understanding the philosophical underpinnings of software engineering research in information systems. *Information Systems Frontiers*, 3(2), 169–183. <https://doi.org/https://doi.org/10.1023/A:1011491322406>
- Grobler, M., Dlamini, Z., Ngoben, S., & Labuschagne, A. (2011). Towards a cyber security aware rural community. *Proceedings of the 2011 Information Security for South Africa (ISSA) Conference.*, 1–7. <https://doi.org/http://hdl.handle.net/10204/5183>
- Grobler, M., van Vuuren, J. J., & Zaaiman, J. (2011). Evaluating cyber security awareness in South Africa. *10th European Conference on Information Warfare and Security 2011, ECIW 2011*, 113–121. <http://hdl.handle.net/10204/5108>

- Hardy, J., Wyche, S., & Veinot, T. (2019). Rural HCI research. *Proceedings of the ACM on Human-Computer Interaction*, 3(CSCW), 1–33. <https://doi.org/10.1145/3359298>
- Hasbi, M., & Dubus, A. (2020). Determinants of mobile broadband use in developing economies: Evidence from Sub-Saharan Africa. *Telecommunications Policy*, 44(5), 101944. <https://doi.org/10.1016/j.telpol.2020.101944>
- Hevner, A. R. (2007). A three cycle view of design science research. *Scandinavian Journal of Information Systems*, 19(2), 87–92. <https://aisel.aisnet.org/sjis/vol19/iss2/4>
- Hevner, A. R., March, S., Park, J., & Ram, S. (2004). Design science in information systems research. *MIS Quarterly*, 28(1), 75–105. <https://doi.org/10.2307/25148625>
- Hevner, B. A. R., March, S. T., Park, J., & Ram, S. (2004). design science in information systems research. *MIS Quarterly*, 28(1), 75–105.
- Holliday, A. (2018). The politics of ethics in diverse cultural settings: Colonising the centre stage. In A. Robinson-Pant & N. Singal (Eds.), *Researching Ethically across Cultures: Issues of knowledge, power and voice* (1st ed., pp. 113–130). Routledge. <https://doi.org/https://doi.org/10.4324/9781315620497>
- Hone, K. E. (2016). *Namibia's digital foreign policy and diplomacy: Towards greater co-operation and prosperity in a connected world*. <http://www.itu.int/net4/ITU-D/idi/2015/#idi2015countrycard-tab&NAM>
- Houtondji, P. (1956). On 'African philosophy'. *Thought and practice*.
- Huntinghawk, F., Richard, C., Plosker, S., & Srivastava, G. (2020). Expanding cybersecurity knowledge through an indigenous lens: A first look. *2020 IEEE Canadian Conference on Electrical and Computer Engineering (CCECE)*, 1–4. <https://doi.org/10.1109/CCECE47787.2020.9255753>

- Hussain, A., Mohamed, A., & Razali, S. (2020). A review on cybersecurity. *Proceedings of the 3rd International Conference on Networking, Information Systems & Security*, 1–7. <https://doi.org/10.1145/3386723.3387847>
- International Telecommunication Union. (2020). *Manual for measuring ict access and use by households and individuals*.
- International Telecommunications Union. (2022). *Digital development dashboard: An overview of the state of digital development around the world based on ITU data - Namibia*.
- Islam, A., & Hoq, K. M. G. (2010). Community internet access in rural areas: A study on community information centres in Bangladesh. *Malaysian Journal of Library and Information Science*, 15(2), 109–124. <https://tamilperaivu.um.edu.my/index.php/MJLIS/article/view/6936>
- Jabareen, Y. (2009). Building a conceptual framework: Philosophy, definitions, and procedure. *International Journal of Qualitative Methods*, 8(4), 49–62. <https://doi.org/10.1177/160940690900800406>
- Kainda, R., Flechais, I., & Roscoe, A. W. (2010). Two heads are better than one: Security and usability of device associations in group scenarios. *Proceedings of the Sixth Symposium on Usable Privacy and Security*, 1–13. <https://doi.org/10.1145/1837110.1837117>
- Kapuire, G. K. (2023). *An Ubuntu lens to Co-Design: Towards a rural community engagement framework* [Doctor of Philosophy]. Queensland University of Technology.
- Kapuire, G. K., Winschiers-Theophilus, H., & Brereton, M. (2017). Deriving engagement protocols within community-based co-design projects in Namibia. *14th International Conference on Social Implications of Computers in Developing Countries (ICT4D)*, 381–393. https://doi.org/10.1007/978-3-319-59111-7_32
- Kivunja, C., & Kuyini, A. B. (2017). Understanding and applying research paradigms in educational contexts. *International Journal of Higher Education*, 6(5), 26. <https://doi.org/10.5430/ijhe.v6n5p26>

- Kritzinger, E., & Solms, S. (2013). A framework for cyber security in Africa. *Journal of Information Assurance & Cybersecurity*, 2012, 1–10. <https://doi.org/10.5171/2012.322399>
- Kuechler, W., & Vaishnavi, V. (2011). Promoting relevance in IS research: An informing system for design science research. *Informing science: The International Journal of an Emerging Transdiscipline*, 14, 125–138. <https://doi.org/10.28945/1498>
- Lincoln, Y. S., & Guba, E. G. (2000). Paradigmatic controversies, contradictions and emerging confluences. In *The Sage handbook of qualitative research* (pp. 97–128).
- March, S. T., & Smith, G. F. (1995). Design and natural science research on information technology. *Decision Support Systems*, 15(4), 251–266. [https://doi.org/10.1016/0167-9236\(94\)00041-2](https://doi.org/10.1016/0167-9236(94)00041-2)
- Markert, P., Bailey, D. V., Golla, M., Durmuth, M., & Aviv, A. J. (2020). This PIN can be easily guessed: Analyzing the security of Smartphone Unlock PINs. *2020 IEEE Symposium on Security and Privacy (SP)*, 2020-May, 286–303. <https://doi.org/10.1109/SP40000.2020.00100>
- Markert, P., Bailey, D. V., Golla, M., Dürmuth, M., & Aviv, A. J. (2021). On the Security of Smartphone Unlock PINs. *ACM Transactions on Privacy and Security*, 24(4), 1–36. <https://doi.org/10.1145/3473040>
- Marufu, A. M. C., & Sibanda, K. (2013). An M-Commerce security framework for ICT4D Contexts. *Southern Africa Telecommunication Networks and Applications Conference (SATNAC), SEPTEMBER 2013*, 271–276. <https://doi.org/10.13140/2.1.1624.1922>
- Mason, M. (2010). sample size and saturation in PhD studies using qualitative interviews. *Forum Qualitative Sozialforschung Forum: Qualitative Social Research*, 11(3). <https://doi.org/https://doi.org/10.17169/fqs-11.3.1428>

- Mathiasen, N. R., & Bodker, S. (2008). Threats or threads - From usable security to secure experience. *Proceedings of the 5th Nordic Conference on Human-Computer Interaction: Building Bridge*, 283–289.
- Mbenzi, P. A., & Ashikuti, S. N. (2018). Uushiindaism as a collective poverty alleviation mechanism and social support. *Journal of University of Namibia Language Centre*, 3(1), 2026–8297.
- McAlaney, J., & Benson, V. (2020). Cybersecurity as a social phenomenon. In *Cyber Influence and Cognitive Threats* (pp. 1–8). Elsevier. <https://doi.org/10.1016/B978-0-12-819204-7.00001-4>
- Merriam, S. B. (2009). *Qualitative research: A guide to design and implementation*. John Wiley & Sons, Inc.
- Merriam, S. B., & Tisdell, E. J. (2016). *Qualitative research: A guide to design and implementation: Vol. Fourth edition* (4th ed.). The Jossey-Bass higher and adult education series.
- Miles, M. B., Huberman, M. A., & Saldana, J. (2014). *Qualitative data analysis: A methods sourcebook* (3rd ed.). Sage Publications, Inc.
- Ministry of Urban and Rural Development. (2017). *Republic of Namibia national rural development strategy technical assistance to the preparation of a rural development Sector programme in Namibia* (pp. 1–72).
- Mkabela, Q. (2005). Using the Afrocentric method in researching indigenous African culture. *The Qualitative Report*, 10(1), 178–189. <https://doi.org/10.46743/2160-3715/2005.1864>
- Mobile Telecommunications Limited. (2019). *2019 Integrated annual report*. [https://www.mtc.com.na/uploads/downloads/annual_reports/MTC Integrated Annual Report 2019_singles.pdf](https://www.mtc.com.na/uploads/downloads/annual_reports/MTC_Integrated_Annual_Report_2019_singles.pdf)
- Mokobane, N. B., & Botha, R. A. (2020). Does ubuntu influence social engineering susceptibility? In *International Symposium on Human Aspects of Information Security and Assurance* (pp. 97–108). Springer, Cham. https://doi.org/10.1007/978-3-030-57404-8_8

- Moosa, D. (2013). Challenges to anonymity and representation in educational qualitative research in a small community: A reflection on my research journey. *Compare: A Journal of Comparative and International Education*, 43(4), 483–495. <https://doi.org/10.1080/03057925.2013.797733>
- Muashekele, C., Winschiers-Theophilus, H., & Kapuire, G. K. (2019). Co-design as a means of fostering appropriation of conservation monitoring technology by indigenous communities. *Proceedings of the 9th International Conference on Communities & Technologies - Transforming Communities*, 126–130. <https://doi.org/10.1145/3328320.3328383>
- Mukiibi, H. (2019). Cyber security in Africa: The boring technology story that matters. *XRDS: Crossroads, The ACM Magazine for Students*, 26(2), 56–59. <https://doi.org/10.1145/3368077>
- Muwanga-Zake, J. W. F. (2009). Building bridges across knowledge systems: Ubuntu and participative research paradigms in Bantu communities. *Discourse: Studies in the Cultural Politics of Education*, 30(4), 413–426. <https://doi.org/10.1080/01596300903237198>
- Mwangala, J., Shava, F. B., & Chitauro, S. (2023). Human intelligence an enabler for cyber resilience: A case for Namibian public institutions. *2023 IST-Africa Conference (IST-Africa)*, 1–10. <https://doi.org/10.23919/IST-Africa60249.2023.10187836>
- Namibia Statistics Agency. (2014a). *2011 Population and housing census - Ohangwena Regional Profile*.
- Namibia Statistics Agency. (2014b). *Namibia 2011 population & housing census*. [http://www.nsa.org.na/files/downloads/Namibia 2011 Population and Housing Census Main Report.pdf](http://www.nsa.org.na/files/downloads/Namibia%202011%20Population%20and%20Housing%20Census%20Main%20Report.pdf)
- Namibia Statistics Agency. (2017a). *2017 Namibia financial inclusion survey (NFIS)*.
- Namibia Statistics Agency. (2017b). *Namibia Inter-censal demographic survey 2016 Report*.

Namibia Statistics Agency. (2024). *2023 population & housing census preliminary report*.

Nandi, S., Thota, S., Nag, A., Divyasukhananda, Sw., Goswami, P., Aravindakshan, A., Rodriguez, R., & Mukherjee, B. (2016). Computing for rural empowerment: Enabled by last-mile telecommunications. *IEEE Communications Magazine*, 54(6), 102–109. <https://doi.org/10.1109/MCOM.2016.7498095>

Nhinda, G. T., & Bhunu Shava, F. (2021). Towards the use of participatory methods in Cybersecurity research in rural Africa: A grassroots approach. *2021 3rd International Multidisciplinary Information Technology and Engineering Conference, IMITEC 2021*, 1–8. <https://doi.org/10.1109/IMITEC52926.2021.9714649>

Nhinda, G. T., & Shava, F. B. (2023a). Co-CEP: A co-designed community engagement protocol as a catalyst for cybersecurity research in Africa: The case of northern Namibia. *Journal of Information and Optimization Sciences*, 44(3), 475–492. <https://doi.org/10.47974/JIOS-1407>

Nhinda, G. T., & Shava, F. B. (2023b). cybersecurity practices of rural underserved communities in Africa: A case study from northern Namibia. *2023 International Conference on Artificial Intelligence, Big Data, Computing and Data Communication Systems (IcABCD)*, 1–7. <https://doi.org/10.1109/icABCD59051.2023.10220449>

NIST. (2023). *NIST cybersecurity framework 2.0 concept paper: Potential significant updates to the cybersecurity framework note to reviewers*.

Oates, B. J. (2012a). *Researching information systems and computing*. Sage Publications Inc.

Oates, B. J. (2012b). *Researching information systems and computing*. Sage Publications Inc.

Oltedal, S., Moen, B., Klempe, H., & Rundmo, T. (2004). *Explaining risk: An evaluation of cultural theory*.

- Pais, A. (2007). Bridging the digital divide by bringing connectivity to underserved areas of the world. *Proceedings International Conference Education without Borders*, 1–5.
- Pathak, P., Pal, P. R., Shrivastava, M., & Ora, P. (2019). Fifth revolution: Applied AI & human intelligence with cyber-physical systems. *International Journal of Engineering and Advanced Technology*, 8(3), 23–27.
- Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A design science research methodology for information systems research. *Journal of Management Information Systems*, 24(3), 45–77. <https://doi.org/10.2753/MIS0742-1222240302>
- Pellerin, M. (2012). Benefits of Afrocentricity in exploring social phenomena: Understanding Afrocentricity as a social science methodology. *The Journal of Pan African Studies*, 5(4), 149–160.
- Plosker, S., & Srivastava, G. (2021). Cybersecurity education in rural indigenous Canada. *2021 IEEE Canadian Conference on Electrical and Computer Engineering (CCECE)*, September, 1–6. <https://doi.org/10.1109/CCECE53047.2021.9569147>
- Prasad, R., & Rohokale, V. (2020). *Cyber security: The lifeline of information and communication technology* (R. Prasad, Ed.). Springer. [https://doi.org/https://doi.org/10.1007/978-3-030-31703-4](https://doi.org/10.1007/978-3-030-31703-4)
- Pries-Heje, J., Baskerville, R., & Venable, J. R. (2008). Strategies for design science research evaluation. *ECIS 2008 Proceedings*, 87.
- Quayyum, F., & Freberg, G. N. (2023). Designing cybersecurity awareness solutions for the young people in rural developing countries: The need for diversity and inclusion. *ArXiv, abs/2312.12073*, 1–17. <https://beinternetawesome.withgoogle.com/en>
- Reichel, J., & Peck, F. (2020). I have too much respect for my elders: Understanding South African mobile users ' perceptions of privacy and current behaviours on Facebook and WhatsApp. *Security*.

Republic of Namibia. (2009). *Communications Act 8 of 2009*.

Republic of Namibia. (2017). *Namibia's 5th National Development Plan (NDP5)*.
https://www.npc.gov.na/?wpfb_dl=294

Republic of Namibia. (2019a). *Electronic Transactions Act 4 of 2019*.

Republic of Namibia. (2019b). *Republic of Namibia National Broadband Policy (NBP) for the Republic of Namibia: 2019-2029*.

Republic of Namibia. (2022a). *Access to Information Act of 2022*.

Republic of Namibia. (2022b). *Namibia national cybersecurity strategy and awareness raising plan 2022-2027* (pp. 1–47).

Rey-Moreno, C., Blignaut, R., Tucker, W. D., & May, J. (2016). An in-depth study of the ICT ecosystem in a South African rural community: Unveiling expenditure and communication patterns. *Information Technology for Development*, 22(sup1), 101–120.
<https://doi.org/10.1080/02681102.2016.1155145>

Rey-Moreno, C., & Graaf, M. (2016). Map of the community network initiatives in Africa. *L. Belli, Community Connectivity: Building the Internet from Scratch, October*, 149–169.

Rey-Moreno, C., Tucker, W. D., Cull, D., & Blom, R. (2015). Making a community network legal within the South African Regulatory Framework. *ACM International Conference Proceeding Series*, 15. <https://doi.org/10.1145/2737856.2737867>

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *The Journal of Psychology*, 91(1), 93–114.

Rowley, J. (2002). Using case studies in research. *Management research news*, 25(1), 16–27.

- Safa, N. S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N. A., & Herawan, T. (2015). Information security conscious care behaviour formation in organizations. *Computers & Security*, 53, 65–78. <https://doi.org/10.1016/j.cose.2015.05.012>
- Salemink, K., Strijker, D., & Bosworth, G. (2017). Rural development in the digital age: A systematic literature review on unequal ICT availability, adoption, and use in rural areas. *Journal of Rural Studies*, 54, 360–371. <https://doi.org/https://doi.org/10.1016/j.jrurstud.2015.09.001>
- Sanders, E. B., & Stappers, P. J. (2008). Co-creation and the new landscapes of design. *CoDesign*, 4(March), 1–16. <https://doi.org/10.1080/15710880701875068>
- Schia, N. N. (2018). The cyber frontier and digital pitfalls in the Global South. *Third World Quarterly*, 6597, 1–17. <https://doi.org/10.1080/01436597.2017.1408403>
- Sefotho, M. M. (2015). A researcher's dilemma: Philosophy in crafting dissertations and theses. *Journal of Social Sciences*, 42(1–2), 23–36.
- Shapopi, J., Limbo, A., & Backes, M. (2023). Namibia's first high performance computer. In *South African Computer Journal* (Vol. 35, Issue 1, pp. 4–18). South African Institute of Computer Scientists and Information Technologists. <https://doi.org/10.18489/sacj.v35i1.1189>
- Shelton, B. K. (1985). The social and psychological impact of unemployment. *Journal of Employment Counseling*, 22(1), 18–22. <https://doi.org/10.1002/j.2161-1920.1985.tb00808.x>
- Shen, L. (2014). The NIST cybersecurity framework: Overview and potential impacts. *Scitech Lawyer*, 10(4), 16–19.
- Shihomeka, S. P. (2017). Engaging citizens: Youth, mobile phones, political leadership and inclusive democracy in the Ohangwena Region, Namibia. *NAWA Journal of Language and Communication (NJLM)*, 11(1), 4–17.

- Shihomeka, S. P. (2019). *Citizen engagement: Politics and digital media in Namibia* [Doctoral]. Erasmus University Rotterdam.
- Shihomeka, S. P., & Arora, P. (2018). Mobile social media and digital political inclusion among Namibia's rural youth. *Conference Proceedings at the International Communication Association*, 1–30.
- Silverio, S. A., Wilkinson, C., & Wilkinson, S. (2022). Academic ventriloquism: Tensions between inclusion, representation and anonymity in qualitative research. In *In Handbook of social inclusion: Research and practices in health and social sciences* (pp. 643–660). ham: Springer International Publishing.
- Smeenk, W., Sturm, J., & Eggen, B. (2019). A comparison of existing frameworks leading to an empathic formation compass for co-design. *International Journal of Design*, 13(3), 53–68.
- Smith, B. J., & Parvin, D. W. (1973). Defining and measuring rurality. *Southern Journal of Agricultural Economics*, July, 109–114.
- Smith, R. C., Winschiers-Theophilus, H., Kambunga, A. P., & Krishnamurthy, S. (2020). Decolonizing participatory design: Memory making in Namibia. *Proceedings of the 16th Participatory Design Conference 2020-Participation (s) Otherwise-Volume 1*, 96--106.
- Staff reporter. (2023, March 30). INFORMATION MINISTRY TO LAUNCH NATIONAL CYBERSECURITY STRATEGY AND AWARENESS PLAN. *Namibia Economist*.
- Stanley, C. (2020). *Community-based co-design of a crowdsourcing task management application for safeguarding indigenous knowledge* [Doctoral]. University of Cape Town.
- Stewart, C. A., Link, M., Simms, S., Hancock, D. Y., & Fox, G. C. (2010). *What is Cyberinfrastructure?*
- Stork, C., & Calandro, E. (2014). Internet gone mobile in Namibia. In *ICT Pathways to Poverty Reduction* (pp. 205–225). <https://doi.org/10.3362/9781780448152.009>

- Stork, C., Calandro, E., & Gillwald, A. (2013). Internet going mobile: Internet access and use in 11 African countries. *Info-The Journal of Policy, Regulation and Strategy for Telecommunications*, 15(5), 34–51. <https://doi.org/10.1108/info-05-2013-0026>
- Suero Montero, C., & Kapinga, A. F. (2019). Design science research strengthened: Integrating co-creation and co-design. *IFIP advances in information and communication technology*, 551, 486–495. https://doi.org/10.1007/978-3-030-18400-1_40
- Sultan, A. (2020). *Improving cybersecurity awareness in underserved populations* (CLTC White Paper Series). <https://cltc.berkeley.edu/2019/04/15/improving-cybersecurity-awareness-in-underserved-populations/>
- Szumski, O. (2018). Cybersecurity best practices among Polish students. *Procedia Computer Science*, 126, 1271–1280. <https://doi.org/10.1016/j.procs.2018.08.070>
- Tanner, K., Plosker, S., & Srivastava, G. (2023). A Reflection on cybersecurity indigenous educational experiences. *2023 IEEE International Conference on Big Data (BigData)*, 4819–4825. <https://doi.org/10.1109/BigData59044.2023.10386338>
- Tansey, J., & O’riordan, T. (1999). Cultural theory and risk: A review. *Health, Risk & Society*, 1(1), 71–90. <https://doi.org/10.1080/13698579908407008>
- Theofanos, M. (2020). Is usable security an oxymoron? *Computer*, 53(2), 71–74. <https://doi.org/10.1109/MC.2019.2954075>
- Vaishnavi, V. K., & Kuechler, William. J. (2007). *Design science research methods and patterns: Innovating information and communication technology*. Auerbach Publications. <https://doi.org/10.1201/9781420059335>
- van Vuuren, J. J., Grobler, M., & Zaiman, J. (2012). The influence of cyber security levels of South African citizens on national security. In *7th International Conference on Information Warfare and Security, ICIW 2012* (pp. 138–147). <http://hdl.handle.net/10204/5832>

- Venable, J., Pries-Heje, J., & Baskerville, R. (2012). A comprehensive framework for evaluation in design science research. In *Design science research in information systems. Advances in Theory and Practice* (pp. 423–438). Springer. https://doi.org/10.1007/978-3-642-29863-9_31
- Venkatesh, V., Sykes, T. A., & Zhang, X. (2020). ICT for development in rural India: A longitudinal study of women's health outcomes. *MIS Quarterly*, 44(2), 1–56.
- Villamarín-Salomón, R. M., & Brustoloni, J. C. (2010). Using reinforcement to strengthen users' secure behaviors. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 1, 363–372. <https://doi.org/10.1145/1753326.1753382>
- Wang, Y. (2017). The Third Wave?: Inclusive privacy and security. *Proceedings of the 2017 New Security Paradigms Workshop*, 13(4), 122–130. <https://doi.org/10.1145/3171533.3171538>
- West, R. (2008). The psychology of security. *Communications of the ACM*, 51(4), 34–40. <https://doi.org/10.1145/1330311.1330320>
- Wiles, R., Coffey, A., Robinson, J., & Heath, S. (2012). Anonymisation and visual images: Issues of respect, 'voice' and protection. *International Journal of Social Research Methodology*, 15(1), 41–53. <https://doi.org/10.1080/13645579.2011.564423>
- Wilkinson, C., & Wilkinson, S. (2017). Doing it write: Representation and responsibility in writing up participatory research involving young people. *Social Inclusion*, 5(3), 219–227. <https://doi.org/10.17645/si.v5i3.957>
- Winschiers-Theophilus, H., & Bidwell, N. J. (2013). Toward an Afro-Centric Indigenous HCI Paradigm. *International Journal of Human-Computer Interaction*, 29(4), 243–255. <https://doi.org/10.1080/10447318.2013.765763>
- Winschiers-Theophilus, H., Chivuno-Kuria, S., Kapuire, G. K., Bidwell, N. J., & Blake, E. (2010). Being participated: A community approach. *Proceedings of the 11th Biennial Participatory Design Conference*, 1–10. <https://doi.org/10.1145/1900441.1900443>

- Winschiers-Theophilus, H., Winschiers-Goagoses, N., Rodil, K., Blake, E., Zaman, T., Kapuire, G. K., & Kamukuenjandje, R. (2013a). Moving away from Erindi-roukambe: Transferability of a rural community-based co-design. *12th International Conference on Social Implications of Computers in Developing Countries*, 363–374.
- Winschiers-Theophilus, H., Winschiers-Goagoses, N., Rodil, K., Blake, E., Zaman, T., Kapuire, G. K., & Kamukuenjandje, R. (2013b). Moving away from Erindi-roukambe: Transferability of a rural community-based co-design. *12th International Conference on Social Implications of Computers in Developing Countries*, 363–374.
- Winschiers-Theophilus, H., Zaman, T., & Yeo, A. (2015). Reducing ‘white elephant’ ICT4D projects: A community-researcher engagement. *Proceedings of the 7th International Conference on Communities and Technologies*, 99–107. <https://doi.org/10.1145/2768545.2768554>
- Wiredu, K. (1988). Toward decolonizing African philosophy and religion. *African Studies Quarterly*, 1(4), 161–179. <http://www.africa.ufl.edu/asq/v1/4/3.pdf>
- Yin, R. K. (2016). *Qualitative research from start to finish* (2nd ed.). Guilford Press.
- Zimmermann, V., & Renaud, K. (2019). Moving from a ‘human-as-problem’ to a ‘human-as-solution’ cybersecurity mindset. *International Journal of Human-Computer Studies*, 131(May), 169–187. <https://doi.org/10.1016/j.ijhcs.2019.05.005>
- Zurko, M. E. (2005). User-centered security: Stepping up to the grand challenge. *21st Annual Computer Security Applications Conference (ACSAC’05)*, 187–202. <https://doi.org/10.1109/CSAC.2005.60>
- Zurko, M. E., & Simon, R. T. (1996). User-centered security. *Proceedings of the 1996 Workshop on New Security Paradigms*, 27–33.

APPENDICES

APPENDIX A: ETHICAL CLEARANCE



NAMIBIA UNIVERSITY
OF SCIENCE AND TECHNOLOGY

FACULTY RESEARCH ETHICS COMMITTEE (F-REC)

DECISION/FEEDBACK ON RESEARCH PROPOSAL

Dear Mr: **NHINDA, Gabriel Tuhafeni**

Research Topic: **Co-Designing a Cybersecurity Practices Framework for Underserved Rural Communities.**

Supervisor (if applicable): **Prof Fungai BHUNU SHAVA**

Qualification registered for (if applicable): **PHD IN INFORMATICS**

(Reference number of application: **FACULTY RESEARCH ETHICS COMMITTEE REGISTRATION NUMBER: 18/2021**)

Re: Ethical screening application No: **F-REC-: 18/2021**

The Faculty of **Computing and Informatics** Ethics Screening Committee of the Namibia University of Science and Technology reviewed your application for the above-mentioned research. The research as set out in the application has been:

Approved ☒ X

(indicate with an X, and N/A if not applicable and proceed)

We would like to point out that you, as researcher, are obliged to maintain the ethical integrity of your research, adhere to the ethical guidelines of NUST, and remain within the scope of your research proposal and supporting evidence as submitted to the F-REC. Should any aspect of your research change from the information as presented to the F-REC, which could have an effect on the possibility of harm to any research subject, you are under the obligation to report it immediately to your supervisor or F-REC as applicable in writing. Should there be any uncertainty in this regard, you have to consult with the F-REC.

We wish you success with your research, and trust that it will make a positive contribution to the quest for knowledge at NUST.

Any ethical issues that need to be highlighted?	Why are these issues important?	What must/could be done to minimise the ethical risk?
No	N/A	N/A

Recommendation: The application is approved: Recommendations of FCI/F-REC, communicated to you on the 19th of August 2021, were addressed to the satisfaction of the Chairperson.

Sincerely,

Prof Fungai BHUNU SHAVA

Chair: Faculty Ethics Screening Committee

Tel: +264-61-207-2510

CC: Co-supervisor: None

APPENDIX B: RESEARCH PERMISSION FROM CLUSTER HEADMAN

16

21 JUL 2021
K. S. S.
OHANGWENA
REP. OF NAMIBIA

Engela Cluster
P.O. Box 451
Ohangwena
21 July 2021

Namibia University of
Science and Technology
13 Jackson Kanyera Street
P/Bag 133388
Windhoek
Namibia

Dear Sir

Re: Seeking Permission to collect
data on cybersecurity practices
from the residents of the Engela
Orukalo, Omaturu, Orukalo
and Oshana villages
through focus groups and
interviews.

I acknowledged receipt of
your letter through my mobile
App device dated 17 July 2021
which refers.

I read through your attached
letter on which you have
detailed your aims and objectives
of your study and where
A.T.O

Extra Collection is required
I have discussed your request
with my Junior Traditional
Council on my Cluster where
by we have agreed to grant
you permission to conduct
the interviews with the
residents of in the village
as requested

You can conduct the follow-
ing people to make all neces-
sary arrangements in their
respective villages

1. Enyela Hengrina Hitula
0812524110 / 0812418464
2. Onghala - Onafund Onghala
0811497677
3. Ouhonga - Jitiel Ndeiluka
0812368825

If you need further information Please
Contact me.



Kind Regards

Popycinawa
Cluster Chairman

APPENDIX C: PERMISSION FROM CONSTITUENCY COUNCILLOR



OHANGWENA REGIONAL COUNCIL ENGELA CONSTITUENCY

TEL: 065 269 010
FAX: 060 269 007

P.O.BOX 791
Ohangwena

04 August 2021

KU: MWENE WOMUKUNDA, NOVAKWASHIWANA

Ombapilla ei otai kwashilipaleke kutya Gabriel Tuhafeni Nhinda omulihongi koshiputudilo sha **NUST (NamibiaUniversity of Science and Technology)** ota ningi omapekaapeko e na sha nelihongo laye moshikandjohoololo Engela.

Omapekaapeko atya ngaha otaa tameke mu August 2021 fiyo omu December 2022.

Omapekaapeko aa oku li pambelewa onghee ohandi ku indile nefimaneko opo u mu yakule ove u mu tambule ko nombili.

Tangi kelongelokumwe.


Elkan Hainghumbi (MP)
Regional Councillor
Engela Constituency
Cell 0811412295



APPENDIX D.1: EXTRACT FROM JOURNAL PAPER I

Journal of Information & Optimization Sciences

ISSN 0252-2667 (Print), ISSN 2169-0103 (Online)

Vol. 44 (2023), No. 3, pp. 475–492

DOI : 10.47974/JIOS-1407

Co-CEP: A co-designed community engagement protocol as a catalyst for cybersecurity research in Africa: The case of northern Namibia

Gabriel Tuhafeni Nhinda *

Fungai Bhunu Shava †

Namibia University of Science and Technology

Faculty of Computing and Informatics

13 Jackson Kaujeua Street

Windhoek

Namibia

Abstract

Through technology, the world has become a global village, connecting geographically distant people into virtual neighbors. This presents many opportunities for individuals, businesses, and remote communities. The advantages of this connectivity have been brought to the fore by COVID-19, as technology and the Internet kept the world connected and functioning. However, in Africa, although much has been done on connecting the unconnected, there remains rural underserved communities. Notwithstanding the benefits of technology and the Internet, the cyber-safety and cybersecurity of those communities living on the fringes of society – rural underserved communities – is unknown. Consequently, many researchers, noting the benefits of technology, have embarked on ICT for Development projects (ICT4D). However, community based ICT4D projects have been failing due to myriad of factors. Some such factors are engagement misalignment, cultural faux pas, communication, power dynamics and community-buy-in of end-products. With the propensity to circumvent the shortcomings indicated above, Participatory Design (PD) processes may be utilized. Co-design extends PD by allowing researchers and participants to be equals in the creation of solutions to problems contrary to traditional research approaches, that abstract researchers from the community within which they work. As an effort to address these challenges, we present a co-designed community engagement protocol (co-CEP) for rural underserved communities in Northern (Oukwanyama), Namibia. This study was qualitative, guided by Ubuntu and Uushiindaism tenets of trust, neighbourliness, respect, familiarity, hospitality, and collective unity as pillars of fostering communication within 4 villages in Oukwanyama,

This research was conducted during the COVID-19 Pandemic and it was sponsored by a grant from the Mobile Telecommunications Company (MTC) Namibia.

* E-mail: gnhinda@nust.na (Corresponding Author)

† E-mail: fbshava@nust.na

APPENDIX D.2: EXTRACT FROM CONFERENCE PAPER II

Cybersecurity practices of rural underserved communities in Africa: A case study from Northern Namibia

Gabriel Tuhafeni Nhinda
Faculty of Computing and Informatics
Namibia University of Science and Technology
Windhoek, Namibia
gnhinda@must.na

Fungai Bhumu Shava
Faculty of Computing and Informatics
Namibia University of Science and Technology
Windhoek, Namibia
fbshava@must.na

Abstract— Globally, Information Communication Technology (ICT) device usage has seen a steep rise over the last few years. This also holds in developing countries, which have embarked on connecting the unconnected or previously disadvantaged parts of their populations. This connectivity enables people to interact with cyberspace, which brings opportunities and challenges. Opportunities such as the ability to conduct business online, attend online education, and perform online banking activities. Challenges experienced are the cost of Internet access and more worrying cyber-risks and potential for exploitation. There remain pockets of communities that experience sporadic connectivity to cyberspace, these communities tend to be more susceptible to cyber-attacks due to issues of lack/limited awareness of cyber secure practices, an existent culture that might be exploited by cybercriminals, and overall, a lackluster approach to their cyber-hygiene. We present a qualitative study conducted in rural Northern Namibia. Our findings indicate that both secure and insecure cybersecurity practices exist. However, through the Ubuntu and Uushiindaism Afrocentric lenses, practices such as sharing mobile devices without passwords among the community mirror community unity. Practices such as this in mainstream research can be considered insecure. We also propose interrogating “common” secure cybersecurity practices in their universality of applicability.

Keywords— cybersecurity practices, Social Cybersecurity, rural underserved communities, Ubuntu, Uushiindaism

I. INTRODUCTION

Information communication technology device usage has seen a steep rise over the last few years. Developing countries are not exempt from this development, where many new Internet users are coming online through mobile Internet-enabled devices. Internet penetration in Africa has been on the increase, the International Telecommunications Union (ITU) reports that between 2019 and 2021 there has been a 23% increase in the number of Internet users [1]. The ITU adds that globally urban residents are twice as likely to use the Internet compared to rural residents. In Africa this connectivity divide is greater, where urban residents are four times (47%) more likely to use the Internet compared to the 13% of rural residents [1]. Internet access is enabled by the availability of broadband access and technological devices with such capabilities. Broadband access in Africa in rural areas as of 2021 still stood at 18% [1]. Technology device ownership and use have outpaced the diffusion of Internet development in many rural African countries [2]. It is projected that by 2025 mobile device ownership will be highest in rural areas with the youth contingent being the highest adopters [3].

ICT device ownership comes with many advantages, such as the ability to communicate with geographically distant relatives; the ability to attend online classes; potential for conducting business online; among many benefits. However, there are also challenges to the ownership of ICT devices, access to electricity to charge these devices, access to broadband to enable Internet access, and the cost of Internet access [4]. Most prevalent is that many in sub-Saharan Africa are mobile-first Internet users and may not be familiar with issues of cyber-hygiene and personal cybersecurity [5]. Mokobane and Both [6] argue that within this region Ubuntu principles that govern interaction may influence social engineering susceptibility. They add that some nefarious characters may abuse various tenets like trust and hospitality to gain the confidence of unsuspecting new Internet users with this ethos. Similarly, there remains scant Internet access especially within rural areas of developing countries [1], to this, many governments have embarked on connecting the unconnected or previously disadvantaged parts of their populations [7]. Therefore, this paper aims to understand current cybersecurity practices within rural communities (villages) in northern Namibia.

A. Case site

The national population of Namibia according to [8] was at 2.1 million in 2014. However, the gini-coefficient which aims to look at economic inequality was recorded at 59.1% in 2015, indicating an uneven society. To get a better understanding of the cybersecurity practices of the inhabitants of rural underserved communities (villages), we conducted a qualitative study within 4 villages in northern Namibia. The choice of these four villages was conveniently chosen to avoid potential issues of language barriers and lost in translation issues as experienced by some community co-design researchers in Namibia [9]. Additionally, we follow the guidance of Mkabela [10] who advises that “researcher must have some familiarity with history, language, philosophy, and myths of the people under study”. In our study, one of the researchers is familiar with people under study. The 4 villages are in Northern Namibia, where villages comprise of multiple Omahangu (pearl millet) fields with homesteads in the centre. These homesteads are constructed in a circular fashion with a boundary made from wooden palisades, the homesteads are comprised of rooms are of the rondavel type connected by intricate passages [11, p. 43]. Each homestead is occupied by one family. Namibia is categorized as a middle-high-income nation. According to the latest population census of reported in 2014, our study location has a population of 24 271 [12]. The 4 villages we conducted our study are reported to have a

979-8-3503-1480-9/23/\$31.00 ©2023 IEEE

APPENDIX D.3: EXTRACT FROM CONFERENCE EXTENDED ABSTRACT III

Using Co-Design to craft Cybersecurity secure practices for rural communities in Africa: A case study from Northern Namibia

Gabriel Tuhafeni Nhinda and Fungai Bhunu Shava

Faculty of Computing and Informatics, Namibia University of Science and Technology

Extended Abstract

With the advent of the COVID-19 pandemic, many services moved onto the internet forcing more people to become first-time internet users, especially on the African continent. This new uptake onto the internet was made possible through mobile computing devices like smartphones. However, the internet is laden with many opportunities and cyber threats. In this abstract, we present our ongoing research utilising co-design to create a cybersecurity secure practices framework for rural and underserved communities in Africa. Co-designing has been used in various areas of research, from Marketing research to Land use planning and human-computer interaction studies. Having roots in participatory methods, which aim to remove the knowledge diffusion from the researcher to a more *equal* participation between participants and researchers. Another noted advantage of co-design is the reported level of ownership of artifacts (Nhinda & Bhunu Shava, 2021), therefore, for our research, we hope that the best practices framework to be co-designed would be embodied by African communities. Cybersecurity research often focuses on technical solutions within organizations and tends to neglect the human factor, when referred to, it is castigated and denoted as the weakest link in any Cybersecurity program. In addition, most studies in cybersecurity practices emanate within Western organizations and countries that have a different ethos and philosophy. We ascribe to what (Zimmermann & Renaud, 2019) referred to as cybersecurity differently, wherein the human is considered as part of the solution in cybersecurity. In our given context, we focus on communities in underserved rural African settings where culture plays a major role in how community members behave (Nhinda & Bhunu Shava, 2021). We rely on Ubuntu and Uushiindaism (Mbenzi & Ashikuti, 2018) as lenses to understand the decisions community

APPENDIX D.4: EXTRACT FROM CONFERENCE PAPER IV

Towards the use of Participatory Methods in Cybersecurity research in rural Africa: A grassroots Approach

Gabriel Tuhafeni Nhinda
Faculty of Computing and Informatics
Namibia University of Science and Technology
Windhoek, Namibia
gnhinda@hotmail.com

Fungai Bhunu Shava
Faculty of Computing and Informatics
Namibia University of Science and Technology
Windhoek, Namibia
fbshava@nust.na

Abstract— As a research domain, Cybersecurity has been around for a long time. However, research methods and outputs have been deeply rooted in western epistemologies, thus leaving pockets of communities in rural Africa at possible risk. Even though some research on the African continent aims to address cybersecurity awareness, they still utilize a top-down approach, with interventions designed and developed for rural end users often without their input. This position paper proposes a new research focus in cybersecurity research within rural communities in Africa and for cybersecurity research in rural African communities. Participatory methods have been utilized in human-computer interactions research with greater impact of end-product adoptability, sense of ownership of communities involved and overall design implications for design research as a whole. We therefore argue that for cybersecurity research to have sustainable effects for these communities on the fringes of society, a participatory design approach needs to be considered in cybersecurity research.

Keywords—Participatory Design, cybersecurity, Ubuntu, Uushindiism

I. INTRODUCTION

Cybersecurity research has often focused on technological solutions to tackle persistent threats. However, cybersecurity is a socio-technical issue that is made up of multiple interconnected components, including processes, technology, and human factors. Researchers have agreed that the human-factor is cybersecurity is the weakest link [1]. Human-factors research has mostly focused in organizations and how compliant people are to security policies. However, there has been little research done in rural communities. Notwithstanding, rural communities in Africa and their access, and cybersecurity practices. Often the term rural is defined by open country land. Literature often describes the term with what is lacking in the area as socio-economically underdeveloped, low population densities, illiterate, limited English language proficiency, and limited familiarity with technology practices [2]. However, it is important to note that these are often western-centric characterizations as rural communities might possess different literacies, i.e. not written but oral literacy. There is no heterogeneous definition of what rurality looks like on the African continent, but characterizations of the distance from urban centres/cities are utilized. Although neglected in cybersecurity research, technology has become a critical part of rural African daily lives with mobile and pervasive technologies such as mobile devices enabled with various actuators and sensors, web 2.0,

Internet technology, and Internet of Things (IoT) devices being used as part of daily life [3]. These technologies enable users to perform tasks from the comfort of their homes. Internet technology has opened up new opportunities as well as new challenges for individuals. One such opportunity being the ability to connect and transact online from nearly anywhere. Albeit all the opportunities, challenges such as the availability of digital literacy, mobile broadband, cost of internet-enabled devices, and cost of mobile data persist in developing countries [4]. Among other challenges, the most alarming is the online safety of technology users creating a new divide, between those who can mitigate and manage cybersecurity risks and those that cannot.

The proliferation and increasing affordability of technological devices has permeated the existing digital divide in more ways than ever before. Previously marginalized communities in rural communities have gained access to digital devices such as mobile phones, tablets and smartphones.

Even though nation-states have invested in cyber defences and offense capabilities, minimal efforts have been directed at the rural communities. In recent years, there has been a number of attempts to understand technology usage patterns and additionally educate rural communities of how to secure themselves online [5]. This populace is disproportionately vulnerable to cyber-crime and may not even know when they have become victims [5]. From a technical perspective, there exist a plethora of interventions that aim to mitigate, prevent, and circumvent any attacks that an individual might experience online. These interventions however often fall short as they aim at targeting users' change in behaviour [6] and are not modelled with and for users' ways of being. Human-Computer Interaction studies have proven that involving users at the end of technological interventions does not yield the adoptability [7] nor encourage the confidence of product/technology use [8]. Participatory Design (PD) has gained popularity as an alternative approach in HCI community based studies in Africa [9]. PD emphasizes including technology/product end-users at the beginning of a project. This can include having end-users or people for whom a project aims to benefit as equal partners. has improved these through the involvement of end-users in technology design as alluded by [2]. [10] argues that despite security training, there remains a pocket of users that often find it difficult to understand technical security mechanisms within organisations [11]. The users thereby continue failing to

APPENDIX E: COMMUNITY MEMBERS INFORMED CONSENT FORM

Part II: Certificate of Consent

I have been invited to participate in this research project titled: “Co-Designing a Cybersecurity Practices Framework for Underserved Rural Communities”. The research project aims to collaboratively identify secure cybersecurity practices within rural communities. It will further look to understand our community practices as it relates to security and risk perceptions. Additionally, the research project will also look at how our community uses technological devices.

I have read the foregoing information, or it has been read to me. I have had the opportunity to ask questions about it and any questions I have asked have, have been answered to my satisfaction. I consent voluntarily to be a participant in this study

Print Name of Participant

Signature of Participant

Date

Day/month/year

*If illiterate*⁸

I have witnessed the accurate reading of the consent form to the potential participant, and the individual has had the opportunity to ask questions. I confirm that the individual has given consent freely.

Print name of witness

Signature of witness

Date

Thumbprint of participant

⁸ A literate witness must sign (if possible, this person should be selected by the participant and should have no connection to the research team). Illiterate participants should include their thumbprint as well.

Day/month/year

Statement by the researcher/person taking consent

I have accurately read out the information sheet to the potential participant, and to the best of my ability made sure that the participant understands that the following will be done:

- 1. Interviews**
- 2. Focus group discussions**

I confirm that the participant was given an opportunity to ask questions about the study, and all the questions asked by the participant have been answered correctly and to the best of my ability. I confirm that the individual has not been coerced into giving consent, and the consent has been given freely and voluntarily.

A copy of this ICF has been provided to the participant.

Print Name of Researcher/person taking the consent GABRIEL TUHAFENI NHINDA

Signature of Researcher /person taking the consent _____

Date _____

Day/month/year

APPENDIX F: CO-DESIGN WORKSHOP DATA COLLECTION INSTRUMENT

Co-design session questions for community members in rural underserved communities.

1. What types of computing devices do you own?
2. What do you use these devices for?
3. As a community, when you struggle with using your phone, whom do you contact to help you?
4. Tell me about a time when you experienced an incident when someone pretended to be someone they are not to try and fool you into giving them money for instance.
5. In your community, how do you identify danger?
6. As a community, how would you react if your neighbour was to fall victim to a robbery? Why would you react in that manner?
7. Have you ever seen messages on how to protect yourself online?
8. Have you ever attended training/been educated on how to protect yourself in cyberspace?
9. When new information is given especially about technology, does it matter whom that information is coming from? How would you want that information to be shared with you?
10. What do you think is the best way for you to receive this information in order for you to remember it?
11. If you do not know how to protect yourself online, how would you like this to be done if you had that responsibility?
12. Have you ever suspected that your data or airtime was stolen from your phone? What made you suspicious? What did you do differently from then on?
13. Have you heard of any situations where someone close to you or yourself was corned out of money by someone you did not know?
14. In this community, if someone does something wrong, how are they corrected?
15. If you were to fall victim to an online scam, would you tell your community members? Why if yes? Why if no?
16. If you were to train other people on how to protect themselves online, how would you go about doing it?
17. Who do you think should be responsible for training people on internet safety?

APPENDIX G: INTERVIEW GUIDE COMMUNITY MEMBERS

Below are the questions that guided the interviews in the communities

Biographical Information

1. Would you prefer to have this interview in English or Oshiwambo?
2. Age
3. Sex
4. Highest level of education
5. Occupation⁹

Current security practices of underserved rural communities.

1. If a stranger comes to your house asking for assistance, how would you treat that person?
Please walk me through that decision?
2. If someone you do not know sends you a message on your device asking for assistance, what would you do?
 - a. If you would/would not respond to them, why?
 - b. What would make you want to help that person?
3. I understand that there is a saying “Omushiinda oye ekipa lofingo” [your neighbour is your backbone], do you generally trust your neighbours? Why? What makes them trustworthy to you?
4. Have you ever received a message from a contact you trust about a company giving away some gifts to customers? What did you do in that instance? Why did you/not click on that link? What was your experience? Would you do it again? Why?
5. Have you heard of the term cybersecurity? If yes, where did you hear it from? Did you understand what they were talking about?
6. What about cyber hygiene?

⁹ This information will allow us to ascertain the most vulnerable sex, and age groups (End-users are the weakest link within any cybersecurity programme.)

7. Have you ever suspected that your data or airtime was stolen from your phone? What made you suspicious? What did you do differently from then on?
8. Have you heard of any situations where someone close to you or yourself was corned out of money by someone? Did you know that person?
9. If your device was to be lost or stolen, would someone be able to use it? Yes/No. If No, why not?

Possible risks that exist in current technology use of underserved rural communities.

1. Do you have any computing devices? Yes/No
2. What type of device is it, feature phone or smartphone or tablet or laptop? May I see it?
 - a. cellphones,
 - b. tablets,
 - c. computers,
 - d. laptops?
 - e. others _____
3. What do you use your device for?
4. Are you the only person that uses your device(s)? Yes/ No
 - a. If no, who else uses your device(s)
 - i. Do you know what they use the device for? If yes, please tell me.
 - ii. Do you have any security settings on your device(s)? Please share on which about them.
 - iii. Do you share those Security settings with the other person(s) that use your device(s)?
 - iv. Are you aware of that person has shared your security settings with others without your permission?
 - b. On your phone, have you registered it for any financial transactions like cellphone banking, banking apps? Yes/No
 - i. If Yes, Are these protected?
 - ii. How are they protected?
5. Does your device have any security features on it? Name them

- a. If yes, How did you come up with that security choice for your device (code/ pattern/passwords/ biometrics)?
 - b. If no, Why do you not have any security enabled (code/password/pattern/biometrics) on your device?
6. How do you charge the battery of your device?
7. Did you ever sell a computing device to another person? What did you do to it before selling it?
8. Have you heard of online cloud storage services? Have you used them?
9. On your device, do you install applications?
 - a. If yes, do you read the terms and conditions of those applications including the permissions before installing? If no, why not?
10. Do you have any information on your device that you would not want others to see?
Yes/No
 - a. If yes, how do you protect it? [RO1]
11. If you were to train other people on how to protect themselves online, how would you go about doing it?¹⁰[RO3]

Online security best practices for underserved rural communities.

1. Do(es) your computing device(s) have Internet access?
 - a. If yes, do you use the Internet on your device? Yes/No
 - b. How often do you use the Internet?
 - i. Over 5 hours per day
 - ii. About 3 hours a day
 - iii. About 1 hour a day
 - iv. Less than 1 hour per day
 - v. About 5 times a week
 - vi. About 3 times a week
 - vii. Once a week

¹⁰ This will enable us to record the preferred mode of delivery of cybersecurity awareness training.

- viii. Maybe twice a month
 - ix. Once a month
 - x. Never
 - xi. Other? Specify
- c. What do you use the Internet for? (Cue: WhatsApp, Facebook, school, business, email, etc.)
- d. When you are online, what type of information do you share?
- 2. Do you know some advantages of the Internet? Name them
- 3. Are you aware of any disadvantages of the Internet? Name them
- 4. On Internet use, when you are online, have you seen adverts that have asked you to click on links for prizes, etc.?
- a. If yes, what did you do? Why did you do that?
 - b. If no, why did you not do it?¹¹
- 5. Do you use any security measures for the online services (social media sites, e-mails, etc.) that you use (etc. Passwords, Biometrics), etc.? Have you used those passwords elsewhere before? If yes, why? If no, why not?¹²
- 6. For the services you access online, do you log into them? Do you always log out of them when you are done using them? If yes, why? If no, why?
- 7. Do you use the internet only on your devices? If no, whose devices do you also use? Do you always log out of those devices after you are done using them?
- 8. If you are stuck with how to use your device(s), who would you ask for help? Why?
- 9. Have you ever used a public Wi-Fi network?

Thank you for your time, this is the end of our interview, do you have any questions for me?

¹¹ Gauges security knowledge

¹² Users sometimes select weak passwords and tend to use them across services and share them with trusted others.

APPENDIX H: INTERVIEW GUIDE MINISTRY

The Interviews with the participants from the Ministry utilised the below interview guide

1. Being the ICT custodian in the nation, do you provide ICT services to users in rural areas?
 - a. Are your services accessible in all rural areas? If no, which ones are not covered? Why? Any plans to service them?
 - b. Are your services secure? How?
2. Have you had incidents reported about cybercriminals from rural areas?
3. If yes, what are the different types of attacks that you mostly are informed of by residents of rural areas?
4. Presently, is there any legislation that provides legal recourse for citizens should they fall victim to cybercriminals?
 - a. If yes, which law(s) are these?
 - i. Are these laws actively being utilised by citizen for legal recourse?
 - ii. How do you educate the citizens on the legislation?
 - b. If no, why not?
 - i. Are there any plans by the ministry to propose such legislation?
5. Have you embarked on any cyber awareness campaigns of any form for the entire country? Any targeting rural communities?
 - a. If yes, have you seen any results from them?
 - i. How do you conduct these awareness campaigns regularly?
 - b. If no, why not?
 - i. Do you have any plans of creating such awareness campaigns?
6. During the security awareness campaigns, are citizens able to engage your staff running the campaigns? Do these come at a cost to the customer?
7. What are the most at-risk populations from your experience of cybercrimes within rural communities?
8. Have you received any reports of cyberattacks from your clients that reside in rural areas?
 - a. What are the frequent types of cyberattacks reported?
 - b. What are some unexpected types of cyberattacks that are devastating as reported by your clients?
9. Are these campaigns that you run available in various native languages?
10. Would you be willing to share some of the materials you use in these campaigns with me?
11. If you were to be trained by other people on how to protect yourself online, how would you want them to go about doing it?

Thank you for your time, this is the end of our interview, do you have any questions for me?

APPENDIX I: MINISTRY INFORMED CONSENT FORM

Part II: Certificate of Consent

I have been invited to participate in this research project titled: “Co-Designing a Cybersecurity Practices Framework for Underserved Rural Communities”. The research project aims to collaboratively identify secure cybersecurity practices within rural communities. It will further look to understand community practices as it relates to security and risk perceptions. Additionally, the research project will also look at how our community uses technological devices.

I have read the foregoing information, or it has been read to me. I have had the opportunity to ask questions about it and any questions I have asked have, have been answered to my satisfaction. I consent voluntarily to be a participant in this study

Print Name of Participant _____

Signature of Participant _____

Date _____

Day/month/year

Statement by the researcher/person taking consent

I have accurately read out the information sheet to the potential participant, and to the best of my ability made sure that the participant understands that the following will be done:

1. Interviews

I confirm that the participant was given an opportunity to ask questions about the study, and all the questions asked by the participant have been answered correctly and to the best of my ability. I confirm that the individual has not been coerced into giving consent, and the consent has been given freely and voluntarily.

A copy of this ICF has been provided to the participant.

Print Name of Researcher/person taking the consent GABRIEL TUHAFENI NHINDA

Signature of Researcher /person taking the consent _____

Date _____

Day/month/year

APPENDIX J: FOCUS GROUP OF EXPERTS EVALUATION TOOL

This section aims to evaluate the proposed framework on how it best solves the identified problem within this study. Artefacts developed using the Design Science Research methodology should make sure that they are contextually relevant. That the appraisal of those artefacts takes contextual factors into consideration, like, the fidelity with the realities of rural life. One of the key points that co-design aims to address is sustainability of developed artefacts within communities, especially in the technology space. Therefore, another criterion for validation is the sustainability of the developed artefact. The framework and its components are presented through a pre-evaluation phase.

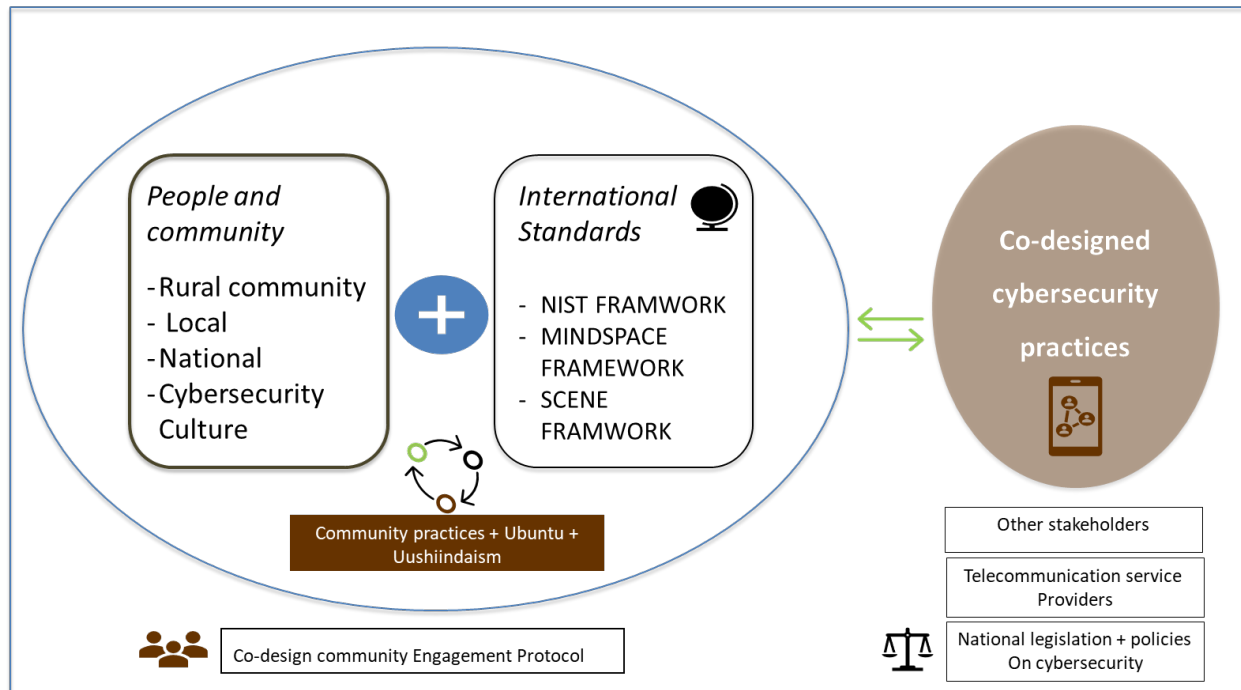


Figure 1: Co-designed cybersecurity practices framework for rural underserved communities

The framework has the following objectives

- 6) To enable community members to resonate with the co-designed secure practices.
- 7) To empower community members to confidently apply the co-designed secure practices in their everyday technology use.

- 8) To reduce the potential susceptibility of community members to both online and technology-mediated attacks.
- 9) To iteratively create a living framework that evolves as the needs change.
- 10) To illuminate the relationship between the different framework components.

This evaluation aims to look at the following aspects:

The evaluation of the framework was conducted to identify the following

- Ecological utility
- Completeness
- Effectiveness

The evaluands are asked the following questions for discussion in order to assist the researcher in refining the framework to firstly, meet community needs for cybersecurity practices, and also the design objectives of this study:

- 1) Based on the framework provided, what do you think it communicates?
- 2) What works well in the framework?
- 3) Based on your experience, what components do you think are missing from the framework?
- 4) What improvements can be made to the framework?
- 5) In which ways do you believe the framework will meet the reality of underserved rural communities?
- 6) Are there additional questions that you need clarification on?

Do you have any other comments:

APPENDIX K: EDITORS LETTER

Dr Theresia Mushaandja BED Sec; BA Hons in English Studies; M.A. in English Studies; Editing and Proof reading certificate (UCT), PHD in English Studies; Senior Lecturer, English (NUST)
JOTERSS English Language and Research Private Academy (Chief Editor)
P. O Box 487, Windhoek Tel: 0816408864 Email: joterss2014@gmail.com

27 February 2025

To: Whom it may concern

Re: Editor's report

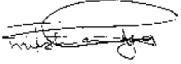
This letter serves as an attestation that I, Dr Theresia Mushaandja, from the language and research academy, cited above, carried out the language editing of the research report by Dr **Gabriel Tuhafeni Nhinda**, student number **200742175**. The research is titled **CO-DESIGNING A CYBERSECURITY PRACTICES FRAMEWORK FOR UNDERSERVED RURAL COMMUNITIES**.

The following linguistic components and features were focused on concord, which is the agreement between subjects and verbs. Sentence construction: at times, one finds that some sentences may need rephrasing to make sense or may need to be shortened or completed for the same effect. Consistency in the use of words, tenses, and forms of language. Another area that I focused on is the use of punctuation, especially the omissions and or the overuse. I also suggested changes where words with the same meaning were used but did not express the idea fully in the context they were used.

As I edit, I set the computer English Language to UK and not to USA. I also made use of track changes, so that the student, and if need be, the supervisor, will be able to track the changes I suggested, to accept or decline them as may be found appropriate.

For additional questions and clarity, do not hesitate to contact me at 08164 088 64 or e-mail me at joterss2014@gmail.com

Sincerely yours,



T. Mushaandja (Language Editor)