[UCI]I804:42014-200000335541

학 석사 학위논문

A Study on National Cybersecurity Strategies

Feature Analysis for Future Cybersecurity Strategy Development

테렌스 네마 이레 (Terrence Nemayire)

Department of International Studies

Legal Informatics and Forensic Science

한림대학교 대학원
(Graduate School, Hallym University)

A Study on National Cybersecurity Strategies

Feature Analysis for Future Cybersecurity Strategy Development

테렌스 네마 이레 (Terrence Nemayire)

Department of International Studies

Legal Informatics and Forensic Science

한림대학교 대학원
(Graduate School, Hallym University)

교수지도

학 석사 학위논문

의 석사 학위논문을 합격으로 판정함

2020 년 07 월 07 일

심사위원장 박노섭

____

심사위원 장윤식

____

심사위원 Joshua I. James

____

Table of Contents

Index of Tables

Index of Figures

List of Abbreviations

List of acronyms and abbreviations

ICT	Information communication technology
AU	African Union
CERT/ CIRT	Computer Emergency/Incidents Response Teams
COBIT	Control Objectives for Information and Related Technologies
ITU	International Telecommunications Union
ITIL	Information Technology Infrastructure Library
ATU	African Telecommunications Union
KISA	Korean Internet Security Agency
SADC	Southern African Development Commission
POTRAZ	Postal Telecommunication Regulatory Authority of

	Zimbabwe
ENISA	European Union Agency for Cybersecurity
EU	European Union
APT	Advanced Persistent Threat
NIST	National Institute of Standards and Technology
NCSS	National Cybersecurity Strategy

CHAPTER 1: INTRODUCTION

1.1 Background

The increasing dependence on digital technology, the interconnectivity of the different sectors of life, ease of access to cyber threat tools and, the rising instability in the global political and international relations arena have sparked a new dimension in the security domain (Akerele & Levanon, 2018). President Donald Trump, in 2018, acknowledged that modern warfare is now being fought in the virtual world and is being approached by some nations in a more reckless approach than in conventional physical domains. The asymmetric growth of cyberspace threats has affected countries differently, hence stimulating the growth of cybersecurity strategies that seem dissimilar but focused on the same threat landscape. Kademi (2014) admits that national cybersecurity strategies (NCSS) in developed countries are fast maturing, while developing countries are struggling to design or implement their first strategic plans in cybersecurity.

This widening gap in national cybersecurity strategy (NCSS) development is a possible result of the divergence of what is involved in cybersecurity, which is a global phenomenon that has no national boundaries or political jurisdictions (Le Sage, 2010). ITU (2007) and James (2018) highlighted that one of the significant constraints to the development of comprehensive NCSS is the divergent perceptions of the significance of cybersecurity threats to the broader national security agenda as reflected by differences in periods at which different countries have developed and adopted such strategies. For instance in Africa, the first NCSS framework was developed and implemented in 2015 by the South African Government, yet the cyber threat domain had already evolved

In comparison, other countries such as the United States of America first appreciated the relevance of threats from the Internet as early as 1986. They announced their first NCSS in 2003, which shows the wide perception gap between developed and developing countries (van Nierkerk, 2017). Furthermore, there has been less discussion on theoretical foundations of cybersecurity bringing to fore weak academic attention to NCSS beside the development of technical issues such as ICT security models to protect computer and information systems, yet without raising such similar efforts at the strategic level, and allowing for the further interactions and research between academia and cybersecurity experts (Atoum & Otoom, 2017).

Only recently, in 2007, the International Telecommunications Union (ITU) took it upon itself to bring awareness and to take the lead in the initiative across the globe for the development and implementation of NCSS through the Global Cybersecurity Agenda (GCA) (ITU, 2007). Between the current practices and the GCA development in 2007, various nations have attempted to develop their NCSS with multiple degrees of success or little success. The challenges stimulated ITU again to propose a toolkit for use by countries to establish comprehensive NCSS (Andrea, 2017).

However, what seems to trend across these NCSS is that society is more dependent on ICTs than never before and continues to increase as the day goes by. Unfortunately, Akerele & Levanon (2018) observed that the emergence of the greater relevance of ICTs across sectors of life brought both blessings and curses. Critical infrastructure (CI) such as health, financial and, even utility systems are connected to the Intenet as a way of either increasing productivity and efficiency or increasing the ease for client and effectiveness. However, cybersecurity threats have also increased in intensity, complexity, frequency, and variety, hence threatening the sustainability of the critical infrastructure. Andrea (2017) and Adomako, Mohamed, Garba, & Saint (2018).

In the modern-day, information is proving to be a source of power, driven by the rapid and dynamic advancement in ICT globally. It has given rise to a virtual yet complex and volatile environment dubbed 'Cyberspace.' At the national, organizational, and individual levels, cyber-related conflicts have emerged. Developing countries in Africa have been affected by this global cyberspace battlefield. For instance, POTRAZ, the ICT regulatory authority of Zimbabwe in its 3rd quarter sectoral performance report highlighted some of the following key trends (Potraz, 2019);

· Active mobile subscriptions grew by 4% from 12.4 million to 12.9 million; hence the mobile penetration rate increased by 3.4% from 84.8% to 88.2%;

· Marked 8% increase in national mobile voice traffic from 1.3 billion minutes to 1.4 billion minutes and internet penetration rate increased by 1.7% from 57.2% to 58.9%.

Irrespective of these statistics showing a positive trajectory, generally, these African developing countries have not done so much concerning cybersecurity and at the rate at which cybercriminals are finding it easy to attack the cyberspace. TechZim, an ICT online publication, highlighted that in 2019, Zimbabwe lost over USD$40 million dollars to cybercrime, with as little as USD$1.5 million recovered as reported by the Zimbabwe Republic Police (Cyber Crime Unit). Subsequently, in the same year, as published by the South African Banking Risk Information Centre (SABRIC), it was estimated that South Africa lost over USD$157 million, Nigeria lost over USD$649 million, Kenya lost over $210 million to cybercrimes.

Recently nations have been gripped by a wave of cyberattacks that are more targeted, resourced, and sophisticated. In general, the challenges have proven to be more complex and difficult to eradicate or minimize since most of these attacks fall into the category of Advanced Persistent Threats (APT). These have necessitated nations to embrace and employ/remodel tactical approaches to curb these security threats (APT). Globally the ITU has been doing various initiatives to improve awareness, support UN member states to design fully, adopt its Global Cybersecurity Agenda drive. Despite these initiatives, a large number of African countries have not yet done so, leading researchers, academia, experts, and policymakers to start on various fact-finding missions as to the challenges these countries face and recommend solutions.

Countries that have developed and implemented NCSS, there are wide discrepancies in the application and comprehensiveness of these strategies. While some countries have included offensive and defensive concepts in their strategies, for example, the USA and China, have mainly focused on the defensive concepts in response to global threats (Kademi, 2014). Furthermore, there is divergence concerning how the NCSS relates to other contemporary strategies such as economic development and security, human and civil rights, and even to the broader national defence security strategies. As defined in the NIST framework, nations need to develop cybersecurity standards and best practices that address issues around interoperability, usability, and privacy to enable more significant development and application of practical, innovative security technologies.

Despite the fact that global efforts have been made to standardize, control, regulate, and enhance the security of information and telecommunication infrastructure, thus transforming from tactical to strategic, from Institutional to Governmental and from an Individualistic to a more collective (multistakeholder) approach oriented more still needs to be done especially for developing nations. Hence to arrive at a significant comprehensive solution, national cybersecurity strategy has to be established as a high-level priority mission. As of the current state of many strategies, the main goals of cybersecurity are to protect critical infrastructures, enhance the economic well-being and national security of its citizens. With these in mind, it turns out that the ultimate objective in achieving this is centred on mitigating cyber risks and threats. Unfortunately, most, if not all, strategies lack a concrete mechanism to address cyberspace as a globally virtual space, interconnected, rather more confined within a state's interest, goals, and objectives.

To set up or to elaborate a National Cyber Security Strategy (NCSS), the policymakers need to pay attention to the balance between openness (freedom) and security, defensive and offensive operations, system modernization and critical infrastructure protection, perceptions and definitions to crucial elements of a nation such a culture, beliefs, ethos and values. Since the issue of cybersecurity might not be peculiar to any particular country, there are core pillars that exist or have shared values between many nations. With strategic problems arising from politically motivated cyber incidents and the ubiquity and sophistication in the threat vector, it is apparent that no single country or international organization would come up with an all and sundry solution.

An approach that combines expertise, resources, and capabilities of national governance, international organizations, and local communities is needed. As the trends show, adversaries have had more enabling capabilities to carry out attacks, which is aided by anonymity, rules, and regulations that end at state borders and high infrastructure connectivity with insufficient securities. These pave the way for a continuous discovery of more unknown vulnerabilities, undetected intrusions, and breaches, as evident by the various global attacks described in the second chapter of this research work. The future that we all seek is that in which vulnerabilities reduced, confidentiality enhanced, the impact of attack reduced and responded promptly.

With this in mind, developing nations still lack in various aspects on managing, handling and responding to most current cyberattacks, hence the motivation for this research study, to explore the African cybersecurity environment and proffer solutions that can be adopted to improve the situation.

1.2 Statement of the problem

Cybersecurity attacks in Africa are considered one of the critical bottlenecks to the continent's economic development resulting in substantial financial losses of over one billion United States (US) dollars in cybercrimes (Adomako, Mohamed, Garba, & Saint, 2018). According to ITU's (2019), Global Cybersecurity Index report, there has been a slight increase in appreciation of the impact of cybersecurity attacks and crimes in Africa. However, the pace of adoption and establishment of the necessary countermeasures is relatively low as compared to other continents. As reported in GCI (2018) report, only eleven (11) countries of the total of fifty-four (54) African countries have specific laws in cybersecurity and cybercrimes. ATU (2018) further states that twelve (12) countries have partial Cybersecurity Laws, while the majority of the thirty (30) countries have no meaningful cyber-crime legislative frameworks.

Most African countries have not yet fully established cybersecurity strategies to adequately protect their cyberspace within their jurisdiction or contributed meaningfully to the international security of the cyber domain (Kademi, 2014). Furthermore, while most parts of the globe, such as Asia, North America, and Europe, have developed NCSS as the beginning of the 20th century, Africa only began to show signs of consciousness in the 21st century and still at a slower pace. South Africa was the first African country to develop and implement an operational cybersecurity document in 2010 (Yusuf, 2019); this was in the form of an ICT Security Policy document.

It is not yet clear why African countries are becoming targets of cybercrime, yet they remain the most left behind in terms of preparedness to counter such attacks. Yusuf (2019) laments that Africa has had rapid Internet growth and high digital connectivity in the last decade. Yet, the growth is unmatched with the necessary commitments to the protection of the cyberspace. In this regard, this study is working on the assumption that; *"d*eveloping countries are not comprehensively designing, adopting and implementing effective NCSS or policies to deter the effects cyberattacks and cybercrimes.

The claim is that most of the existing strategies are replicas of international frameworks that fail to capture realities of developing countries and assume that generic cybersecurity models are inadequate to address cybersecurity challenges of developing nations".

1.3 Objectives of the study

1. To understand the standard features of the current existing NCSS.

2. Evaluate the existing approaches and NCSS for a selected sample from the developed countries and see the underlying factors that drive their model and strategies to NCSS.

3. To know the cybersecurity needs and requirements for developing countries, and evaluate against those from developed countries.

4.To recommend key actions, approaches, and policy guidelines for policymakers to improve the cybersecurity status as well as the design and formulation of their NCSS.

1.4 Research Questions

The research questions are crafted with the view of guiding the research process to achieve the objectives of this study;

The main research question;

1. Can developing African countries adopt current NCSS proposals from international groups?

The sub research questions;

2. What are the significant challenges, being faced by developing African countries affecting the designing and implementing NCSS?

3. What are the cybersecurity needs and requirements in these developing countries, and do what role they play in NCSS?

1.5 Contribution

This study builds on a lack of precise diagnosis of the cybersecurity situation in developing nations upon which the recommendation of cybersecurity frameworks will be made. The framework seeks to add a new dimension as opposed to contemporary proposals that are generic and prescriptive. Past research has highlighted that these frameworks have not improved the situation in developing nations, especially in Africa. Many authors such as Angwe-Mbarika, Angwe-Akuta, Mong'oa, & Jones (2011) and Internet Society (2017) have highlighted that Africa's underdevelopment challenges might worsen due to increased exposure to current and future cybersecurity attacks. And the lack of adequate response mechanisms as NCSS will not help the situation.

The study also is a motivation for the researcher who strives to design a new framework for cybersecurity, stimulating his further interests in the protection of cybercrime prevention and ensuring that adequate countermeasures are implemented to create a safe and secure cyberspace environment for developing nations. The researcher has a great interest in finding homegrown solutions that are sustainable and responsive to the direct environment, complementing, and comprehending other existing global products and solutions that counter cybersecurity challenges.

1.6 Research assumptions

The study assumes that developing countries need a framework or NSCC model that provides the standard that produces the ideal cyber counter results regardless of differing values as perceived from the outcry from many authors about the worsening cybersecurity situation in Africa, currently and in the future.

1.7 Thesis Scope

The study is focused on developing countries in Africa, focusing on the formulation of cybersecurity strategy at the national level and does not purport to provide a complete treatment of all cybersecurity subject matters globally.

The study also focuses on the literature review of already developed and implemented NCSS from developed countries.

1.8 Relevance of the Study

This study seeks to bring relevance to Government policymakers from developing countries, which are an integral part of bringing/coordinating various stakeholders together in discussing, consulting, designing, and implementation of NCSS. The study gives insights into the composition of stakeholders involved in NCSS processes, areas for improvement and focus pillars when formulating strategy. The study also provides insight into how experts view the current cyber state in the country and expressed their views on participation and involvement. With the existence of other models and frameworks, results from this study seek to further contribute to their improvement, taking into cognisance the highlighted needs and requirements from the study.

1.9 Thesis Structure

1. **Introduction**: The first chapter introduces the thesis giving an insight into the African cyber landscape, the issues to be discussed during this research, and the objectives of the research, research questions, research assumptions, relevance and scope of the study.

2. **Background Research**: This chapter starts by giving a background study on national cybersecurity as a subject matter, followed by various definitions of cybersecurity by International Organisations. The section further highlights the challenges being faced by developing countries, as viewed by other authors. Analysis of developed countries NCSS and an insight into the global NCSS adoption and implementation strategies are

discussed in this chapter. The chapter ends by briefly highlighting some of the significant global cyberattacks at the national level.

3. **Research Methodology**: The third chapter highlights the methods and methodologies employed in carrying out this research, the research design matrix, highlighting the strategies to be followed by the researcher. Furthermore, the chapter discusses the population and sample size for the survey, then further explores the data collection methods and procedures to be carried out. The chapter ends by taking note of the study limitations.

4. **Results**: The chapter will explain the results obtained from the conducted survey. Each question from the study will be discussed, and the results obtained expressed using various statistical methods and presentations.

5. **Analysis and Discussion**: The chapter starts with the evaluation of the various NCSS approaches used by developed nations. A comparative analysis is made of these approaches against results from the study. The section further explains the focus areas that African experts noted as significant in NCSS formulation. Through the literature review, the research gives an analysis of the effects and application of culture in NCSS formulations. The chapter ends with answers to the research questions as supported by the results gathered in Chapter 4 (four) and analysis done in this chapter.

6. **Conclusions**: This chapter includes recommendations for developing countries, the study conclusions made, and future work

7. **References:** This section contains a detailed bibliography of the citations made throughout this thesis.

Appendices: This section contains additional information not included in the body of the thesis.

In conclusion, this chapter introduces this research, problem statement, and the objectives of this study, research questions, research scope, research assumptions, and relevance of the study followed by the structure of the thesis.

CHAPTER 2: BACKGROUND RESEARCH

2.0 Introduction

As part of the background research, the author seeks to study the national cybersecurity strategies adopted in developed countries. In selection for study, the author will be guided by the definition and country classification as described by the United Nations Charter (United Nations, 2019). As defined by the UN, a '*developed country*' (industrialized sovereign state) is "a state that has a mature and sophisticated economy." It is a measure of its gross domestic product (GDP), its average income per resident, the advancement in technology and citizen's ability to access quality health care and higher education. For this study, the following five (5) developed countries that will have their NCSS under review include; The United States of America (USA), United Kingdom (UK), South Korea (ROK), China (ROC) and, Australia (AUS).

The comparison matrix focuses on key strategies that describe the main actors and their tasks (in particular the relationship and the harmonized integration between civilian and military authorities in the fields of 'security,'' defense,' 'law enforcement,' 'privacy' and, 'civil rights'). The background study will furthermore identify the challenges faced during the planning, formulation, designing development, organizing, and implementation of the National cybersecurity strategies in these developed countries. An interesting analogy of cybersecurity aspects, as definitions of terms, perceptions, culture, its application concerning the model or framework used in NCSS development.

NCSS should describe how it relates or intends to with other strategies at local, regional, and international levels. The NCSS stakeholders need to understand and comprehend how the NCSS's vision and activities related to different strategies. Strategies associated with NCSS include National Defense and Security strategy, National CI Protection strategy, National Digital Strategy, the National Economic Development Strategy (EC, 2010). The cohesion between these various strategies is an essential aspect for preserving national interests and foresting national security, economic development and protection of the citizens.

2.1 Background Study of National Cyber Security

The subject matter of cybersecurity strategy at the national level came into being around the year 2000 globally. The United States of America (US) had already started on cybersecurity issues since the 1990s. The US was the first nation to acknowledge cybersecurity at the strategic level. The term national security was first used within the US under the publication of a "National security strategy" in the year 1987 (Bartolotto .J, 2004). In those days, the notion of computer security or information security was not so much of national significance. With the evolution of technology and threat landscape, the term 'national security' was narrowed down to define the 'safeguarding the territorial integrity of a nation'. However, the meaning was perceived from a military standpoint.

With the continued evolvement of ICT post the Cold War era, there has been considerable development in security policies and the re-definition of 'national security'. Various authors started to incorporate the notion of "comprehensive security", that encompasses security from multiple domains as; economic, energy, environmental and, human security. The domains acknowledged non-state actors in addition to the state-centric territorial view of national security (Nicholas .P, 2013). These changes in security perspective, policy procedure, and narrative gave rise to the need for a concretely unified approach that meets the evolving security challenges and threats at national and international stage.

In the US, the "National Strategy to Secure Cyberspace" was released in February 2003 by the Department of Homeland Security. This was part of the overall national security strategy for homeland security developed responding to the September 2011 attack. The policy was designed purposely to "engage and empower the Americans to secure the Cyberspace, operate, control, and interact with (Washington, DC: White House, 2003). The September 2011 attacks became a significant yadistic supporting the notion that cybersecurity has evolved to become a critical domain in national security, as it generated threats affecting national assets, infrastructure and citizens.

Globally, the September attacks triggered action plans and strategy changes as cybersecurity matters began to draw attention of policymakers, Government leaders and experts across the globe. However, before the September attacks in the US, other nations had started making slight initiatives in cybersecurity. In the year 2005, the Germany republic developed and adopted the "National Plan for Information Infrastructure Protection" (German Interior Ministry, 2005), subsequently Sweden, in July 2006, established a "Strategy to improve internet security in Sweden." The Stuxnet attack in 2007 triggered the development of the Estonian Cybersecurity strategy in 2008, focusing on the protection of public and private sector information systems, and critical infrastructures (Estonian Ministry of Defence, 2008).

In the years that followed, Australia, Canada, and the UK developed and implemented their NSCC; however, the contents of these strategies were considered to be comprising of relatively narrow scope. The NSCC scope viewed what key elements constitutes cybersecurity. Authors argue that these strategies were focused on individual nations' protection (national interests) that disregards the global view of cybersecurity as a matter of International interest (Graaf, P. 2013). The Republic of South Africa was the first African country on the continent to develop and enact a national security strategy

(National Cybersecurity Framework). The strategy document by the South African Government focused on objectives that emphasized on bringing security and confidence to Government systems and critical infrastructures (Pretoria: South Africa Government, 2012).

The increase and variation in cyberattacks, global threats, incidents, vulnerabilities, and the impact that cyber threats have on national and global economies and societies have led to a slightly increased adoption and implementation of NCSS around the years from 2010 to 2014 (ITU, 2015). In these increased global threats incidents, there has been the emergence of some state-sponsored global attacks, notably politically and diplomatically motivate. In this regard, the Korean attacks in 2013 were significant national cyber threat incidents, where computer networks running three (3) major South Korean banks and two largest broadcasters were attacked. This attack saw the immediate crafting and adoption of the Korean National Security Strategy (New York Times, 2013).

2.2 Defining Cybersecurity

Nowadays, cybersecurity should not be equated to internet security, information security, information assurance, or ICT security as the former is more now more comprehensive. Cybersecurity now includes aspects as information perseveration, confidentiality, integrity, availability, authentication, and non-repudiation. Though not all countries are defining or describing what they mean by cybersecurity in their NCSS, the varying perception falls into either; protection of information systems, secure ICT system, and services or mitigation of threat from cyberspace. That is to say, there is a narrower rather than holistic perception and usage.

Graaf, P. (2013), highlighted that a typical strategy should establish common ground by specifying and wording the critical concepts. While nations pursue their interests, the cyber domain also lacks accepted norms and principles of proportionality (Geneva: ITU, 2011). When international approaches are discussed, this brings about confusion and difficulties. Examples of frequently mentioned and fundamental terms are illustrated in the table below and how International bodies define them.

Table 1: Cyberspace and Cybersecurity definitions.

INTERNATIONAL BODY	CYBERSPACE	CYBERSECURITY
International Telecommunications Union (ITU)	"Connected Systems and services either directly to or indirectly to the internet, telecommunications, and computer networks."	"Collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies used to protect the cyber environment and organization and User's assets. "
International Standards Organisations (ISO)	"the complex environment resulting from the interaction of people, software and services on the internet by means of technology devices and networks	"The preservation of confidentiality, integrity, and availability of information in Cyberspace."

	connected to it, which does not exist in any physical form."	
European Union (EU)	"the virtual space in which the electronic data of worldwide PCs circulate."	"Safeguarding and action plans that can be used to protect the cyber domain, both in the civilian and military fields, from those threats that are associated with or that may harm its interdependent networks and information Infrastructure.”

Barclay (2014) stated that NCSS should establish common ground by defining the fundamental notions and scope since the understanding of cybersecurity differs significantly with other nations having defined or described the concept through focusing on approaches and methodologies. Different countries use a holistic, top-down approach that focuses on the protection against threats from cyberspace and information security. Speer (2000) emphasized that the lack of harmonized cybersecurity definitions globally causes confusion between nations when discussing international approaches and cooperation to the global cyberspace threats and issues. A national cybersecurity strategy typically takes the form of a policy framework that outlines a vision and articulates the priorities, principles, and approaches needed to be understood as nations manage cyber risks.

2.3 International Cyber-security Standards

International models and standards are a starting point for a framework that gives a guide to the designing and formulation of NCSS (ITU, 2011). Research indicates that vulnerability tools do not detect as much as 40% of all attacks, or either do they even fall under the scope of the already set framework (Scully, 2011). This highlights the problems of security countermeasures that are designed only to target infrastructure and boundaries of networks, leaving the information inside the system vulnerable once access is achieved (Scully, 2011).

The threats from both internal and external factors to the nation follow different attack strategies such as point attack, spread spectrum, application, and hardware-based attacks (Saini and Saini, 2007) and for various reasons ranging from bragging rights to financial gain (Scully, 2011). In this view, international standards give guidance and provide a basic framework, which might not entirely be adequate to counter the threat from cyberspace due to the dynamicity in technology. Some of the international standards already developed include;

2.3.1 ISO 27032 Standard

ISO 27032, is one of the globally recognized standards for cybersecurity standards. The ISO 27032 standard addresses security gaps arising from the lack of communication between the different users and providers of cyberspace (ISO, 2012). The standard tackles any risks not covered by the current Internet, network, and information and communication technology security. The standard designed because;" ISO/IEC 27032, "devices and the connected networks that support cyberspace have multiple owners – each with their own business, operational and regulatory concerns." Not only do the different users and providers share little or no input, but each has a different focus when dealing with security. Such a fragmented state opens up vulnerabilities in cyberspace. ISO/IEC 27032 will provide an overarching, collaborative, multi-stakeholder solution to reduce risks associated with information sharing, coordination, and incident handling (ISO, 2012).

2.3.2 ENSIA Cyber-Security Guide

The European Network of Information Security Agency (ENISA) is a conglomerate working for the European Union (EU) Institutions and member states (ENISA, 2010). ENISA was set up as the EU's response to cyber-security threats to the Union. The Cyber-Security Strategy guide identifies a strategic plan of actions, of which strategic objectives are categorized as mission-critical and measurable Key Performance Indicators (PKI). The ENISA guide has two key phases in governing a national cyber-security strategy: Developing and executing the strategy and Evaluating and adjusting the plan (ENISA, 2010). The structure follows the highly accepted Deming's 'Plan-Do-Check-Act' (PDCA) model for the governing of their national cyber-security strategy. The PDCA model also facilitates the monitoring and continuous improvement of procedures, policies, processes, and products. Also, ENISA identified three approaches pursued in governing strategies identified;

- A linear approach: The strategy is developed, implemented, evaluated and eventually terminated (or replaced);

- A lifecycle approach: From output from the evaluation phase is used to maintain adjust and remodel the strategy itself; or
- A hybrid approach: The approach has several continuous improvement made on the cycles from different levels.

2.3.3 ITU Cybersecurity Guide

The International Telecommunications Union (ITU) is a specialized agency of the United Nations whose responsibility covers ICT's across member states. The ITU has derived a Global Cybersecurity Agenda (GCA), which is a holistic framework for coordinating, developing, and implementing a robust global culture of cybersecurity (ITU, 2011). Since cybersecurity is a national policy issue, Ends-Ways-Means strategy paradigm was adopted due to its popularity with national policymakers (ITU, 2011). The model relates to objectives that are to be achieved on a national level, the ways *to* identify how these objectives and the means are the resources used to achieve these objectives (ITU, 2011).

The ITU Cyber Security guide focuses on the issues that countries should consider when elaborating or reviewing national cybersecurity strategies (ITU, 2011). As national capabilities, needs, and threats vary, the ITU recommends that countries use national values (culture and national interests) as the basis for strategy formulation guide.

2.3.4 NIST framework

Most nations have developed and implemented cybersecurity conceptual frameworks based on the NIST framework, model and standards. The NIST Cybersecurity Framework seeks to provide organizations with a common way to;

- Describe their current cybersecurity state or posture.
- Describe their desired cybersecurity state.
- Identify and prioritize opportunities for improvement within the context of a continuous and repeatable process.
- Make a progress assessment of the desired cybersecurity state.
- Make internal or external communication with stakeholders about cybersecurity risk.

One exciting aspect of the NIST framework is the establishment of a standard assessment procedure that assists in the assessment of the effectiveness of security controls in Government systems. The assessment methods and procedures are used to determine if the security controls are implemented correctly, operating as intended, and producing the desired outcome concerning meeting the security requirements of the organization (NIST SP800-53A, 2014).

2.4 Cybersecurity challenges faced by developing nations

Kabanda (2019), in his research work, highlighted that despite the slight progress in developing countries with respect to cybersecurity, a lot still needs to be done. Kabanda, further went on to note the following as the significant challenges faced by developing African nations;

i) Legal frameworks (Norwegian Institute of International Affairs, 2018).

ii) Infrastructure (International Telecommunications Union, 2009).

iii) Lack of harmonized legislature (Bande, 2018).

iv) Balancing harmonization and country-specific needs (ITU, 2012).

v) Lack of adequate frameworks that speak to their cybersecurity needs (Tagert, 2010).

vi) Lack of information sharing frameworks (Tagert, 2010).

vii) Reporting and communicating frameworks on cybersecurity incidents (Republic of Mauritius Cybercrime strategy 2017-2019).

A special report by the United Nations Economic Commission for Africa (UNECA) in 2018 highlighted that Sub-Saharan Africa had been labelled as "a new cybercrime harbour." This report was due to the inadequate protection of and increased cyber threats to its ICT infrastructure resulting from the availability of fast Internet access, a growing number of Internet users, and weak cybercrime laws. The implications reach far beyond geographical or political borders (UNECA, 2018).

2.4.1 Global NCSS Adoption Statistics

According to the ITU report of 2017, 38% of countries have developed and implemented NCSS globally, while 12% are in the process of developing (Global Cybersecurity Index 2017). Another report for the start of 2020, noted that 78 countries have now fully completed and published their NCSS from the 193 United Nations member states (Cyber Regulation Index, 2020), and this represents 40.4% global adoption, that's a 2% increase from 2017 to 2020. In respect to African nations, only 14 % have developed a national cybersecurity strategy or at least have cybersecurity and data protection regulations, instruments and laws, despite the continent making strides in improving its digital ecosystem.

A survey conducted by the African Union Commission (AUC, 2020), out of the fifty-five (55) African states, only eight (8) countries have a national cybersecurity strategy, with thirteen (13) countries with a CERT or CSIRT, fourteen (14) states having personal data protection laws, and eleven (11) with cybercrime laws. In summary, these brief statistics of adoption and implementation of various cybersecurity initiatives, fall short when compared to the impact and effects associated with cybersecurity breaches globally. Table 2, below shows statistics and current status in seven (7) developing African countries which are part of this study.

Table 2: Status of African developing Countries that are part of this research- as of December 2019.

Country	Cybersecurity Laws	CERT’s Existenc	Internet Access / Penetration rate	Existence of NCS
Botswana	Enacted	Pending	47.0%, 4.0%	Pending
Mozambique	Enacted	Pending	20.9%, 7.0%	Pending
South Africa	Enacted	Established	55.0%, 35.9%	Established
Zambia	Enacted	Established	53.7%, 12.3%	Pending
Zimbabwe	Enacted	Pending	56.5%, 6.7%	Pending
Tanzania	Enacted	Established	38.7%, 7.2%	Pending
Malawi	Enacted	Established	14.2%, 2.6%	Pending

Notes:

- Enacted - The country already has some form of laws or legal instruments that govern computers, computer networks, data, information, or usage.
- Pending - The country has initiated the process to formulate, design, or develop, but it’s still not recognized and in use or referenced.
- Established - The country has already developed, adopted, and implemented.

2.5 Analysis of NCSS for Developed Countries

National cybersecurity strategies of the USA, UK, Australia, South Korea, and China are mainly acknowledged worldwide for mentioning dual aspects of cybersecurity, i.e., both offensive and defensive cybersecurity action plans (Dunn, 2019). Besides the UK and US, South Korea and Australia are amongst the few top countries that have implemented and continued to update their NCSS. These five (5) nations have been selected for Literature review as part of this study. Some of the already published NCSSs adopted a holistic approach to NCSS and all the related interdependent areas. However, some ended up marginalizing the actions on specific components of the cyberspace domain hence and limiting the scope of focus (Graaf, P. 2013). These variations and narratives from the selected countries give this research a broader perspective.

A comparative matrix will be used to understand how developed nations formulate and implement NCSS. The matrix will highlight the primary focus areas, perception, how the nation's culture, beliefs, values, and ethos have an impact on the process.

2.5.1 United States of America (USA) NCSS

The United States released its International Strategy for Cyber-space (Updated National Cyber Security Strategy) in May 2011, which describes a set of activities across seven interdependent areas, based on a collaborative model involving government, international partners and the private sector: The strategy highlights for America to;

- Economy: Promoting International Standards and Innovative, Open Markets.
- Protecting Our Networks: Enhancing Security, Reliability, and

Resiliency.

- Law Enforcement: Extending Collaboration and the Rule of Law.
- Military: Preparing for 21st Century Security Challenges.
- Internet Governance: Promoting Effective and Inclusive Structures.
- International Development: Building Capacity, Security, and Prosperity.
- Internet Freedom: Supporting Fundamental Freedoms and Privacy.

The American NCSS is focused on ensuring that the USA Government defends the homeland by protecting networks, systems, functions, and data; Promoting American prosperity by nurturing a secure, thriving digital economy and fostering strong domestic innovation (Whitehouse, 2018). Preserve peace and security by strengthening the ability of the United States in concert with allies and partners yet to deter and, if necessary, punish those who use cyber tools for malicious purposes (Whitehouse, 2018).

2.5.2 United Kingdom (UK) NCSS

In the year 2011, the UK established its first National Cyber Security Strategy that underpinned the UK's commitment to cybersecurity, as witnessed by a considerable investment by the British Government's of £860m towards the National Cyber Security Programme (HM, Government, 2016). In 2016, the British Government revisited and updated its NCSS, creating 2016-2021 strategy plans. The UK's approach is concentrating on the national objectives that are linked to the evolving cyber world. The national objectives include; making the UK the major global economy of innovation, investment, and quality in the field of ICT. These national objectives gave the UK the drive to tackle the risks from cyberspace like cyber-attacks from criminals, vulnerabilities, terrorists, and states sponsored attacks to make it a safe space for citizens and businesses (Enisa, 2012). All its efforts as enshrined in their NCSS are anchored on these three principles; **D**efend, **D**eter, and **D**evelop the UK.

2.5.3 China's NCSS

In the year 1993, two years after the Gulf War, the Chinese military adjusted its military-strategic document in which it set its focus to "winning wars in conditions of modern technology, particularly high technology" as the primary aim of preparations for military struggle. In 2004, the military's strategy was changed to "winning local wars under conditions of informationization" (Jinghua. L, 2004), already China was shaping its National Cyber Security Strategy as early as 1993. China published its NCSS with the theme focusing on peace, security, openness, cooperation, and order. The strategy is focused on enabling economic growth, developing military capacity, procuring globally emerging technologies for cyber espionage operations for the Chinese Government (DARICILI and ÖZDAL, 2018). The strategy is anchored on the following four (4) principles;

- Respecting and protecting sovereignty in cyberspace
- Peaceful use of cyberspace
- Governing cyberspace according to the law
- Comprehensively manage cybersecurity and development

In response to several global incidents such as the mass street protests in Iran's 2009 presidential election disputes, the Arab Spring (Egypt, Syria, Tunisia, and Libya), as well as the 2011 US's Occupy Wall Street movement and the London Riots of 2011, China updated its Cyber Security Strategy since the adoption and usage of social media was instrumental in all of the above-listed events. In 2013 again, updated its strategy describing some objectives of its "cyber capabilities" to include: a) cyberspace situation awareness, b) cyber defense, c) support for the country's endeavors in cyberspace, and d) participation in international cyber cooperation programs.

2.5.4 Australia NCSS

Australia first established its NCSS in 2013, and reviewed the strategy in 2016; this strategy is focused on "securing Australian prosperity in a connected world." The new policy seeks to build from an investment of $230 Million to continue to support Australia meet the rapidly evolving cyber threat environment as well as take advantage of the enormous growth opportunities afforded by a trusted, digitally-enabled economy (Austcyber, 2020). The strategy seeks to establishes five key theme actions for Australian Government's cybersecurity for the next four (4) years till 2020:

- A national cyber partnership
- Strong cyber defenses
- Global responsibility and influence
- Growth and innovation
- A smart cybernation

As of writing this publication, Australia is in the process of reviewing its National cybersecurity strategy 2020, to meet with the evolving cyber threat landscape (Australian Home Affairs, 2020).

2.5.5 South Korea's (ROK) NCSS

South Korea is the world's most wired nation, yet the Government operated without a national cybersecurity strategy up until late 2019. The country suffered a wide variety spate of very large attacks, such as the breach that affected over 35 million accounts on the Cyworld website as well as the Nate web portal both run by SK Communications (BBC, 2019). The Korean Communications Commission (KCC), in 2019, highlighted that the recently adopted NCSS by the ROK "is one that explicitly considers the cyberspace as an independent operational domain just like the sea or air were each requires state-level attention, focus and ultimate defense mechanisms."

The NSCC goals include a) Ensuring stable operations of the state, b) Responding to cyber attacks, and, c) Building a strong cybersecurity foundation (the Republic of Korea, 2019). The new strategy seeks to give control over cybersecurity at the Government level to the National Cyber Security Centre (NCSC). In 2016, the Ministry of National Defense released a white paper that focused on highlighting the primary threat vector targeting ROK from internal and external attacks. Two major threats noted were threats emanating from the

Democratic People's Republic of Korea and Cybercrime targeting the digital economy and the financial sector (Ministry of National Defense, 2016).
Considering these challenges highlighted above the Korean NSCC was formulated encored on the following three guiding principles,

- Balance individual rights with cybersecurity: Strike a balance between protecting cyberspace and safeguarding the fundamental rights of the people, for example, privacy.
- Conduct security activities based on the rule of law: Carry out the government's cybersecurity policies and activities in a transparent manner and compliance with domestic and international laws.
- Build a system of participation and cooperation: Encourage individuals, businesses, and the government to participate in cybersecurity activities, and pursue close collaboration with the international community.

2.6 Evaluation of NSCC Approaches

The evaluation and comparative analysis matrix seek to highlight the areas and focus pillars that experts from developing African countries in this study have noted against the literature from the survey done on the five (5) developed countries' NCSS. The NCSS discussed in the above section, and all NCSS studied seem to be more concerned or inclined towards safeguarding against external threats, rather than threats emanating from internal. All the five (5) countries have little or no consensus on what constitutes cybersecurity threats and the threat topology. The threat topologies outlined in these strategies are centred primarily on cybercrime, cyber espionage, cyber terrorism, cyberactivism, and lately, cyber warfare.

The scope of terminologies and their extensive usage are influenced by what a nation perceives to be cyberspace and its technological advancement. Kabanda

(2019) noted that there are still misunderstandings regarding the definition of some basic terms, for example, incorporating the concept of "information security" instead of "cybersecurity" and hence a lack of inherent comprehensiveness or scope definition.

National strategies discussed generally lay out a narrative that varies between nations, hence leading to the introduction of various objectives and concepts. These strategies, nevertheless share familiar concepts of holistic, integrated or comprehensive approaches. However, is a general agreement amongst authors for a more holistic approach to cybersecurity policymaking seeking to include all stakeholders. A comprehensiveness approach, in this context, means the inclusion of all domains to the cybersecurity challenges. Domains such as economic, social, educational, legal, law enforcement, technical, diplomatic, military, and intelligence-related aspects, The integrated approach stresses the participation inside the Government and outside, the society (including businesses and individuals) and with foreign partners.

The Australia Government aims to develop a "Government-led coherent, integrated approach" (Australian Government, 2009), and the US government seeks to 'integrate competing interests to derive a holistic vision and plan' (US White House, 2009). The UK NCSS supports a coherent approach to cybersecurity in which the Government, Organizations across all sectors, the public, and International partners all have a part to play, (United Kingdom, 2013). The South Korean Government is aimed at "creating free and safe cyberspace to support national security, promote economic prosperity, and contribute to international peace."

Similarly, all strategies discussions acknowledge cybercrime as it causes enormous financial loses to individual, companies, nations and the global economy at large, South Korea, UK and Australia are the nations that define almost all cyber-related notions in their strategies, some described the basic terms as can be exemplified in the United States of America's strategy. This brings up the issue of international cooperation or standardization in approaches, with the varying approaches and notions in NSCC, this bringing confusion and difficulties in achieving this global cooperation. One case that can be sighted is the protracted "historical, economic and political" standoff between South Korea and Japan (The Diplomat, 2019), the question remains, can they be able to produce any sound bilateral agreement towards working together on national cybersecurity matters?

Another case that can be sighted is the global standoff between the United States of America and the People's Republic of China relations on political, economic, and technological fronts. Globally, the relationship in respect to cybersecurity has termed, the "Cyber-problem" and with this brings issues of international cooperation, standardization into question again (Harold et al., 2016) Given these divergent views and NCSS approaches worsened, by China's abandonment of formal talks on cybersecurity with the United States. One example of the difference arising from adherence to each of the two ideal types is the case of the United States were it seeks to punish North Korea for its attack on Sony Pictures Entertainment, as a way to signal to all nations that cyberattacks cannot be conducted with impunity, (Harold et al., 2016).

2.7 Signification Cyberattacks

The growth of politically motivated attacks triggered the speedy development of NCSS, although attacks of such nature had occurred before the 2007 attack on Estonia. International attention has understandably significantly increased since then. Some of the major Global National Cybersecurity attacks and breaches include;

- **Estonia (2007)**- Cyberattacks which began on 27 April 2007 and targeted websites of Estonian organizations, including Estonian parliament, banks, ministries, newspapers, and broadcasters, amid the country's disagreement with Russia about the relocation of the Bronze Soldier of Tallinn (Wikipedia, 2007), Most of the attacks that had any influence on the general public were distributed denial of service type attacks ranging from single individuals using various methods like ping floods to expensive rentals of botnets usually used for the spam distribution.

- **Myanmar (2010)**- Distributed denial-of-service attacks (DDoS) that began on 25 October, occurring ahead of the 2010 Myanmar general election. This election was the first that Myanmar had had in 20 years. The attacks were significantly larger than attacks against Estonia and Georgia in 2007 and 2008, respectively (BBC, 2010).

- **Singapore (2013)** –Series of hack attacks initiated by the hacktivists group Anonymous, under the online handle "The Messiah." The cyberattacks were in response to the web censorship regulations that were instituted in Singapore. The censorship regulations were seen as targeting, specifically independent free media news outlets (BBC, 2013).

- **South Korea and the United States (2009)** – A series of coordinated cyberattacks against major government, news media, and financial websites in South Korea and the United States. The attacks involved the activation of a botnet that hijacked a large number of computers by maliciously accessing targeted sites, causing their servers to overload due to the influx of traffic (Park. J, 206).

- **United States (2016)** - The Democratic National Committee cyber attacks took place in 2015 and 2016, in which 'alleged' Russian computer hackers infiltrated the Democratic National Committee (DNC) computer network, leading to an enormous data breach. Cybersecurity experts and the US Government stated that the cyber espionage was the work of state-sponsored agents from the Russian Federation (BBC, 2016).

- **Global (2017)-** The WannaCry ransomware attack was a May 2017 worldwide cyberattack emanating from the WannaCry ransomware (cryptoworm). The attack targeted computers running Microsoft Windows Operating System through encrypting user data and demanding ransom payments in the form of Bitcoin cryptocurrency. It propagated through EternalBlue; an exploit allegedly developed by the United States National Security Agency (NSA).

- **Ukraine (2017)** – Series of cyberattacks that used the Petya malware began on the 27th of June, 2017 targeting websites of Ukrainian Organizations, Banks, Ministries, News sites, and electricity firms. Similar infections and attacked were also reported in France, Germany and, Italy.

- **Iran (2010)** - Stuxnet attack was a malicious computer worm, uncovered in September 2010, that targeted the supervisory control and data acquisition (SCADA) systems. Stuxnet attack was believed to be responsible for substantial damage to Iran's nuclear program.

- **South Africa (2014)-** South Africa reportedly lost approximately ZAR50 billion in 2014 due to cyber-attack incidents, and over half a billion online personal records were lost or accessed illegally in South Africa during 2015 (SABC News, 2017). Another national level significant incidents were the Gautrain incidents which involved computer-related theft/fraud committed by a group of persons (Insiders), and the Eskom incident all reportedly worth over R20 Million (Symantec, 2016).

- **Global** (2020)- As the world has been battling to contain the COVID-19 pandemic, there has been a fivefold increase in cybersecurity and cybercrime-related incidents globally as attackers are taking advantage of the pandemic and changing the cyber threat landscape (WHO, 2020). Cybercriminals are attacking the computer networks and systems of individuals, businesses, and global organizations (INTERPOL, 2020).

2.8 Chapter Summary

The chapter highlighted the background research to the thesis work; the main focus on background study was national cybersecurity. The section further gives various meanings and perspectives of the term cybersecurity, as explained by multiple International organisations such as ITU, NIST, and ISO. The chapter provided a brief explanation of some international standards currently being used in guiding nations in formulating NCSS. Global NCSS adoption statistics and challenges being faced by developing countries concerning cybersecurity are discussed. As part of the literature review, the chapter gave an analysis of selected nations NCSS from developed nations. The chapter ends by outlining some major global cybersecurity attacks targeting various countries globally.

CHAPTER 3: RESEARCH METHODOLOGY

3.1 Introduction

This section of the research discusses the research methods, underlying reasons for the choice of such techniques used to answer research questions stated in chapter 1. It discusses the overall research plan to be adopted. The study examines the sequential mixed methods of qualitative and quantitative methods, discussion on the target population, the sample size, and the sampling techniques to be used. Purposive sampling will be used to select several crucial cybersecurity entities such as national regulators, cybersecurity regional and international organizations, including the International Telecommunications Union, and the African Telecommunications Union. The use of secondary data sources will also complement the study.

3.2 Research philosophy

The research philosophy considered for this study takes on a pragmatic perspective by considering that cybersecurity issues in Africa or developing countries can best be understood by observing the situation. It is the emerging reality from the observation that informs what exists and how knowledge of this reality can be obtained. For instance, understanding the cybersecurity needs for Zimbabwe is best understood from the subjective meanings given by different stakeholders in Zimbabwe. It is their lived experiences that provide a better understanding of what they require to decide on an idea NCSS model is appropriate and responsive to the needs of the communities. According to Dlamin, Tute, & Radebe (2018), cybersecurity depends on perceptions of people and how they securitize cybersecurity threats.

How cybersecurity is prioritized and viewed in Africa against the rest of the world is based on subjective perceptions and opinions of the players in those regions. However, identifying the challenges of cybersecurity in developing African countries takes a two-pronged approach. Social meanings attached to cybersecurity indeed provide closer information on what the affected think of cybersecurity. But accumulated literature has already identified some standard features of cybersecurity. Such features are existing realities with single realities, and it is appropriate also to consider objectively how such reality manifests in developing countries. Furthermore, Wamala (2012) takes the view that the international community appreciates the independent existence of cybersecurity threats and models which only requires to be discovered and adopted for each specific country and in response to its protracted national interests and values.

This study considers that issues such as cybersecurity models can be understood by considering some suggested models rather than subjectively assessing the views of different participants. A single worldview to the cybersecurity issues in African developing countries will lead to a biased understanding (Ahmed, 2008). A more holistic view takes on the two warring views for this social research subject matter: interpretivism and positivism. To understand the underlying reasons why Africa lags behind other world regions, it is prudent to consider the problems from the lived experiences of the African people. The way the people, local experts, understand the threats and attacks and why they remain a target of such attacks remains constructed meanings from the very people who are experiencing the phenomenon.

Against this perspective, a more interpretive and interactionist approach will be considered. However, the majority of the issues to be investigated in this study remains objective and scientific realities that can easily be observed independent of the subjective biases of the researcher or the subjects of study.

The cybersecurity practices, the effectiveness of the cybersecurity measures, and models of cybersecurity threat countermeasures are objective and single realities that can be measured and objectively observed. Thus a mix of subjective and objective views to the cybersecurity issues in Africa will be considered providing a more precious insight into the problems as opposed to a bias towards a single angle of viewing the problem.

Siedchlag and Jerkovic (2018) in their book, Homeland Security and, Culture, explored the role that culture plays in the study and practice of national security from a whole community and all Government scope. It does so by analyzing and discussing strategic, organizational, operational, and social cultures in the various nations and from an international perspective. In this regard, this research work will qualitatively analyze the multiple cultures from the developed countries and see how culture has influenced the approaches, models, or its application to NCSS formulation and implementation.

3.3 Research design

A research design is an overall blueprint upon which the entire study will be based (Cooper & Schindler, 2016). This study expects to use the survey research plan, which is more descriptive and exploratory. The new dimensions of exploring the reasons why cybercriminals are targetting Africa is a relatively new concept. Discoveries are expected to be brought to fore after the study. An exploratory design will help the researcher find unique aspects of the nature of appropriate cybersecurity model for these developing countries and other developed countries that have rarely been studied. However, the descriptive plan will help the study to get more insights into cybersecurity needs and requirements.

3.4 Research matrix

According to Choguill (2005), every research project requires a clear planning strategy on how the data will be collected to answer which specific study objectives. This provides some clear strategy which the researcher might follow and reduce the collection and analysis of redundant data. The research design matrix is a simple table with rows and columns showing how each major design element will be addressed from the methodology to be used to the analysis expected on each item. In this study, a similar approach has been used in which the study's major design issues: research objectives, methodology, and analysis techniques are addressed, as indicated in Table 3 below.

Table 3: Research design matrix for studying cybersecurity in developing countries

Research objective	**Methodology**	**Analysis**
(1) To understand the standard features of the current NCSS.	• Documentary review of features identified in the literature • Structured survey questionnaires send to cybersecurity experts in selected developing African countries.	• Qualitative analysis of the features in literature – manual analysis procedure. • Using weighted mean scores and bar graphs to describe the features
(2) To evaluate the current approaches and NCSS for a selected sample from the developed countries, and	• Review of existing strategies from both developed and developing countries	• A qualitative comparison of different strategies will seek to identify criteria's that can

see what the underlying factors that drive their model and approaches to NCSS are.	• Use comparison table using criteria developed from key features of the surveyed strategies.	be used to define NSCC for developing countries.
(3) To know the cybersecurity needs and requirements for developing countries, and evaluate against those from developed countries.	• Interview at least10 experts as in purposively sampled • Structured survey questionnaires send to cybersecurity experts in selected countries.	• Use thematic analysis to identify the major requirements and needs from a comparative study of themes with the criteria defined.
(4) To recommend key actions, approaches, and policy guidelines for policymakers to improve the cybersecurity status as well as the design and formulation of their NCSS.	• I am using strategy formulation and guideline processes as reported in the Global Agenda for Cybersecurity and other Models for reference.	• Use the pillars identified in surveys and the Criteria to recommend a strategy framework and approaches for the developing countries.

3.5 Research methods

In this study, the approach will involve the use of qualitative and quantitative methods, as indicated in Table 3.1. To understand the cybersecurity threats, needs, and requirements in African countries, the study will use quantitative techniques by using a structured questionnaire on a five-point psychometric Likert scale were; (one) 1 refers to disagree strongly, two (2) disagree, three (3) not sure/neutral/moderately, four (4) yes agree and, five (5) strongly agree.

This data will be triangulated by a qualitative method of manual/content analysis of documents from previous literature. Then to identify the key requirements and needs of a responsive NSCC cybersecurity framework for developing countries, interviews with experts will be done, which provides qualitative data and expose this to theoretical thematic analysis. A strategy approach process will be followed based on data collected (both quantitative and qualitative) to outline the recommendation for developing countries.

3.6 Population

The population will consist of cybersecurity experts, professionals who are in the cybersecurity, or ICT regulators in Africa. Others include the individual experts, academia, Government Ministries, Citizens, Security sector representatives (Military, LEA's), and bodies such as POTRAZ, ATU, and ITU who proffer expertise in cybersecurity. The population can vary continuously as some experts emerge with new qualifications and expertise in security-related fields during the data gathering process; thus, the population is not a fixed total but a dynamic number that changes over time.

3.7 Sample size

A purposive sample will be considered in which the sample size will emerge from data saturation criteria. Saturation will determine the sample size. The survey will be working with a sample of approximately 200 participants from around 10 African developing nations, drawn from the SADC region, The Southern African Development Community (SADC) is a regional economic community comprising of sixteen (16) Member States that includes, Angola, Botswana, Comoros, Democratic Republic of Congo, Eswatini, Lesotho, Madagascar, Malawi, Mauritius, Mozambique, Namibia, Seychelles, South Africa, Tanzania, Zambia and Zimbabwe (SADC, 2018).

3.8 Sampling methods

Purposive and convenient sampling will be used to select the participants. Only experts with relevant information on African cybersecurity status will be considered, and the collection will continue till saturation begins to emerge. Furthermore, five cybersecurity strategies will be selected conveniently, from the already developed countries. The chosen countries from the developed nations have been selected purposively due to their rankings on the Global Cybersecurity Index, and their contribution, preparedness to global cybersecurity matters. The nations are the United States of America, the United Kingdom, Australia, the Republic of Korea, and the People's Republic of China.

3.9 Data collection procedure

The data will be collected through a survey (questionnaires). Before collecting the data, consent will be sought from the participants. A Google survey form will be created and distributed. For sharing, various means as email links, social media chat platforms (Twitter, Facebook and, WhatsApp) to be used to reach a wider sample population from different countries.

3.10 Data Analysis

Data from interviews will be analyzed using a qualitative analysis approach by Braun and Clarke (2006). These authors proposed a six-step theoretical thematic analysis. R Studio will be used to analyze qualitative and quantitative data. The numerical data from survey questionnaires will be analysed through statistical methods; namely, descriptive statistics to synopsize data from a sample exercising the mean or standard deviation, and inferential statistics to view the data as a subclass of a specific population or a sample class.

3.11 Study Limitations

There are some limitations to this study, and they are as follows;

Self-reported study: Responses from the survey were self-reported by the respondents. Respondents completed the survey based on their knowledge and perspective to the matters in question, making the responses subjective. Self-reporting might mean, the same study might not get the same results if conducted in other developing countries; hence a global perspective, or provide a comprehensive overview of all developing African countries can not be achieved based on these results.

Sampling Size: Cybersecurity experts are not in abundance across the world, let alone in South Africa (Business Tech SA, 2019), in South Africa, if there are one-hundred (100) expert in charge of cybersecurity in each country. There are 54 countries in the developing African countries; it makes a total of five thousand, four hundred (5400) experts in the world that deal with cybersecurity. The study received a hundred and one (102) responses from eight (7) countries, which limits the research as it cannot be generalized to cater for an overall perspective since the majority of the developing countries were not represented in the study.

Non-response Bias: Non-response bias might be possible as the survey was sent out also to the security sector establishments (Military, Police, and Intelligence Agencies), but only a few responded to the survey. This could be as a result of a lack of interest in the subject matter, or work conflict of interest and issues related to privacy and security clearances.

Global Coronavirus pandemic- One of the significant limitations to this study, was that the research was conducted during the period when the world was fighting to contain the spread and effects of the COVID-19 virus that affected nations and killed hundreds of thousands of people. At the time of the survey, all the developing African countries under study had been placed under lockdown.

3.12 Chapter Summary

This chapter discussed the survey design method used to collect the data from the experts and the types of analysis that will be employed. A questionnaire tool was designed and used to collect data from one-hundred and two (102) cybersecurity experts from various sectors and stakeholders around seven (7) countries sampled from the SADC region. The chapter also provides the reliability, validity, and limitations that have affected the research. In the next chapter, the results are presented and explained.

CHAPTER 4: RESULTS

4.1 Survey Structure

The questionnaire created for the study was designed using Google forms as the survey platform for the dissemination of nine (9) questions on the survey. One hundred and two (102) responses were received in a month's time, running from 17 April to 11 May 2020. Two (2) records where removed during data cleaning since they were not accurately completed.

4.2 About the Respondents

The first set of questions were meant to ascertain the demographic view of the respondents, based on the country of origin and sector they belong to.

4.2.1 Country representation

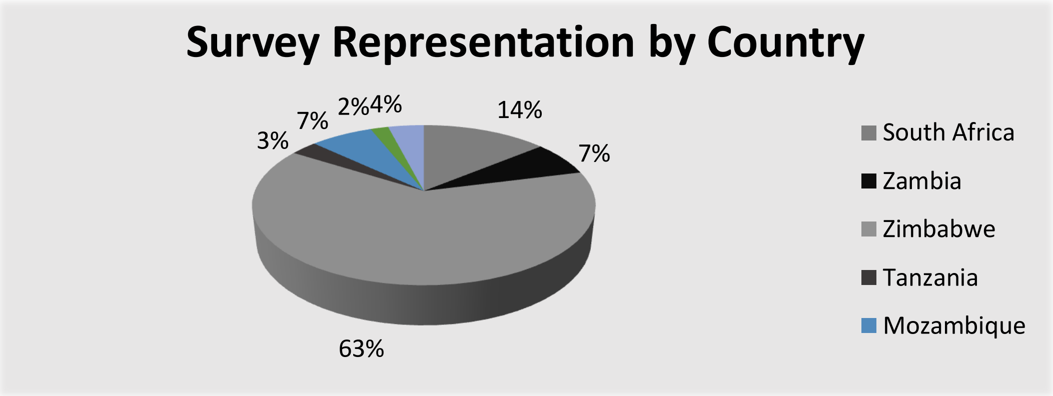


Figure 1: Pie chart showing countries representation in the survey

The first question asked was the country that the respondents came from. The gathered data showed that 63% of the respondents were from Zimbabwe, South Africa had a 14% representation, while Mozambique and Zambia both had 7% representation, respectively. Botswana, Tanzania, and Malawi had proportion representation of 4%, 3%, and 2%, respectively. According to Yount (2006), for a survey, it is required that the response rate approximate more than 40% of the population. Lower response rates may distort the interpretation and relevance of the research results. In this study, a response rate of 67.33% was achievable through regular follow-ups and distribution of the questionnaires through emails and social media platforms such as Whatsapp.

4.2.2 Sectors represented by participants

The participants were drawn from key sectors that play a critical role in the formulation of the NCSS. The survey brought experts from the Security sector (Military and National Intelligence Agencies)); the security sector represented 7.9%. 25.7% was Government Officers representation; this was comprised of experts from the ICT Ministries’, Departments’, and Legislative entities. 38.6% of participants came from the Private sector, and the industry represented experts from the Media fraternity, Telecommunications, Financial experts, and private ICT stakeholders.

The Academia comprised of Professors in the field of policy formulation, and experts from Research Centre’s, the academia had a 14.9% representation. Other views were drawn from the Civic Society (policy activists and advocacy groups); this group was 4% of the survey participants. Law enforcement Agencies, drawn from the National Police force, had 2% representation. 6, 9% represented Citizens' views.

Table 4: Number respondents based on sector representation

Sector participation and representation

Number of Participants	Sector
39	Private Sector (incl, Media, Telecommunications, ICT firms, and Finance)
25	Government (incl, Ministry, Department or any Public entities)
15	Academia - Experts hailed from, Universities, Colleges, Research Institutes)
7	Citizen
7	Security Sector (incl, Military or Intelligence Community)
4	Civic Society (Local NGO's, Activist, Lobby Groups or others)
2	Law enforcement Agency (Private LEA, Police, Judiciary)

In summary, the highest respondents came from the Private sector, Government, and Academia, in that order, this can be an indicator of how the Private sector is critical in matters surrounding NCSS. Responses from the Academia, signifies, how research and education in cybersecurity at an operational and strategic level is considered valid and of importance to developing countries.

4.3 Understating the Cybersecurity environment

The second set of questions was meant to give the researcher an understanding of the respondents who have been involved in cybersecurity matters in their countries. This set of questions would allow the researcher to get experts to view from developing African Countries on their direct/indirect involvement in Cybersecurity matters and knowledge or existence of cybersecurity legislature.

4.3.1 Heard of any Cybersecurity incidents from their country?

The question was meant to ascertain the level of knowledge or hearing of cybersecurity incidents from their countries, incidents such as hacking, credit card fraud, and identity theft, or any cybercrime incident. The question was set as a scale of 5 with one being never heard of any incident at all, two being slightly heard, three being moderately heard, four being has heard, and five being heard a lot of incidents.

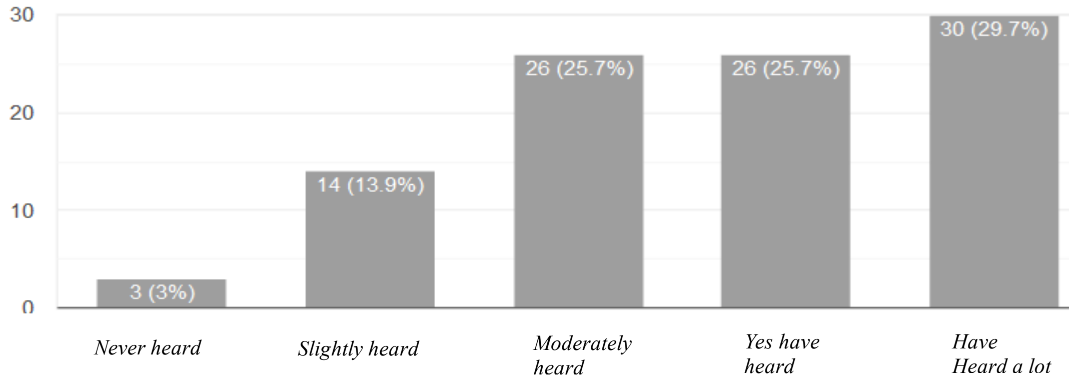


Figure 2: Responses from the respondents on having heard any cybersecurity incidents

From the responses, 29.7% said they have heard a lot of incidents relating to cybersecurity from their country. 25.7% of the respondents said yes, they have heard of some incidents relating to cybersecurity, and 25.7% said they have moderately heard of cybersecurity incidents from their countries. 13.9% of the respondents have slightly heard of cybersecurity incidents, while 3% of the respondents said they have never heard of any cybersecurity incidents from their countries.

Reviewing literature by Bada & Agrafiotis (2019), it is evident that cybersecurity awareness is an essential step in the fight against cybersecurity threats in developing countries. For that reason, it is necessary for any African country that intends to implement interventions in this area to have a holistic understanding of the level of cybersecurity awareness in that country. From the obtained results, with a mean of 3.66 and a median of 4, this can indicate that the respondents "have heard" about cybersecurity issues in their countries. This supports literature from other researchers, highlighting that there are existing efforts in Africa coordinated, through, Government, Industry and communitywide efforts to inform and educate citizens on safe and responsible use of computers and the Internet so that the inherent risks can be minimized.

4.3.2 Cybersecurity state in their respective countries

The question was meant to get an overview understanding of the participants to view the current state of cybersecurity in their country. The question was set on a scale of 1-5, with one being not safe and secure, two being slightly safe and secure, three being moderately safe and secure, four being safe and secure, and five being very safe and safe.

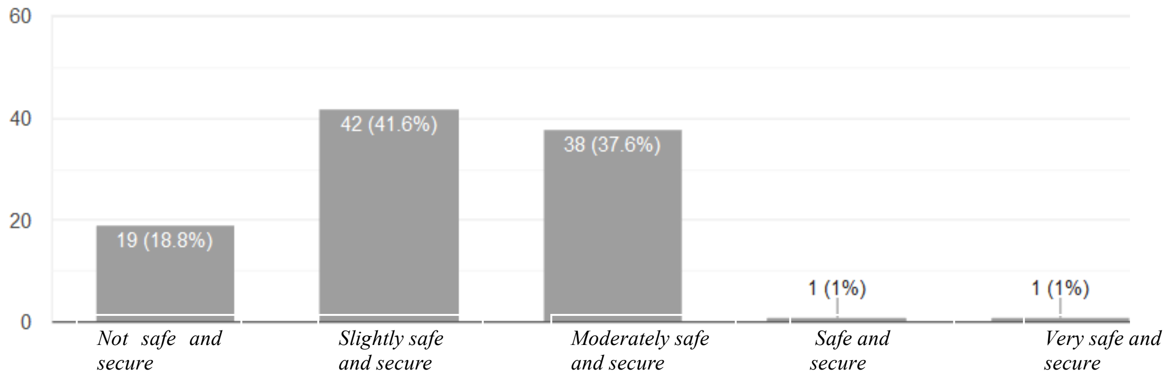


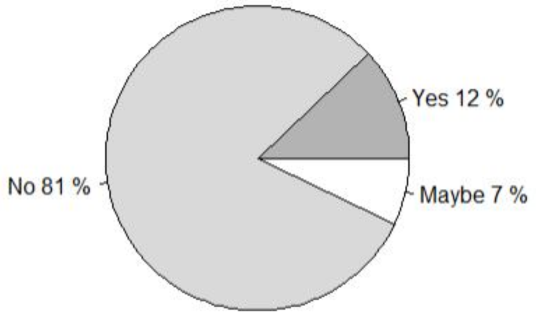
Figure 3: Responses from the respondents on how they view the cybersecurity status

From the responses, 18.8% indicated that they are not safe and secure concerning cybersecurity from their country. In comparison, 41.6% of the respondents said they view the cybersecurity state as slightly safe and secure, while another 37.6 % of the respondents said they view that state of their country as being moderately safe and secure. 1% of the respondents consider the state as safe and secure, while another 1% of the respondents view the state as very safe and secure.

Hamadoun Toure, an ex-secretary-general of the International Telecommunications Union (ITU), indicated that "At the moment, cybercriminals see Africa as a haven to operate illegally with impunity" (Kshetri.N, 2019). The results from this survey support the statement by the ITU ex Secretary-General, Hamadoun Toure. The respondents from this question have a statistical mean value of 2.232 and a median of 2.00, which indicates that the cybersecurity status of African countries is slightly safe and secure.

4.3.3 Respondents participation in cybersecurity issues from their country

The question seeks to bring an understanding to the study, if the respondents had been involved or participated in any cybersecurity issues in their country, also the question would help the researcher to understand which sector has the highest number of respondents who participate in cybersecurity issues in these countries.



Key:

Yes: -Has participated in cyberserity issues
No: -Has not participated in cybersecurity issues
Maybe: -Not sure, might have

Figure 4: Pie Chart showing responses on if the respondents have participated in cybersecurity issues

The question was set in a manner where respondents had to choose from three options, the first option being yes, meaning that the respondent has fully participated in cybersecurity issues from their country, option two being no, saying the responded has not participated in any cybersecurity issues from their country, and the last option being maybe, to indicate that the responded maybe has participated, but without full knowledge or understanding of the cybersecurity issues, they have participated in. From the survey, 81% indicated that they have not participated in cybersecurity matters, 12% of the respondents indicating that yes, they have participated while 7% indicating that, maybe they might have participated.

The issue of participation and involvement, which is consistently echoed in recommendations from various authors on cybersecurity in Africa, the study results have shown that experts who took part in this survey still view as not being involved in cybersecurity issues, in particular national policies and strategies. The chairperson of the SADC expert's group on CIRT and PKI highlighted that there was an urgent need to provide the SADC Member States "with a model strategy that could be used in harmonizing the cooperation, coordination of cybersecurity issues" (SADC, 2018).

As highlighted in Table 5 below, the highest numbers of respondents whose responce was No (Having not participated in Cybersecurity issues), where draw from the Private sector, Academia and Governement. According to Karake, Rana & Ayas (2017), "Any cybersecurity policy document will fall short if it does not address the role of the private sector in securing cyberspace."

Table 5: Number respondents who haven't participated in Cybersecurity matters in their Countries

Sector Participation		
Sector	Participation	Respondents selected No
Private Sector (incl, Media, Telecommunications, ICT firms, and Finance)	No	27
Government (incl, Ministry, Department or any Public entities)	No	22
Academia (incl, Universities, Colleges, Research Institutes)	No	15
Citizen	No	7

4.3.4 Knowledge and understanding of Cyber Law or any legal instrument(s)

This question was meant to get an overview of the respondents' knowledge or understanding of any existing (if any) cyberlaw(s) or any legal instrument(s) concerning cybersecurity from their country. This question is modeled from the GCI Legal pillar on the cybersecurity conceptual framework (ITU, 2019).

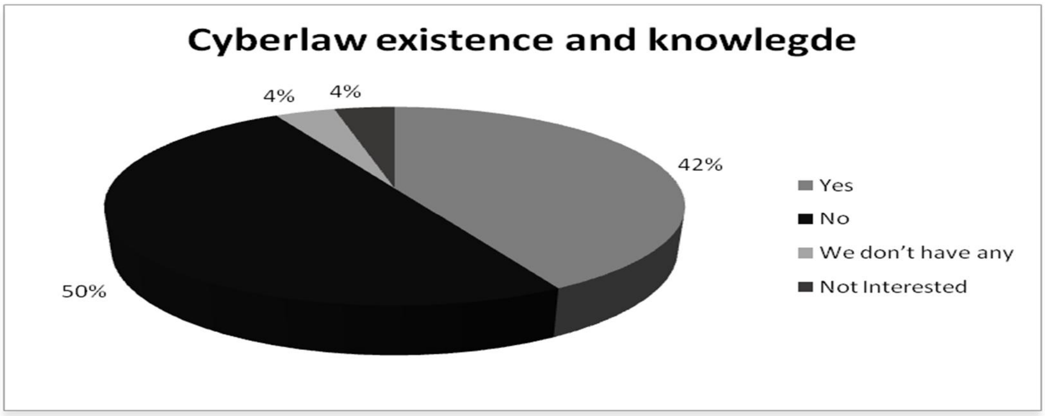


Figure 5: Pie Chart showing responses to the knowledge and understanding of the existence of cyber laws on their country

50% of the respondents did not understand the existing cyber law(s) or any cyber legal instrument(s), 4% highlighted that they did not have any cyber law(s). In comparison, another 4 % highlighted that they were not interested in cyber legal issues and, 42% understood the existing cyber law(s) and cyber-related legal instrument(s) from their countries.

As a way of providing a measure of these results, the research is guided by the Global Cybersecurity Index (GCI), According to the African GC1 sub-report of 2017 report, Africa had an average score of 0.29, in respect to the legal pillar (GCI, 2018) being represented. The table below supports the expert's views that African developing countries are slowly making strides in cyber legislation, as from the 2012 SADC adopted Model Law on computer crime and cybercrime (ITU, 2013).

Table 6: Average score of the African Countries under this study as of 2018 (GCI)

	South Africa	Botswana	Zambia	Malawi	Mozambique	Zimbabwe	Tanzania
CGI (2018)	0.652	0.440	0.436	0.275	0.158	0.186	0.642
Average CGI- as of 2018	0.398 (*Average CGI of the 7 Countries under this study as per 2018 GCI score)*						
Average GCI of 2020 - from this Study	0.416 *(Overall percentage score of respondents with knowledge, understanding, and acknowledgment of cyber legislature in their countries)*						

4.4 NCSS Focus Points and Improving Cybersecurity

The third set of questioning was driven by the researcher need to understand the respondents' view on the focus areas they would want to be prioritized when formulating NCSS. Another question was set to help the study in understanding the current cybersecurity status in the respective countries which are part of the survey. In this question, the respondents had to highlight how best in their knowledge, the cybersecurity status in their country can be improved. The last question from this set was meant to get an overview of respondents views in adopting already set models and standards against developing own models and standards ideal for their developing African nations.

4.4.1 Focus pillar(s) in NCSS formulation

The question was, “In your view, your National Cybersecurity Strategy should focus on which pillars, they had the option of selecting or suggesting.” The focus pillars options were (1) Citizen's Data and Information Security, (2) National Defense and Security, (3) Economic Security and Development, (4) Protect and safeguard Human & Civic rights and, (5) Economic Cybercrimes. In coming up with the focus pillars, the author was guided by the Collier's (2013), four domains of Cybersecurity which are; the Physical domain, Information, Cognitive and Social domain (Collier ZA, 2013).

Table 7: Number of times responded selected the same set of primary focus areas

National Cybersecurity- Focus Pillars Selected	**Frequency**
Citizen's Data and Information security; National Defense and Security; Economic Security and Development; Protect and safeguard Human & Civic rights	27
Citizen's Data and Information security; National Defense and Security	12
Protect and safeguard Human & Civic rights	12
Citizen's Data and Information security; National Defense and Security; Protect and safeguard Human & Civic rights	7
Citizen's Data and Information security	6
Citizen's Data and Information security; Economic Security and Development; Protect and safeguard Human & Civic rights	6
Citizen's Data and Information security; National Defense and Security; Economic Security and Development	6
National Defense and Security	6
National Defense and Security; Economic Security and Development; Protect and safeguard Human & Civic rights	4
Citizen's Data and Information security; Economic Security and Development	3
Economic Security and Development	3
Economic Security and Development; Protect and safeguard Human & Civic rights	3
Citizen's Data and Information security; Protect and safeguard Human & Civic rights	2
Citizen's Data and Information security; National Defense and Security; Economic Security and Development; ECONOMIC CYBER CRIMES	1
National Defense and Security; Protect and safeguard Human & Civic rights	1
Total Respondents who answered the question	**99**

Table 7 above shows the frequency a particular focus pillar or a combination of pillars were selected by the respondents, and Figure 6 below shows the aggregate responses based on each focus pillars indentified from the survey.

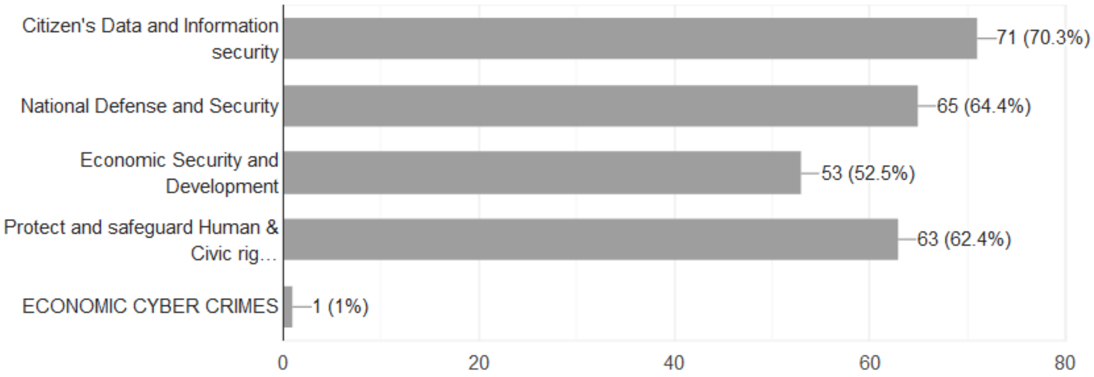


Figure 6: Frequency, the respondents, chose a primary focus pillar

From the survey data, seventy-one (71) of the respondents selected an option that included the need for a NCSS primarily focusing on Citizen's data and information security and representing 70.3% of focus strength. Sixty-five (65) respondents highlighted that they would expect a NCSS that concentrates on ensuring National Defense and Security; this represented 64.4% focus strength. Sixty-three (63) respondents indicated that they would prefer a NCSS that primarily focuses on Protecting and safeguarding human and civil rights; this representing a focused strength of 62.4%. Fifty-three (53) respondents (52.5%) highlighted that focus should be on ensuring economic security and development. In contrast, 1% of the respondent indicated that a NCSS should focus on ensuring and safeguarding against economic cybercrimes.

Literature review from other researchers, namely Bada et al. (2019), after surveying six (6), African states, the author indicated that cybersecurity awareness should be amongst the top focus areas for African countries as a way to mitigate effects of cybersecurity.

4.4.2 Improving the Cybersecurity environment

The question was, "How can your country improve from the current cybersecurity status? The question was meant to find out what the respondents think is lacking in their country when dealing with the challenges posed by cybersecurity and this improvement should be a core element in the NCSS formulation process.

Table 8: Response on which area to focus on (in rank) so as improve the Cybersecurity environment in their countries

Improvement focus area	**Number of Respondents**	**Percentage representation**	**Improvement need(s) ranking**
Cybersecurity Awareness Education and involvement of the Citizens	73	72.3%	First (1)
Improving and Securing Technical Infrastructure in the Country	60	59.4%	Second (2)
Enact, Improve or Update Laws and Legal Framework	45	44.6%	Third (3)
More Cooperation between Public and Private Sectors	25	24.8%	Fourth (4)
Improving Regional and International Cooperation	18	17.8%	Fifth (5)

Interesting responses from the survey participants highlighted that most respondents view having cybersecurity awareness education and involvement of the citizens, as a top key priority in improving the cybersecurity environment from in African developing countries.

4.4.3 NCSS Model for developing countries

The question "In your view, how best can African developing countries improve the cybersecurity situation.?" The question was meant to understand how respondents view the formulation of a NCSS by using any of the three options presented. The first option was the use of currently developed international standards and models, the second option being, for developing countries to establish their standards and models whilst the other option included the combination of both options (Mixed/Hybrid approach).

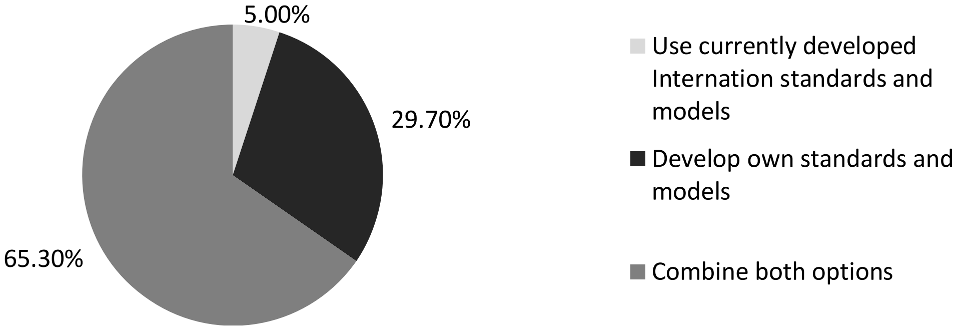


Figure 7: Pie chart, showing respondents ideal approach to NCSS model

From the survey, sixty-six (66) respondents (65.30%), highlighted that the cybersecurity situation in developing African countries could be improved by combining both options. In comparison, thirty (30) respondents (29.70%), indicated that the cybersecurity situation can improve if they develop their own standards and models whilst five (5) respondents (5%), highlighted that the cybersecurity situation can still be improved without developing own models and framework. In further analysis, the 29.70% that indicated that Developing own standards and models would be the ideal approach, was mainly respondents from Zimbabwe (66.6%) and South Africa (20%). From the 30 respondents, 20 highlighted that they have not participated in Cybersecurity issues, which can be attributed to the response of developing own models and standards.

Table 9: Top 2 countries, whose respondents selected "Develop own standards and model that suit developing countries" and No participation in Cybersecurity

Country	Model_Choice	No Participation

Country	Model_Choice	No Participation
Zimbabwe	Develop own standards and models that suits African developing countries.	17
South Africa	Develop own standards and models that suits African developing countries.	3

4.7 Qualitative Analysis to Study

According to Braun and Clarke (2006), the term thematic analysis refers to the method of identifying, analyzing, and reporting patterns (or themes) within dat. From the data methodology employed for this study, the researcher adopted a blended approach (deductive and inductive approach) to analyze the survey data. The inductive approach is based on 'open coding,' meaning that the researcher freely created the categories or themes based on the content. At the same time, the deductive content analysis requires the prior existence of a theory to underpin the classification process.

4.7.1 Verification of Qualitative methods

Irrespective of the methodology used for any research work, it is always recommendable to consider the aspect of reliability and validity. The reliability of the method refers to the question of whether if a different researcher repeats at another time and place would come to the same result as this study (Silverman 2006). Achieving reliability is especially difficult in qualitative studies. Taylor and Bogdan (1998), says that it is not possible to achieve perfect reliability if we are to produce valid studies of the real world. Additionally, qualitative studies emphasize validity, and they "are designed to ensure *a close fit between the data and what people say and do*" (Taylor and Bogdan 1998).

Another important concept for research in social science is validity. The question of validity is the question of whether a study accurately measured what it intended to measure (Silverman 2006). In qualitative studies the answer to this question is less straight forward than in quantitative research. Hence, for the validity of a qualitative study, it is crucial that the observations made, fit to the theories that are developed out of them (Bryman 2008).

For this study, a structured questionnaire (survey), as described by Pole and Lampard (2002), seemed to be a suitable method since a structured survey guide made it possible to keep orientation during the process respondents were filling out the survey. Furthermore, the structuring made sure that important theoretical issues were covered in the questionnaire, and it further facilitated analysis using the inductive approach according to categories/open coding created by the researcher.

The themes (codes) that have been identified from this survey and supported through literature were; Multistakeholder approach with citizen involvement, Data and information protection, The protection, and safeguarding of human and civil rights, National defense and security and the last theme was Economic security and development. From the literature review, Culture has emerged as one fundamental theme in this research and has been noted that national culture, beliefs, and ethos play an essential role in the approach, formulation, and implementation of a NCSS.

Multistakeholder approach and Citizen involvement- Seventy-one (71) of the respondents from this study indicated that for a successful NCSS process, a multistakeholder approach be adopted, incorporating and recognizing all the critical stakeholders involved in the process. Another question from the survey supported this were seventy-three (73) participants equally noted that to improve the cybersecurity environment, there is need to prioritize cybersecurity awareness, education and, citizens' involvement during all process. In support of the study results, Bada et al., (2019) further noted that under the deductive theme analysis, “it is evident that a national program for cybersecurity awareness is critical. In many cases, stakeholders mentioned that ‘lack of awareness is an institutional problem, not a user problem’ and also that ‘a proper cyber awareness program is needed.’”

Data and Information protection - Data and Information protection was another theme that was noted in this survey. For an effective cybersecurity environment, a NCSS should be anchored on ensuring that citizens' data and information in the private and public domain is safe and secure. Respondents expressed that they do not feel safe and secure in the cyber domain. Another question from the survey revealed that 59.4% of the respondents highlighted the need to improving and securing technical infrastructures in their countries.

Protection and Safeguarding of human and civil rights- This survey has brought one topic already seized by policymakers, the topic on human rights, privacy against national security and defense. This theme is aimed at strengthening fundamental rights and public freedoms as enshrined in their constitutions. According to Perez, (2020), personal privacy is protected by law, hence outweighs national security and subsequently national security measures don’t always “necessarily” increase security to the nation.

Economic Security and Development- African is a developing continent, which is slowly moving towards a digital economy according to a recent publication by the Adomako et al., (2018). Per estimates, cybersecurity costs African economies a total of over US $1 billion every year. This narrative gives support to respondent’s views that developing countries ought to focus on ensuring that the NSCC framework accords appropriate focus to the economic security and development theme.

Culture- In 2002, Jeffrey Lantis compiled a large body of theories on strategic culture that relate to state strategies and policy formation. From his work Lantis stated that, "the theory of strategic culture has evolved in recent years in explaining national security strategy formulation and the influence it has on state behavior." Social psychologist Geert Hofstede defined culture as a "collective programming of the mind." Various strategic cultural dimensions can be used to define the conceptual view of how developed nations (Patton .DE, 2016). Qualitative approach used in this subject matter, has noted that Culture is of paramount importance in the NCSS process. In the next chapter (Analysis) the study will highlight how culture contributes and determines the approach taken in NCSS formulation and implementation.

4.8 Chapter Summary

This chapter reported on the research results which emerged from the survey and literature review. The obtained results have been presented using both qualitative and quantitative approaches to align, support, or offer new narratives from the respondent's views and induce meaning and interpretation against those proven theories or past research work. The chapter noted the themes which need to be incorporated or addressed to ensure that the research questions are answered satisfactorily, and still achieving the set objectives of this research work.

CHAPTER 5: ANALYSIS AND DISCUSSION

5.1 Comparative Analysis

Analysis of the results reported in the previous chapter are explained and discussed in this chapter. Answers to the research questions will be provided, lastly the relevance and study contributions are also highlighted.

Table 10a: An analysis matrix of approaches, needs, and challenges of the developing and the developed countries under this study

Criteria		Country					
		Developing Countries	Developed Countries				
		NCSS focus areas African from Developing Countries	USA (2018)	UK (2016)	China (2016)	S.Korea (2019)	Australia (2016)
1	Strategic focus/ pillars	-Citizen's data and information security	✓	✓	•	✓	✓
		-National Defense and Security	✓	✓	✓	✓	•
		-Protecting and safeguarding human and civil rights	✓	✓	•	✓	•
		- Economic Security and Development	✓	✓	•	✓	✓

2	**Major Challenges addressed during NCSS formulation**	-Cybersecurity Awareness Education and involvement by the Citizens	✓	✓	●	✓	✓
		-Improving and Securing Technical Infrastructure in the Country	✓	✓	✓	✓	✓
		-Enact, Improve or Update Laws and Legal Framework	✓	●	●	✓	✓
		-Ownership and Responsibilities	✓	✓	●	✓	✓

Notes:

Explicitly ✓ Item was fully discussed and is a key element of the NCSS

Implicitly ● Item was discussed in the NCSS but is limited set of related actions/activities

Table 10b: An analysis matrix of approaches, needs, and challenges of the developing and the developed countries under this study (Continued)

Criteria		Country					
		Developing Countries	Developed Countries				
		NCSS focus areas African from Developing Countries	USA (2018)	UK (2016)	China (2016)	S.Korea (2019)	Australia (2016)
3	**Models, approach and standardization**	-Combining current models and developing own standards and models	✓	✓	●	✓	●
		-Developing own Model and standards	●	✓	✓	●	●
		-Using already developed models and standards	●	●	●	✓	✓
4	**Stakeholder**	-Multi-stakeholder	✓	✓	●	✓	✓

	Involvement	approach					

Notes:

Explicitly ✓ Item was fully discussed and is a key element of the NCSS

Implicitly • Item was discussed in the NCSS but is limited set of related actions/activities

5.2 What makes up NCSS, Developing Countries Perspective

Conceptually, a strategy is defined as the relationship among ends, ways, and means. Ends are the objectives or goals sought, and the means are the resources available to pursue the objectives, and ways or methods are how one organizes and applies the resources (ITU, 2018). Each of these components suggests a related question. A NCSS seeks to model the relationship between national approach, culture and distinctive notion, the goals, the available resources, and the methodology to be employed, which a continuous process is striving to fit national information infrastructures within its changing environment into a trustworthy and resilient domain. Experts from developing African countries, according to this research, have identified some of the key pillars and focus areas that should guide the formulation of their NCSS.

Table 11: Responses from the African experts on which focus areas should guide the approach

Focus areas	Number of	Percentage	Priority
Citizen's Data and Information security	71	70.3%	One (1)
National Defense and Security	65	64.4%	Two (2)
Protect and safeguard Human & Civil rights	63	62.4%	Three (3)

Economic Security and Development	53	52.5%	Four (4)

From the table above, African experts are advocating for a NSCC model that gives higher priority to citizen's data and information protection. From the responses, it can be noted that information security and privacy are of paramount importance. Secondly, there is an emphasis on the need to safeguard the nation through national defense and security. Thirdly the survey has revealed that protection and safeguarding of human and civil rights should be a priority focus area. In the the proposed framework, the study will incooperate these focus areas amongst other principles.

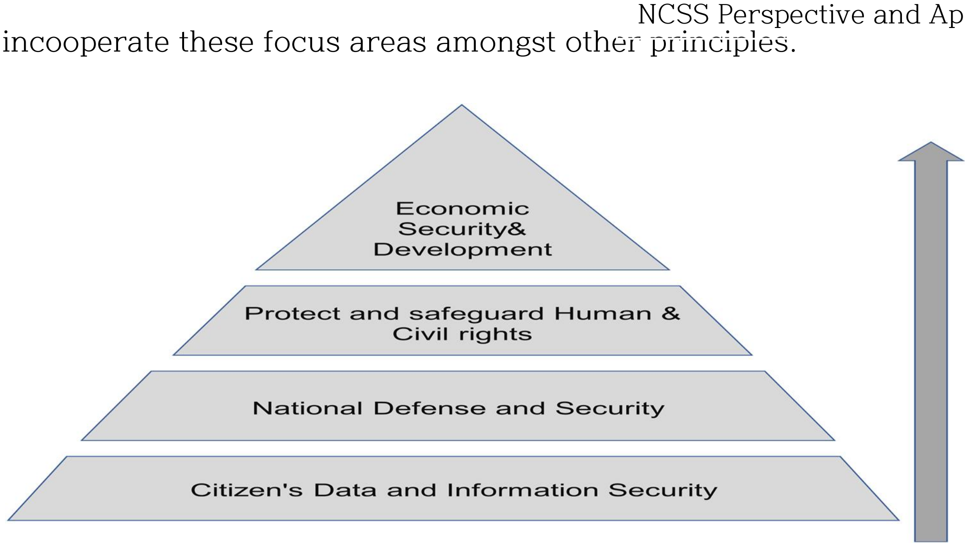

NCSS Perspective and Approach
Economic Security& Development
Protect and safeguard Human & Civil rights
National Defense and Security
Citizen's Data and Information Security

Figure 8: NCSS approach & perspective from developing African countries experts

Accordingly, the national perception must then be conceptualized relative to the nation's position within an international strategic context. Also, an understanding of the political, social, cultural, and economic environment is imminent when adopting NCSS models in cybersecurity.

5.3 Culture in NSCC formulation

This section of the thesis seeks to analyze cultural research work on the developed countries under this study, i.e., USA, UK, Australia, South Korea, and China. Highlights will also include cultural dimensions from developing African countries. In this analysis the author intends to show how culture is applied or how it influences the NSCC formulation and implementation.

African countries, from a historical point of view, have endured an era of colonialism, imperialists, and capitalistic societies. Post-independence, Africans have adopted a socialistic cultural approach, where all means are in the hands of the people, shared views, and ideals. Mugumbate .J (2013), wrote "the African socialism is a cultural belief on sharing and working in harmony together on the bases of humanity, 'I am because we are,'" In this view, African experts believe that one of the cornerstones in shaping cybersecurity culture is knowledge, awareness, and involvement Metalidou (2014).

The United States of America is a task-oriented nation that places high values on goals and measures (Hofstede, 2002). Zachary TM, (2000), further added that "USA's cultural values connected with effort and activity ads to the American belief that 'it is better to do something than to sit back and do nothing.' The American culture values technology, innovation, individual initiatives, and embraces scientific advancement to secure national interests. In this regard, the US views and asserts itself as a global powerhouse in cybersecurity, leading, giving guidance and, directions to other nations. However, another researcher argues that the US's strategy focuses on symmetrical and conventional enemies rather than an asymmetrical enemy (Gray.C, 2018).

The culture in the United Kingdom (UK) is rooted in the country's long history, that is influenced by elements of its countries i.e. England, Scotland, Wales, and Northern Ireland. The UK adopted a culture of socialism, where the economic system is characterized by social ownership, control of the means of production, cooperative management of the economy, and a political philosophy advocating such a system across the EU. In application to NSCC, the UK culture, being a central force in the EU bloc, has formulated or led the formation of strategies and cyber legal instruments as a guide for other EU member states.

The Ministry of Home Affairs in Australia (2019), described the Australian society as one that values respect, the freedom and dignity of its individuals, freedom of religion, commitment to the rule of law, democracy, equality whilst embracing mutual respect, tolerance, fair play and, compassion for those in need or in pursuit of the public good. The Australian culture, like the UK, is a close ally to the USA and a member of the FIVE eyes arrangement (Pfluke. C. C, 2019). The Australian cybersecurity culture extends into military, national, and homeland security, emphasizing the need for strong national leadership, responsibility-sharing, and risk management (Barbas. JMA, 2015).

South Korea- Kim. HS and Newton. J, (2012), highlighted that the legacy of Confucianism remains a fundamental part of Korean society, that shapes the moral system, way of life and, social relations between old and young. The dynamicity in South Korea has seen it becoming among the world leaders in ICT, with over 85% of South Korean citizens connected to the Internet. ROK's approach has played a significant role in the development and revolution of its commerce and trade. However, part of its NCSS formulation guidelines is also anchored against the history and culture ramification emanating from the diplomatic standoff against the Democratic People's Republic of Korea (North Korea), which has transcended into a national cybersecurity matter for ROK (Ministry of National Defense, 2016).

The Peoples Republic of China (ROC) is historically known and perceived as a peace oriented nation that is driven by morality, concepts of harmony between information and weaponry. (Li Bingyan, 2020). Johnson Iain A, (1995) noted that

China exhibits tendencies of a controlling, politically-driven defensive approach as part of its culture. The attribute of secrecy in the Chinese is inherent in authoritarian-type of Governments where they must keep broader control over information to remain and consolidate power. In NSCC, this auspice of secrecy is seen in the information network infrastructure in China, from "the Great Firewall", Internet censorship and the security monitoring/public surveillance program instituted under the Golden Shield project (Ensafi. R & Winter. P, 2015).

The basis of the China's strategy is informatization i.e., the transformation from a traditional mechanized force to an information-based one mirroring the goal of expansion of the information society within China. China's strategic culture is heavily influenced by the how they value information. Information flow is controlled by the Government and is a function of the high power as evident in Chinese national culture and history (Patton. DE, 2016).

However, currently available literature on national cybersecurity strategies has lacked a deep analytical evaluation of how the culture, beliefs, and norms play a critical role in the trajectory of the state's intended goals and principles in the cyber domain or NCSS formulation. This study has analyzed some of the cultural traits from the USA, UK, Australia, South Korea, China and, that of African countries. In summary, culture influences the framework and approach a country undertakes during NCSS formulation process,

5.4 Mapping NCSS to Culture

Many factors influence a country's strategic culture, from the analysis made from the five (5) developed countries, a nation's chosen approach to a variety of issues for example culturally-driven, may significantly impact on its cybersecurity approach and strategy. The matrix diagram below of the various strategic cultural dimensions are meant to be viewed as a continuum, as opposed to binary concepts, applicable to the development and implementation of national strategies and doctrines. These concepts adopted from Siedschlag. A, (2018) have been applied to this research work.

Privacy vs. Security- This concept focuses on the degree to which security is valued within the nation. High security attributes corresponds with strong secrecy, denial of access, and a protection of information. Low security attributes indicate openness, accessibility, and a tendency towards disclosure of information, whilst a balance between secrecy and openness indicates moderate approach.

Government vs. Private Sector-This dimension is the evaluation of Government and Private sector involvement or participation in NCSS. A state where there is no coordination, cooperation and little involvemetnt between Government and Private sector, tends to have a '*less*' multistakeholder approach whilst *'More'* indicates strong existence of multistakeholder approach in NCSS processes.

Military vs. Civilian mission-The Military dimension conceptualizes the cyberspace as an information space and domain for warfare, with the view that political, social and, economic stability are top issues of national security. In the civilian missions, civilian agencies take the leading role in protecting and safeguarding critical infrastructures, governance and, general oversights of cybersecurity environment.

Centralized vs. Dispersed- The centralized dimension, has established a central autonomous authority at national level to coordinate, implement and govern all cybersecurity operations in the country, whilst a dispersed dimension has established and distributed its authority to various agencies or centres to coordinate, implement and govern cybersecurity operations within their environmnent.

Table 12a: Mapping Cultural approach to NCSS

	Privacy vs. Security	**Government vs. Private Sector**	**Military vs. Civilian mission**	**Centralized vs. Dispersed**
USA	Strong Security and moderate Privacy	Less Government role	Mixed mission	Dispersed
UK	Strong Security and strong Privacy	Less Government role	Civilian mission	Centralized
China	Strong Security low Privacy	Strong Government role	Military mission	Centralized

Note

a) **Privacy vs. Security**- *Strong, Moderate, Low*

b) **Government vs. Private Sector**-*Less, Mixed, More*

c) **Military vs. Civilian mission**-*Military, Mixed, Civilian*

d) **Centralized vs. Dispersed**- *Dispersed, Centralized*

Table 12b: Mapping Cultural approach to NCSS (Continued)

	Privacy vs. Security	Government vs. Private Sector	Military vs. Civilian mission	Centralized vs. Dispersed
S.Korea	Strong Security and strong Privacy	Mixed approach	Civilian mission	Centralized
Australia	Strong Security and moderate Privacy	Less Government role	Mixed mission	Dispersed
African Developing Nations	Strong Security and moderate privacy	Mixed approach	Civilian mission	Centralized

Note

e) Privacy vs. Security- *Strong, Moderate, Low*

f) Government vs. Private Sector-*Less, Mixed, More*

g) Military vs. Civilian mission-*Military, Mixed, Civilian*

h) Centralized vs. Dispersed- *Dispersed, Centralized*

5.5 Answers to Research Questions

1. Can developing African countries directly adopt current NCSS proposals from foreign groups?

This is the main research question; the study has shown that African developing countries do not need their cybersecurity models and standards to address the identified cybersecurity challenges, hindering the designing and implementation. As stated in the research assumption (hypothesis), that "developing countries need own frameworks or models," from the survey 65.3% of the survey respondents, indicated that developing countries do not need new frameworks, but Africa needs to adopt a combined approach (hybrid) that allows for takes own models, frameworks, methods (cultural-based) being integrated with other currently developed international standards and models as a way to address the cybersecurity challenges in developing countries adequately.

Past research done in 2013 by Dr. Newmeyer, done on a case study of Jamaica, highlighted that "developing nations have been slow to develop and implementing cybersecurity strategies despite the growing threats to governance and public security," despite the study being from 1 (one) nation, it concluded that there was a need for the development of own specific standards and models for developing countries. This notion has not been supported by this study or answered by the main research question.

2. What is the major challenge, being faced by developing African countries in designing and implementing National Cybersecurity Strategies?

From the study done, based on opinions and views from the surveyed cybersecurity experts, the major challenge noted is the lack of cybersecurity awareness, education, and the involvement of citizens at the national level. This challenge subsequently affects the designing, formulation, and implementation process of NCSS. This challenge was noted by 72.3% of the respondents. Results from other questions can support this challenge on participation and involvement were 29.7% of the respondents highlighted that they had heard a lot of cybersecurity incidents. In contrast, 25.7 have heard, and 25.7 have moderately heard about cybersecurity. Yet 80.8% of the respondents have not participated in any cybersecurity issue in their respective countries; see section 4.3.

The research assumption states that “developing countries need a framework or NCSS model that can ideally assist their challenges in formulating NCSS. The major challenge identified is the need for national cybersecurity awareness, education, and citizen involvement, which has a multi-stakeholder approach. This finding supports the work of Bada. M, (2019) concluded by highlighting that Governments do not have active national programs for raising awareness.
These extremely low ICT literacy levels hinder any design of cybersecurity campaigns, to be able to prepare and defend against threats emanating from the cyberspace.

African countries need to establish central authorities that will coordinate the existing ad-hoc efforts in awareness campaigns involving citizens at the grassroots level (Bada) From other NCSS that have been reviewed in this research, and this finding is attributed to the approach and how culture influences NCSS process. The ROC which has a military approach and based on a culture of secrecy will not most likely focus on citizens awareness and involvement, yet USA NCSS that has an openness approach has citizens involvement, awareness, and participation as one of its guiding pillars.

3. What are the Cybersecurity needs and requirements in African developing countries?

From the study and research conducted, it has revealed that these African developing countries need factors in the aspect of culture as a key element in the designing and implementation process of NSCC. As highlighted in section 5.4, culture defines and detects how a nation aligns with its values and beliefs in understanding the environment, its changes, and its people. From the mapping matrix, developing countries needs and requirements are summarized in the table below;

Table 13: Needs and Requirement for developing African nations from the survey

Cultural Practice	**Cultural Need**	**Primary focus areas from Survey**
Privacy vs. Security	Strong Security and moderate	1. Citizen's Data and Information security

	privacy	2. Improving and Securing Technical Infrastructure in the Country 3. Enact, Improve or Update Laws and Legal Framework
Government vs. Private Sector	Mixed approach	1. More Cooperation between Public and Private Sectors
Military vs. Civilian mission	Civilian mission	1. Cybersecurity Awareness Education and involvement by the Citizens. 2. Protect and safeguard Human & Civic rights
Centralized vs. Dispersed	Dispersed	1. More Cooperation between Public and Private Sectors

The study revealed that 18.8% of the respondents view the current state of cybersecurity from their countries as being not safe and secure. Yet, only 1% view the state of cybersecurity as being very safe and secure. This calls for a need for a strong security focus in the NSCC formulation. The 80.8% of respondents highlighted that they had not been involved in any cybersecurity-related matters, considering that the sample population took an inclusive multi-sectoral approach.

The study hypothesis highlighted the need for a new approach and model towards the formulation of a NCSS in developing African countries. The needs and requirements, as indicated by the study can reveal that African do not need a new model or approach, as, during the literature review, it has highlighted these needs and requirements have shared common themes. In summary, the study has highlighted and answered questions on the significant challenges, needs, and requirements for developing African countries to be able to design and implement a NSCC that can be able to best counter current and future cyber-attacks and other cybersecurity matters.

5.6 Chapter Summary

The analysis of the results reported in the previous chapter have been explained and discussed in this chapter. The research questions for this study have been answered using the results obtained from the survey. In collaboration with past work and literature review, the set hypothesis has been answered for each research question. Developing countries do not need own models or standards but instead adopt a mixed hybrid approach that recognizes some of the set models, standards, and practices, yet formulating homegrown bassed approaches that cater to the needs and requirements, challenges highlighted through the research questions.

CHAPTER 6. CONCLUSIONS

This chapter proposes recommendations and best practices for use by policymakers. These recommendations are based on the study results, whilst others are in support of past research work. A newly proposed NSCC framework for developing countries will be discussed as part of the recommendations, The last section of the includes the future work intended in order to further explore and provide a wider perception to this study.

6.1 NCSS Best Practices

Below are some considerable best practices for adoption;

- Not a single entity/ nation is able to address cybersecurity challenges on its own.

- Governments to take a shared responsibility approach in adopting and developing best practices, technology, compliance, regulation and many more measures. This would serve as an incentive to persuade other stakeholders to do the same, and foster a multistakholder approach, which the study has releaved.

- Note that there is no absolute security in an information system environment (cyberspace), hence efforts to deter, mitigate and minimize effects of cyberattacks.
- Framework for coordinating, developing and implementing a national cybersecurity culture that is derived from the nation's culture, values

and ethos, should be employed from Organisational to Governmental institutions.

- The success of the NSCC depends upon the involvement and participation of all stakeholders, who are the ultimate beneficiaries of a safe national cybersecurity environment or in turn the ultimate victims of an unsafe national cyber environment.

Every nation has to choose the most effective approach and best practices to address cybersecurity challenges. In the case of South Korea an inter-agency committee is headed by the National Security Office, with membership from various Governmental bodies, information security experts, private sector and, citizens participation. In the case of developing countries the study revealed that a holistic approach would be ideal which brings together relevant stakeholders, to create and orchestrate the NCSS whilst paying attention to the current and future needs in cybersecurity.

6.2 NCSS Recommendations

Following the study and analysis, the following recommendations are aimed at providing useful insights which should form baseline measures and actions that will assist in the formulation and implementation of the NSCC for African developing countries. The recommendations are being made in line with the themes, needs and requirements as highlighted through survey.

6.2.1 Invest in Capacity Building, Awareness and, Involvement

Capacity building seeks to improve the knowledge and expertise across the relevant areas in order to strengthen the capacity of countries programs towards cybersecurity. Appropriate management, awareness and involvement of all critical stakeholders, will facilitate monitoring procedures to continuous review and assessments of national programs and how they impact the overall NCSS. This important recommendation will ensure that for instance, cyber security educational programs are formulated at grass roots level; skills and expertise are harnessed from both Government and private sectors level. The holistic approach of involvement, being recommended for the African developing countries, will also address the issue on knowledge management; this involves the use of information collaboratively in the context of cyber security across both the private and public sectors and building capacity through knowledge sharing which is currently lacking in these countries.

Cybersecurity knowledge management offers benefits to the nation through improved processes, countermeasures and skilled competencies. The skills and training programs are necessary to bridge the gap in technical and managerial expertise. In developing countries, there is more training from the private sector than the government, attributed to financial constrains, hence in Government, LEA's, regulatory authorities and other critical infrastructure operators have deficiencies in this regard.

There is also the need for information security courses spanning to the citizens as adequate education and skills can foster and support economic development, and the skills will assist in implementing best practices highlighted above and safeguarding the cyberspace. At grass root levels fundamentals of information security and cyber security awareness to be incorporated into the national education curriculum at primary, secondary and tertiary institutions as a way of spreading knowledge to users and the citizens. The South Korean and Australian NCSS have made this particular recommendation explicitly in their strategies as one of its key guiding principles, as it fosters the involvement and participation by multi-stakeholders, and developing cyber-educational programmes for the citizens.

6.2.2 Cyber Security and Culture

The South African Government Gazette, (2015), acknowledged that a culture of cybersecurity is fundamental to the overall national security planning, as it promotes minimum cybersecurity measures, despite this call by the South African Government, there is an apparent lack of a practical plan or strategy to cultivate a cybersecurity culture. According to Patton (2016), existing literature on cyber strategies has been lacking a cultural analysis to determine the trajectory of nations' intended goals in the cyber domain. In support of this notion, this study has also revealed that a cultural strategy should be formulated and be a backbone to which the nations guiding principles are anchored upon.

In this respect it is recommended that developing countries, recognize strategic culture in the NCSS promise, with the mind that cybersecurity threat vector has evolved to include, state and non-state vectors. These threats being influenced by global interconnections, which are not limited by geopolitical boundaries, have a direct effect on the population and national culture.

6.2.3 Ratification of Legal Controls and Instruments

Legal jurisdiction over information and telecommunication technology and services is by far and away an urgent facet to secure the interconnected space. Over a period of time Africa national policy makers have remained passive observers and slow in responding to the transformation into 'information society' that the world has been undergoing, subsequently Cyber Laws and regulations have to transform as well. In the NSCC process, legal controls and measures, should be in place to evaluate the gaps existing in the current legal framework against other globally accepted standards, at the same aligning with the countries laws and constitution, African developing nations need to quickly re/align laws with the changes in technology, pass and enact cyber laws as a first priority in formulating the NCSS. The laws for the NCSS should enhance the balance between security vs privacy.

Legislation as part of the survey, 50.3 % of the participants highlighted that they do not have understanding, knowledge or existence of any cyber laws in their respective nations, Case in point, Zimbabwe had the first Cyber bill draft since 2016 and to date 2020, the bill is still to be enacted into Law. With the lack of such instruments, there no effective controls to safe guard and secure citizens data, information systems and critical infrastructure, making all these vulnerable and susceptible to cyber attacks.

Legal Authority, a key aspect of legislation is legal authority, the stakeholder responsible for the formulation of cyber laws. In developing countries, private stakeholders (ISP's, ICT companies, Academia) are the most leading group spearheading the inception of new Technologies (5G, AI, IoT, Big Data and, Block Chain), this puts them at a position to be an integral part of legal authority, in design, formulation and adoption. In the same regard, regional and International regulations from the cyberspace should be borderless; a comprehensive legislation can only be achieved through partnership with regional and international union's and other cyber security organizations and institutions across the world (SADC, AU, ITU and ATU).

6.2.4 Technical and Operational Controls

The technical and operational considerations include security control measures that will provide the necessary assurance in safeguarding the confidentiality, integrity and availability of critical National IT infrastructure and Information assets will require a security in-depth strategic approach measures (Kabanda, 2019). Some of the considerations include;

- Best practices as explained above in section 6.1, and also adopting some cybersecurity international practices from the developed countries and industries, these should ensure that every industry or organisation has minimum security requirements, standards and compliance.

- Comprehensive incident and response management structures, at government and private sector level. This should see a bottom up approach being implemented in regards to incidents and responses strategies.

- Continuous education, training and awareness for the private players, citizens, LEA's and Government, as part of the technical process, since they are the ones who have a direct interaction with cyber infrastructures.

From the survey, respondents indicated, as of the themes, being the Protection and safeguarding of Citizens data and information both from at private and public sector level. In order for these nations to be able to meet this focus area, sound technical and operational controls should be implemented. As indicated in Table 2, from the seven (7) African countries, four (4) have established CERT centre and three (3) countries are still to implement such technical and operational controls. This recommendation is also supported by all the five (5) developed countries that have been studied.

6.2.5 Proposed NCSS framework for Developing Countries

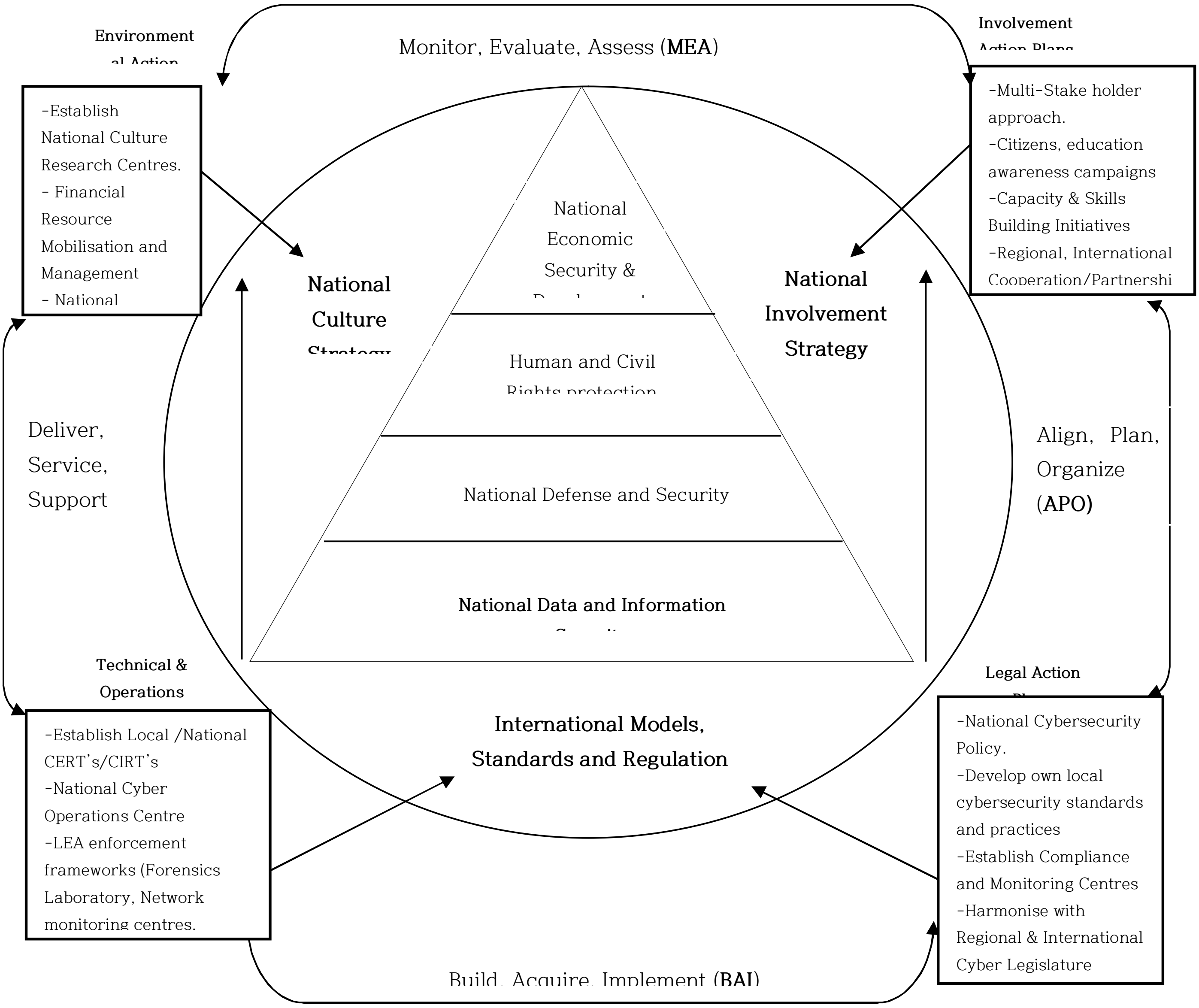


Figure 9: Proposed NSCC framework and model approach for developing countries

A model serves as a guide towards, the development and implementation process of NCSS aimed at reducing and minimizing cybersecurity risks and Threat, at the same time aiming to increase increasing security at human, technical, social and national level. This proposed model is a human construct that aids in understanding and conceptualizing actual systems and processes emphasizing the need for strong cybersecurity frameworks capable of managing the dynamicity in technology and escalating threat vectors. This model, is borrows some of the its principles from the Control Objective for Information and Related Technologies (COBIT) framework, that emphasizes the principle of Multi-stakeholder approach, and the application of a single integrated framework. As releaved by the study results and the hypothesis, African developing nations are recommended to employ an integrated model approach, anchored national data and information security and citizen's involvement.

6.4 Conclusion

This research as noted and supported the narrative given by various authors, that the African continent still remains the lowest ranked continent on cybersecurity preparedness, despite calls for the urgent formulation and implementation of relevant countermeasures. Generic challenges such as the lack of resources (Human and financial), high tech infrastructure, governance supported by sound legislature, national strategic planning (NCSS), still remain one of the leading challenges in dealing with the growing rate of cyber threats in the continent. Globally the use of ICT's and in particular the Internet has become a matter of strategic importance for human, social and, economic development. A free, open and, secure Internet is an engine for economic growth and social development that facilitates communication, innovation, research and, business transformation. Under this backdrop, it has become imperative for researchers and experts to interrogate whether the current models and approaches are working in developing countries or since they are predominantly modelled from developed nation's perspective, it's crucial a time for developing countries to start on focusing on their own models and approaches.

This research has been carried at a moment when the world is battling to contain the deadly COVID-19 pandemic; hence some of the proposed methods and methodologies could not be effectively carried out. However from the data obtained and analysed (qualitative and quantitative), the research was able to give satisfactory answers to the research questions and study assumptions. In order to give an in-depth understanding and background to the study, the study analysed and evaluated NSCC approaches from five (5) developed nations (UK, USA, South Korea, Australia and China). Research has identified that there is no "one size fits" all solution or model to challenges and approaches to NCSS. Since 2001, there is a growing body of literature on national cybersecurity strategy, which is at present aimed largely at developed nations. Cole et al. (2008), Tagert (2010), and Phahamohlaka et al. (2011) found that the models proposed by the developed nations and the international organizations failed to meet the needs and cyber requirement for developing African nations.

Based on the data obtained (experts opinion), this research work can conclude by highlighting that in order for African nations to urgently address the issue of NCSS development and formulation, an integrated (mixed) model approach should be applied, paying particular attention to the implication of national culture, multistakeholder and citizenry involvement, awareness and, education. Focuse areas include, improving the legislative, technical and, operational controls, protection of human and civil rights should be key guiding principles to a successful NCSS formulation and implementation process.

6.5 Future Work

This study was focused on a sample from African developing countries, as a way to understand how cybersecurity experts view as being the leading challenges deterring the design and, implementation of NCSS, as a way to counter cybersecurity threats. In the future, the researcher intends to further this survey to include other developing countries from other regions and continents, so as to get a wider and broader perspective, in understanding if the current models and frameworks are being used by developed countries, if they are the best models for developing countries, taking cognizance of the various environmental circumstances and cultural perception. In future studies various methods and methodologies will be applied so as to acquire enough quality study data that can be used to give a global perspective on an ideal model and framework approach for developing countries globally.

REFERENCES

Adomako, K., Mohamed, N., Garba, A., & Saint, M. (2018). Assessing cybersecurity policy effectiveness in Africa via a cybersecurity liabiluty index. *TPRC 46: The 46th Research Conference on communication, information and internet policy 2018* (p. 21). TPRC.

Ahmed, A. (2008). *Ontological, epistemological and methodological assumptions: Qualitative versus quantitative.* UK: University of Exeter.

Akerele, T., & Levanon, A. (2018). *Cyber threats on African subjects.* Herzliya: International Institute for Counter-Terrorism.

Allen, K. (2019). *Is Africa cybercrime-savvy?* Africa: ISS.

Andrea, R. (2017). *National cyber security strategy (NCS) toolkit.* New York: United Nations.

Angwe-Mbarika, E., Angwe-Akuta, E., Mong'oa, I., & Jones, C. R. (2011). Combating cyber crime in sub-Saharan Africa; A Discourse on law, policy and practice. *Journal of peace, gender and development studies , 1* (4), 129-137.

Annum, G. (2015). *Research instrument for data collection.* KNUST Gh.

Antonio, I. (2010). *Research methods made easy* (3rd ed.). Gweru: Mambo Press.

Atoum, I., & Otoom, A. A. (2017). A classification scheme for cybersecurity models. *International journal of security and its application , 11* (1), 109-120.

ARICILI, A.B., ÖZDAL, B., 2018. Çin Halk Cumhuriyeti'nin Siber Güvenlik Stratejilerinin Analizi. Güvenlik Strat. Derg. 14, 1–35. https://doi.org/10.17752/guvenlikstrtj.495748.

Australia's 2020 Cyber Security Strategy https://www.homeaffairs.gov.au/reports-and-publications/submissions- and discussion-papers/cyber-security-strategy-2020.

Azeus. (2019). *Cybersecurity risk management: Why it is needed and how to proceed.* USA: Convene.

BANDE S., (2018).Legislating against Cyber Crime in Southern African Development Community: Balancing International Standards with Country-Specific Specificities. *International Journal of Cyber Criminolog*y Volume 12 Issue 1 January-June 2018.

Carmen Cristiana Cirlig. *Cyber Defence in the EU- Preparing for cyber warfare?* 2014.http://www.europarl.europa.eu/EPRS/EPRS-Briefing-542143 Cyberdefence in-the-EU-FINAL.pdf

Chandran, E. (2015). *Research Methods: A Quantitative Approach.* Nairobi, Kenya: Starbright Services Ltd.

Choguill, C. L. (2005). The research design matrix: A tool for development panning research studies. *Habitat International , 29*, 615-626.

Cooper, D., & Schindler, P. (2016). *Business Research Methods* (10th ed.). New York: McGraw-Hill Publishing Company Limited.

Collier, Z.A., Linkov, I. & Lambert, J.H. Four domains of cybersecurity: a risk-based systems approach to cyber decisions. *Environ Syst Decis* 33, 469–470 (2013). https://doi.org/10.1007/s10669-013-9484-z.

Dhaouadi, R. (2019). *Cyber crime/ North Africa should fight online crim the right way.* North Africa: ENACT.

Dlamin, I., Tute, B., & Radebe, J. (2018). *Framework for an African policy towards creating cyber security awareness .* Pretoria: Council for Scientific and Industrial Research.

Dunn, M. A Comparative Analysis Of Cybersecurity Initiatives Worldwide. *WSIS Thematic Meeting on Cybersecurity.* 2008.

Dunn, 2019, International Cybersecurity And Data Privacy Outlook And Review 2019 https://www.gibsondunn.com/international-cybersecurity-and-data privacy-outlook-and-review-2019/#_Toc536455441.

Ensafi, Roya & Winter, Philipp & Mueen, Abdullah & Crandall, Jedidiah. (2015). Analyzing the Great Firewall of China Over Space and Time. Proceedings on Privacy Enhancing Technologies. 1. 10.1515/popets-2015-0005

Enisa, 2012. National Cyber Security Strategies 15. https://doi.org/10.2824/3903.

Filmer, Robert, *Sir Robert Filmer: Patriarcha and Other Writings*, Johann P. Sommerville (ed.), Cambridge: Cambridge University Press, 1991. doi:10.1017/CBO9780511812644.

Flick, D. (2011). Research Methods. *Social Science* , 31-55.Gercke, M., 2011. International Telecommunication Union Cybercrime Legislation Resources UNDERSTANDING CYBERCRIME: A GUIDE FOR DEVELOPING COUNTRIES. Int. Telecommun. Union Cybercrime Legis. Resource.

Global Cybersecurity Index. ITU. 2014. Retrieved from http://www.itu.int/en/ITU- D/Cybersecurity/Documents/WP-GCI-101.pdf

Global Forum on Cyber Expertise. (2019). *Cyber security and cyber crime trends in Africa.* USA: Global Forum on Cyber Expertise.

Griffiths, J. L. (2016). *Cyber security as an emerging challenge to South African national security* . Pretoria: University of Pretoria.

Harold, S., Libicki, M., Cevallos, A., 2016. Getting to Yes with China in Cyberspace, Getting to Yes with China in Cyberspace. https://doi.org/10.7249/rr1335.

Harold, S., Libicki, M., Cevallos, A., 2016. Getting to Yes with China in Cyberspace, Getting to Yes with China in Cyberspace. https://doi.org/10.7249/rr1335.

HM, Government 2016, https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021.

Hooker, Richard, 1594, *Of the Laws of Ecclesiastical Polity*, A. S. McGrade (ed.), Cambridge: Cambridge University Press, 1975.

INTERPOL COVID-19 cyberthreats alerts https://www.interpol.int/en/Crimes/Cybercrime/COVID-19-cyberthreats.

Internet Society. (2017). *Internet infrastructure security guidelines for Africa: A joint initiative of the Internet Society and the Commission of the African Union.*

ITU. (2007). *ITU global cybersecurity agenda (GCA).* Geneva: International Telecommunications Union (ITU).

James, C. (2018). *Cyber security: Threats, challenges and opportunities.* Africa: ACS.

Johnston, Alastair Iain. *Cultural Realism: Strategic Culture and Grand Strategy in Chinese History.* Princeton, NJ: Princeton University Press, 1995.

Lantis, Jeffrey S. Lantis. "Strategic Culture and National Security Policy." *International Studies Review* 4, no. 3 (Autumn, 2002): 87-113. http://www.jstor.org/stable/3186465.

KABANDA, G., (2013). "African context for technological futures for digital learning and the endogenous growth of a knowledge economy", *Basic Journal of Engineering Innovation (BRJENG)*, Volume 1(2), April 2013, pages 32-52, http://basicresearchjournals.org/engineering/PDF/Kabanda.pdf.

Kademi, A. M. (2014). *National cyber security strategy (NCSS): A model for Nigeria.* Nigeria: Yasar University .

Kaimba, B. (2017). *Africa cyber security report 2017: Demystifying Africa's cyber security poverty line.* Africa: Serianu.

Kenyanito, E. P., & Chima, R. J. (2016). *Room for improvement: Implementating the African cyber security and data protection convention in Sub-Saharan Africa.* Africa: African Union Conventionon Cyber-security and Personal Data.

Kshetri, N. (2019). Cybercrime and cybersecurity in Africa. *Journal of global information technology management , 22* (2), 77-81.

Le Sage, A. (2010). *Africa's irregular security threats: Challenges for US engagement .* Africa: National Defence University .

Locke, John, *Works*, 10 volumes, London, 1823; reprinted, Aalen: Scientia Verlag, 1963.

Luiijf, E., Besseling, K., & de Graaf, P. (2013). Nineteen national cyber security strategies. *International journal of critical infrastructures , 9* (1/2).

Luiijf, H. A., Besseling, K., Spoelstra, M., & de Graaf, P. (2016). *Ten national cyber security strategies: A comparison.* Netherlands: Capgemini.

Mathe, A. (2019). *The misunderstood world of cybersecurity in Africa.* Africa: Policy Centre for the New South .

Nir Kshetri (2019) Cybercrime and Cybersecurity in Africa, Journal of Global Information Technology Management, 22:2, 77-81, DOI: 10.1080/1097198X.2019.1603527.

No winner in Japan-South Korea conflict https://hediplomat.com/2019/08/there-will-be-no-winner-in-the-japan South. Korea-dispute/

Nouri, A. (2011). *A study about research & research methods.*

Ntoko, A. (2011). *Global cybersecurity agenda (GCA): A framework for international cooperation .* Geneva: International Telecommunications Union (ITU).

Pring, R. (2010). *Philosophy of educational research.* London: Continuum.

Reegård, Kine & Blackett, Claire & Katta, Vikash. (2019). The Concept of Cybersecurity Culture. 10.3850/978-981-11-2724-3_0761-cd

Saini, H.H. and Saini, D.D. (2007) Proactive Cyber Defense and Reconfigurable Framework for Cyber Security. *International Review on Computers and Software*, 2, 2, 89-97.

Sarker, K., Rahman, H., Rahman, K. F., Arman, S., Biswas, S., & Bhuiyan, T. (2019). A comparative analysis of the cyber security strategies of Bangladesh. *International journal of cybernetics and informatics , 8* (2).

Saunders, M. (2015). Understanding research philosophy and approaches to theory development . United Kingdom: Pearson Education .

Saunders, M., Levin, P., & Thornhill, A. (2016). *Research methods for business students* (2nd ed.). London: Prentice-Hall.

Shafqat, N., & Masood, A. (2016). Comparative anaylis of various national cyber security strategies. *International journal of computer science and information security , 14* (1).

Slimani, M. (2016). *Enhancing cyber security in Africa: New challenges for regional organisations?* Khartoum, Sudan: African Telecommunications Union .

Schwartz, P. (1991) *The Art of the Long View: Paths to Strategic Insight for Yourself and Your Company*. Doubleday, New York.

Scully, T. (2011) The Cyber Threat, Trophy Information and the Fortress Mentality. *Journal of Business Continuity and Emergency Planning*, 5, 3, 195-207.

Silverman, David (2000), *Doing Qualitative Research – A Practical Handbook*. London, Thousand Oaks, New Delhi: Sage Publications.

Silverman, David (2006), *Interpreting Qualitative Data – Methods for Analyzing Talk, Text and Interaction*. London, Thousand Oaks, New Delhi: Sage Publications.

South Korea to give up developing country status in WTO talks. https://www.reuters.com/article/us-southkorea-trade-wto/south-korea- to- give- up-developing-country-talksidUSKBN1X401W

Symantec. (2016). *Cyber crime an cyber security trends in Africa.* USA: Symantec.

THE Mauritius Cybercrime Strategy 2017-2019, (2017). http://certmu.govmu.org/English/Documents/Cybercrime%20Strategy/

Nat ional %20Cybercrime%20Strategy-%20August%202017.pdf.

Tikk, E., Kaska, K. and Vihul, L. (2010) International Cyber Incidents: Legal Considerations, Cooperative Cyber Defense Center of Excellence (CCD

Trump, D. J. (2018). *National cyber strategy of the United States of America.* Washington DC: The White House.

UNECA. (2014). *Tackling the challenges of cyber security in Africa.* Washington DC:

United Nations Economic Commission for Africa (UNECA).

UNITED Nations Economic Commission for Africa. (2014).Tackling the challenges of cybersecurity in Africa.

van Nierkerk, B. (2017). An analysis of cyber-incidents in South Africa. *The African journal of information and communication , 20*, 113-132.

Wamala, F. (2012). *ITU national cybersecurity strategy guide.* Geneva: International Telecommunications Union (ITU).

WEF. (2016). *Global agenda council on cybersecurity .* Europe: World Economic Forum (WEF).

Whitehouse, 2018) https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

Wooten, Kevin B. “Chinese National Security Strategy: Implications for a 21st Century Air Force.” Master’s thesis: Air War College, Air University (2005). http://dtlweb.au.af.mil/webclient/DeliveryManager?pid=36962.

Yount, R. (2016). Population and sampling. In *Research Fundamentals* (4th ed.).

Yusuf, K. (2019). *Africa is leaving itself dangerously exposed to cyber attacks.* United Kingdom: ACCA.

Zachary, Todd M. “Wearing the White Hat: The Effect of American Strategic Culture on Implementing National Strategy.” Master’s thesis: School of Advanced Airpower Studies, Air University (2000).

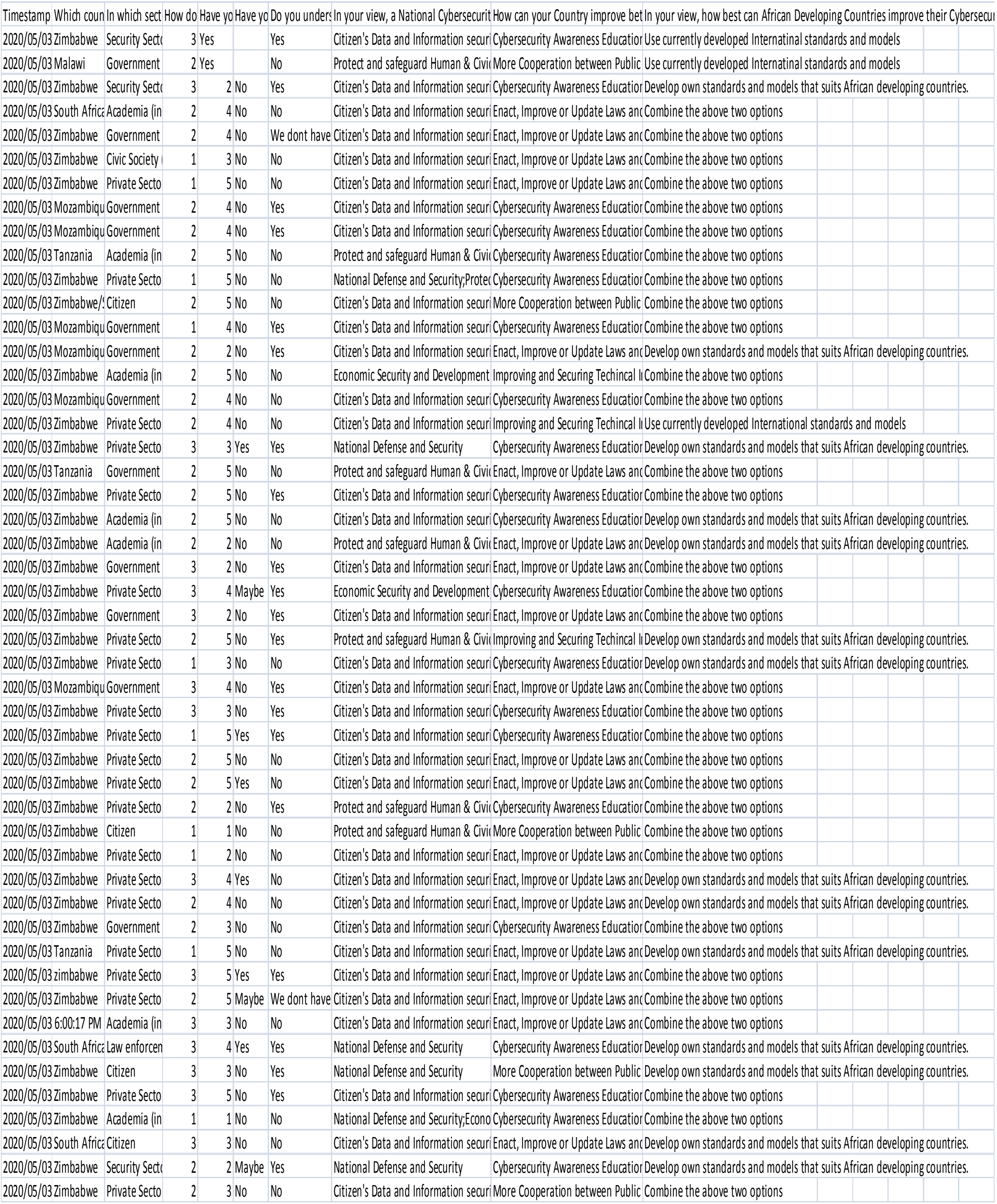
APPENDICES

Appendix 1. List of countries and sector respondents represented

Country	Sector	Frequency
Botswana	Private Sector (incl, Media, Telecommunications, ICT firms and Finance)	2
	Academia (incl, Universities, Colleges, Research Institutes)	1
	Government (incl, Ministry, Department or any Public entities)	1
Malawi	Government (incl, Ministry, Department or any Public entities)	1
	Security Sector (incl, Military or Intelligence Community)	1
Mozambique	Government (incl, Ministry, Department or any Public entities)	7
South Africa	Private Sector (incl, Media, Telecommunications, ICT firms and Finance)	4
	Citizen	4
	Academia (incl, Universities, Colleges, Research Institutes)	3
	Law enforcement Agency (Private LEA, Police, Judiciary)	2
	Security Sector (incl, Military or Intelligence Community)	1
	Academia (incl, Universities, Colleges, Research Institutes)	1

Country	Sector	Frequency
Tanzania	Government (incl, Ministry, Department or any Public entities)	1
	Private Sector (incl, Media, Telecommunications, ICT firms and Finance)	1
Zambia	Government (incl, Ministry, Department or any Public entities)	5
	Private Sector (incl, Media, Telecommunications, ICT firms and Finance)	2
Zimbabwe	Private Sector (incl, Media, Telecommunications, ICT firms and Finance)	30
	Government (incl, Ministry, Department or any Public entities)	10
	Academia (incl, Universities, Colleges, Research Institutes)	10
	Security Sector (incl, Military or Intelligence Community)	5
	Civic Society (Local NGO's, Activist, Loby Groups or others)	4
	Citizen	3

Appendix 2. Raw Data from the Comma Delimited File (CSV)



Timestamp	Which coun	In which sect	How do	Have yo	Have yo	Do you unders	In your view, a National Cybersecurit	How can your Country improve bet	In your view, how best can African Developing Countries improve their Cybersecur
2020/05/03	Zimbabwe	Security Sect	3	Yes		Yes	Citizen's Data and Information securi	Cybersecurity Awareness Educatio	Use currently developed Internatinal standards and models
2020/05/03	Malawi	Government	2	Yes		No	Protect and safeguard Human & Civi	More Cooperation between Public	Use currently developed Internatinal standards and models
2020/05/03	Zimbabwe	Security Sect	3	2	No	Yes	Citizen's Data and Information securi	Cybersecurity Awareness Educatio	Develop own standards and models that suits African developing countries.
2020/05/03	South Afric	Academia (in	2	4	No	No	Citizen's Data and Information securi	Enact, Improve or Update Laws an	Combine the above two options
2020/05/03	Zimbabwe	Government	2	4	No	We dont have	Citizen's Data and Information securi	Enact, Improve or Update Laws an	Combine the above two options
2020/05/03	Zimbabwe	Civic Society (	1	3	No	No	Citizen's Data and Information securi	Enact, Improve or Update Laws an	Combine the above two options
2020/05/03	Zimbabwe	Private Secto	1	5	No	No	Citizen's Data and Information securi	Enact, Improve or Update Laws an	Combine the above two options
2020/05/03	Mozambiqu	Government	2	4	No	Yes	Citizen's Data and Information securi	Cybersecurity Awareness Educatio	Combine the above two options
2020/05/03	Mozambiqu	Government	2	4	No	Yes	Citizen's Data and Information securi	Cybersecurity Awareness Educatio	Combine the above two options
2020/05/03	Tanzania	Academia (in	2	5	No	No	Protect and safeguard Human & Civi	Cybersecurity Awareness Educatio	Combine the above two options
2020/05/03	Zimbabwe	Private Secto	1	5	No	No	National Defense and Security;Prote	Cybersecurity Awareness Educatio	Combine the above two options
2020/05/03	Zimbabwe/S	Citizen	2	5	No	No	Citizen's Data and Information securi	More Cooperation between Public	Combine the above two options
2020/05/03	Mozambiqu	Government	1	4	No	Yes	Citizen's Data and Information securi	Cybersecurity Awareness Educatio	Combine the above two options
2020/05/03	Mozambiqu	Government	2	2	No	Yes	Citizen's Data and Information securi	Enact, Improve or Update Laws an	Develop own standards and models that suits African developing countries.
2020/05/03	Zimbabwe	Academia (in	2	5	No	No	Economic Security and Development	Improving and Securing Techincal I	Combine the above two options
2020/05/03	Mozambiqu	Government	2	4	No	No	Citizen's Data and Information securi	Cybersecurity Awareness Educatio	Combine the above two options
2020/05/03	Zimbabwe	Private Secto	2	4	No	No	Citizen's Data and Information securi	Improving and Securing Techincal I	Use currently developed International standards and models
2020/05/03	Zimbabwe	Private Secto	3	3	Yes	Yes	National Defense and Security	Cybersecurity Awareness Educatio	Develop own standards and models that suits African developing countries.
2020/05/03	Tanzania	Government	2	5	No	No	Protect and safeguard Human & Civi	Enact, Improve or Update Laws an	Combine the above two options
2020/05/03	Zimbabwe	Private Secto	2	5	No	Yes	Citizen's Data and Information securi	Cybersecurity Awareness Educatio	Combine the above two options
2020/05/03	Zimbabwe	Academia (in	2	5	No	No	Citizen's Data and Information securi	Cybersecurity Awareness Educatio	Develop own standards and models that suits African developing countries.
2020/05/03	Zimbabwe	Academia (in	2	2	No	No	Protect and safeguard Human & Civi	Enact, Improve or Update Laws an	Develop own standards and models that suits African developing countries.
2020/05/03	Zimbabwe	Government	3	2	No	Yes	Citizen's Data and Information securi	Enact, Improve or Update Laws an	Combine the above two options
2020/05/03	Zimbabwe	Private Secto	3	4	Maybe	Yes	Economic Security and Development	Cybersecurity Awareness Educatio	Combine the above two options
2020/05/03	Zimbabwe	Government	3	2	No	Yes	Citizen's Data and Information securi	Enact, Improve or Update Laws an	Combine the above two options
2020/05/03	Zimbabwe	Private Secto	2	5	No	Yes	Protect and safeguard Human & Civi	Improving and Securing Techincal I	Develop own standards and models that suits African developing countries.
2020/05/03	Zimbabwe	Private Secto	1	3	No	No	Citizen's Data and Information securi	Cybersecurity Awareness Educatio	Develop own standards and models that suits African developing countries.
2020/05/03	Mozambiqu	Government	3	4	No	Yes	Citizen's Data and Information securi	Enact, Improve or Update Laws an	Combine the above two options
2020/05/03	Zimbabwe	Private Secto	3	3	No	Yes	Citizen's Data and Information securi	Cybersecurity Awareness Educatio	Combine the above two options
2020/05/03	Zimbabwe	Private Secto	1	5	Yes	Yes	Citizen's Data and Information securi	Cybersecurity Awareness Educatio	Combine the above two options
2020/05/03	Zimbabwe	Private Secto	2	5	No	No	Citizen's Data and Information securi	Enact, Improve or Update Laws an	Combine the above two options
2020/05/03	Zimbabwe	Private Secto	2	5	Yes	No	Citizen's Data and Information securi	Enact, Improve or Update Laws an	Combine the above two options
2020/05/03	Zimbabwe	Private Secto	2	2	No	Yes	Protect and safeguard Human & Civi	Cybersecurity Awareness Educatio	Combine the above two options
2020/05/03	Zimbabwe	Citizen	1	1	No	No	Protect and safeguard Human & Civi	More Cooperation between Public	Combine the above two options
2020/05/03	Zimbabwe	Private Secto	1	2	No	No	Citizen's Data and Information securi	Enact, Improve or Update Laws an	Combine the above two options
2020/05/03	Zimbabwe	Private Secto	3	4	Yes	No	Citizen's Data and Information securi	Enact, Improve or Update Laws an	Develop own standards and models that suits African developing countries.
2020/05/03	Zimbabwe	Private Secto	2	4	No	No	Citizen's Data and Information securi	Enact, Improve or Update Laws an	Develop own standards and models that suits African developing countries.
2020/05/03	Zimbabwe	Government	2	3	No	No	Citizen's Data and Information securi	Cybersecurity Awareness Educatio	Combine the above two options
2020/05/03	Tanzania	Private Secto	1	5	No	No	Citizen's Data and Information securi	Enact, Improve or Update Laws an	Develop own standards and models that suits African developing countries.
2020/05/03	zimbabwe	Private Secto	3	5	Yes	Yes	Citizen's Data and Information securi	Enact, Improve or Update Laws an	Combine the above two options
2020/05/03	Zimbabwe	Private Secto	2	5	Maybe	We dont have	Citizen's Data and Information securi	Enact, Improve or Update Laws an	Combine the above two options
2020/05/03	6:00:17 PM	Academia (in	3	3	No	No	Citizen's Data and Information securi	Enact, Improve or Update Laws an	Combine the above two options
2020/05/03	South Afric	Law enforcen	3	4	Yes	Yes	National Defense and Security	Cybersecurity Awareness Educatio	Develop own standards and models that suits African developing countries.
2020/05/03	Zimbabwe	Citizen	3	3	No	Yes	National Defense and Security	More Cooperation between Public	Develop own standards and models that suits African developing countries.
2020/05/03	Zimbabwe	Private Secto	3	5	No	Yes	Citizen's Data and Information securi	Cybersecurity Awareness Educatio	Combine the above two options
2020/05/03	Zimbabwe	Academia (in	1	1	No	No	National Defense and Security;Econo	Cybersecurity Awareness Educatio	Combine the above two options
2020/05/03	South Afric	Citizen	3	3	No	No	Citizen's Data and Information securi	Enact, Improve or Update Laws an	Develop own standards and models that suits African developing countries.
2020/05/03	Zimbabwe	Security Sect	2	2	Maybe	Yes	National Defense and Security	Cybersecurity Awareness Educatio	Develop own standards and models that suits African developing countries.
2020/05/03	Zimbabwe	Private Secto	2	3	No	No	Citizen's Data and Information securi	More Cooperation between Public	Combine the above two options

2020/05/03	Zimbabwe	Citizen	2	3	No	No	Protect and safeguard Human & Civi	Enact, Improve or Update Laws an	Combine the above two options
2020/05/03	Zimbabwe	Private Secto	3	3	No	Yes	Citizen's Data and Information securi	Cybersecurity Awareness Educatio	Develop own standards and models that suits African developing countries.
2020/05/03	South Africa	Private Secto	3	5	No	Yes	Citizen's Data and Information securi	Enact, Improve or Update Laws an	Combine the above two options
2020/05/03	South Africa	Private Secto	3	5	No	Yes	Citizen's Data and Information securi	Enact, Improve or Update Laws an	Combine the above two options
2020/05/03	Zimbabwe	Security Sect	1	3	No	No	National Defense and Security	Cybersecurity Awareness Educatio	Combine the above two options
2020/05/03	Zimbabwe	Academia (in	3	2	No	Not Interested	Protect and safeguard Human & Civi	Improving and Securing Techincal I	Develop own standards and models that suits African developing countries.
2020/05/03	Italy	Academia (in	5	4	No	No	Citizen's Data and Information securi	Cybersecurity Awareness Educatio	Develop own standards and models that suits African developing countries.
2020/05/03	Zimbabwe	Government	2	3	No	No	Citizen's Data and Information securi	Enact, Improve or Update Laws an	Combine the above two options
2020/05/03	Zimbabwe	Government	2	4	No	No	Protect and safeguard Human & Civi	More Cooperation between Public	Develop own standards and models that suits African developing countries.
2020/05/03	Zimbabwe	Private Secto	1	4	No	No	National Defense and Security;Econo	Cybersecurity Awareness Educatio	Combine the above two options
2020/05/03	Zimbabwe	Academia (in	2	4	No	No	Citizen's Data and Information securi	Improving and Securing Techincal I	Develop own standards and models that suits African developing countries.
2020/05/03	Zimbabwe	Academia (in	2	4	No	Not Interested	Citizen's Data and Information securi	Enact, Improve or Update Laws an	Develop own standards and models that suits African developing countries.
2020/05/03	Zimbabwe	Private Secto	2	5	Maybe	Yes	Citizen's Data and Information securi	Enact, Improve or Update Laws an	Combine the above two options
2020/05/03	Zimbabwe	Academia (in	3	3	No	No	Protect and safeguard Human & Civi	Cybersecurity Awareness Educatio	Combine the above two options
2020/05/03	Zimbabwe	Private Secto	1	5	No	No	Citizen's Data and Information securi	Cybersecurity Awareness Educatio	Develop own standards and models that suits African developing countries.
2020/05/03	Zambia	Private Secto	3	2	No	Yes	Citizen's Data and Information securi	Cybersecurity Awareness Educatio	Combine the above two options
2020/05/03	Zambia	Government	3	3	No	No	Citizen's Data and Information securi	Cybersecurity Awareness Educatio	Combine the above two options
2020/05/03	Zimbabwe	Academia (in	1	4	No	No	Citizen's Data and Information securi	Enact, Improve or Update Laws an	Combine the above two options
2020/05/03	Zambia	Government	4	3	No	Yes	Citizen's Data and Information securi	Enact, Improve or Update Laws an	Combine the above two options
2020/05/03	Zambia	Government	3	3	No	Yes	Citizen's Data and Information securi	Enact, Improve or Update Laws an	Combine the above two options
2020/05/03	Zimbabwe	Government	3	1	No	No	Citizen's Data and Information securi	Cybersecurity Awareness Educatio	Develop own standards and models that suits African developing countries.
2020/05/03	Botswana	Academia (in	3	5	No	Yes	Economic Security and Development	Cybersecurity Awareness Educatio	Combine the above two options
2020/05/03	Zambia	Government	1	3	No	No	Citizen's Data and Information securi	Enact, Improve or Update Laws an	Develop own standards and models that suits African developing countries.
2020/05/03	Zimbabwe	Private Secto	2	4	No	No	Protect and safeguard Human & Civi	Enact, Improve or Update Laws an	Use currently developed International standards and models
2020/05/03	Botswana	Private Secto	2	3	Maybe	No	Citizen's Data and Information securi	Cybersecurity Awareness Educatio	Combine the above two options
2020/05/03	Zambia	Government	1	5	No	We dont have	Citizen's Data and Information securi	Cybersecurity Awareness Educatio	Combine the above two options
2020/05/03	Zimbabwe	Government	3	2	No	No	Economic Security and Development	Cybersecurity Awareness Educatio	Combine the above two options
2020/05/03	Zambia	Private Secto	2	5	Maybe	Yes	Citizen's Data and Information securi	Enact, Improve or Update Laws an	Combine the above two options
2020/05/03	Zimbabwe	Academia (in	3	2	No	No	Citizen's Data and Information securi	Enact, Improve or Update Laws an	Combine the above two options
2020/05/03	South Africa	Private Secto	3	4	No	Yes	Citizen's Data and Information securi	Enact, Improve or Update Laws an	Combine the above two options
2020/05/03	Zimbabwe	Private Secto	2	2	No	No	Citizen's Data and Information securi	Enact, Improve or Update Laws an	Combine the above two options
2020/05/03	Zimbabwe	Private Secto	1	3	No	Not Interested	Protect and safeguard Human & Civi	Improving and Securing Techincal I	Combine the above two options
2020/05/03	Zimbabwe	Private Secto	2	4	No	Not Interested	Citizen's Data and Information securi	Enact, Improve or Update Laws an	Combine the above two options
2020/05/03	Zimbabwe	Private Secto	1	2	No	Yes	Citizen's Data and Information securi	Cybersecurity Awareness Educatio	Combine the above two options
2020/05/03	Malawi	Security Sect	2	4	No	No	Economic Security and Development	Improving and Securing Techincal I	Develop own standards and models that suits African developing countries.
2020/05/03	South Africa	Security Sect	3	4	No	Yes	Citizen's Data and Information securi	Cybersecurity Awareness Educatio	Develop own standards and models that suits African developing countries.
2020/05/03	South Africa	Law enforcem	3	5	No	No	Citizen's Data and Information securi	Enact, Improve or Update Laws an	Use currently developed International standards and models
2020/05/04	South Africa	Private Secto	3	5	Yes	Yes	Citizen's Data and Information securi	Enact, Improve or Update Laws an	Combine the above two options
2020/05/04	Zimbabwe	Civic Society (	2	3	No	No	National Defense and Security;Econo	Cybersecurity Awareness Educatio	Develop own standards and models that suits African developing countries.
2020/05/04	Zimbabwe	Civic Society (	2	3	No	No	National Defense and Security;Econo	Cybersecurity Awareness Educatio	Develop own standards and models that suits African developing countries.
2020/05/04	South Africa	Citizen	3	3	No	Yes	Citizen's Data and Information securi	Cybersecurity Awareness Educatio	Combine the above two options
2020/05/04	South Africa	Citizen	3	3	No	Yes	Citizen's Data and Information securi	Cybersecurity Awareness Educatio	Combine the above two options
2020/05/04	Zimbabwe	Civic Society (	2	3	No	No	Economic Security and Development	Enact, Improve or Update Laws an	Combine the above two options
2020/05/04	Mozambiqu	Government	1	3	No	No	National Defense and Security	Enact, Improve or Update Laws an	Develop own standards and models that suits African developing countries.
2020/05/05	Zimbabwe	Government	3	4	Yes	Yes	Citizen's Data and Information securi	Enact, Improve or Update Laws an	Combine the above two options
2020/05/05	Zimbabwe	Private Secto	2	5	Maybe	Yes	Citizen's Data and Information securi	Enact, Improve or Update Laws an	Combine the above two options
2020/05/06	Zimbabwe	Security Sect	3	5	Yes	We dont have	Citizen's Data and Information securi	Enact, Improve or Update Laws an	Combine the above two options
2020/05/06	Zimbabwe	Government	3	5	No	Yes	Citizen's Data and Information securi	Cybersecurity Awareness Educatio	Develop own standards and models that suits African developing countries.
2020/05/06	Zimbabwe	Security Sect	2	5	Yes	Yes	Citizen's Data and Information securi	Improving and Securing Techincal I	Combine the above two options
2020/05/07	Ethiopia	Government	2	5	Yes	Yes	Citizen's Data and Information securi	Enact, Improve or Update Laws an	Develop own standards and models that suits African developing countries.
2020/05/07	Zimbabwe	Government	3	4	Yes	Yes	Citizen's Data and Information securi	Enact, Improve or Update Laws an	Combine the above two options
2020/05/09	Zimbabwe	Private Secto	3	4	No	No	Citizen's Data and Information securi	Cybersecurity Awareness Educatio	Combine the above two options

Appendix 3. SQL Code snippets for used in data analysis.

```
1.SELECT [Data from Questionnaire].Sector, [Data from Questionnaire].Participation, Count([Data from Questionnaire].Sector) AS [Respondents selcetd No]
FROM [Data from Questionnaire]
GROUP BY [Data from Questionnaire].Sector, [Data from Questionnaire].Participation
HAVING ((([Data from Questionnaire].Participation)="Yes"))
ORDER BY Count([Data from Questionnaire].Sector) DESC;
```

```
2.SELECT [Data from Questionnaire].How_to_Improve
FROM [Data from Questionnaire]
WHERE ((([Data from Questionnaire].How_to_Improve)="Cybersecurity Awareness Education and involvement by the Citizens"));
```

```
3.SELECT [Data from Questionnaire].Country, [Data from Questionnaire].Sector, Count([Data from Questionnaire].[Sector]) AS Frequency
FROM [Data from Questionnaire]
GROUP BY [Data from Questionnaire].Country, [Data from Questionnaire].Sector
ORDER BY Count([Data from Questionnaire].[Sector]) DESC;
```

```
4.SELECT [Data from Questionnaire].Model_Choice, Count([Data from Questionnaire].[Sector]) AS Expr1, [Data from Questionnaire].Country, [Data from Questionnaire].Participation
FROM [Data from Questionnaire]
```

```
GROUP BY [Data from Questionnaire].Model_Choice, [Data from Questionnaire].Sector, [Data from Questionnaire].Country, [Data from Questionnaire].Participation
HAVING ((([Data from Questionnaire].Model_Choice) Like "Develop own standards and models that suits African developing countries.") AND ((([Data from Questionnaire].Country) Like 'South Africa' Or ([Data from Questionnaire].Country)='Zimbabwe') AND ((([Data from Questionnaire].Participation) Like 'No'));
```

Appendix 4. R -Code snippets for used in quantitative analysis

```
title: "SURVEY"
author: "Terrence_Nemayire"
date: "May 10, 2020"
output:
  html_document:
    df_print: paged
  pdf_document: default
  word_document: default
---
##Key-
Q1 -Which country do you come from?
Q2 -In which sector does your profession belong to?
Q3 -How do you view the Cybersecurity state of your country?
Q4 -Have you heard of any Cybersecurity incident (e.g hacking, cybercrime, creditcard  fraud, identity theft, etc, in your country?
Q5 -Have you ever been part of a team participating in?
Q6 -Do you understand any of the existing  Cyber Laws (if any), Acts or any Legal requirements that concern Cybersecurity in your country?
```

Q7 -In your view, a National Cybersecurity Strategy should primarily focus on which of the following pillars?

Q8 -How can your Country improve better from the current Cybersecurity statUS?

Q9 -In your view, how best can African Developing Countries improve their Cybersecurity situations?

~~~~
##
```{r}
install.packages ("readxl")
library(readxl)
survey_data <- read_excel("C:/R- Studio/Thesis/Data.xls")
survey_data ## the name of the file when loaded in the r studio package
survey_frame <- survey_data [, c("Q1","Q2","Q3","Q4","Q5","Q6","Q7","Q8","Q9")]
survey_frame
library(plyr)
countries <- count(survey_frame$Q1)
countries
cou_chart <- c(4, 2,7,14,3,7,62)
cou_labels <- c("Botswana","Malawi","Mozambique","South
Africa","Tanzania","Zambia","Zimbabwe")
pct <- round(cou_chart/sum(cou_chart)*100)
cou_labels <- paste (cou_labels,pct)
cou_labels <- paste (cou_labels,"%",sep ="")
pie(cou_chart,labels = cou_labels, col=rainbow(length(cou_labels)),
   main=" Survey Representation by Countries")
q4 <- (survey_frame$Q4)
q4
summary (q4)
q3 <- (survey_data$Q3)
~~~~

```
q3
summary (q3)
q5 <- factor(survey_data$Q5)
q5
summary (q5)
improve <- c ( (survey_data$Q7))
improve

library(tidyverse)
country_heard <- survey_frame %>% select(1,4)
country_heard
country_heard %>% filter(Q1 != 'Zimbabwe')
no_zim <- country_heard %>% filter(Q1 != 'Zimbabwe')
no_zim
levels (no_zim$Q4)

counts <- table(no_zim$Q4)
counts

barplot(counts, main="Response distribution without Zimbabwe (Outweighted)",
   xlab="Responces of heaving heard any cybersecurity issues",
   ylab ="Number of Respondents",col = c("blue"),
   names.arg=c(" Slightly heard", " Moderately heard", " Yes have heard"," Have heard alot"))

install.packages(c("foreign", "survey", "knitr"))
table (survey_data$Q5)
count_primary_focus <- count(survey_frame$Q7)
count_primary_focus
```

```
library(xlsx)
write.xlsx(count_primary_focus, "C:/R- Studio/Thesis/primary_focus.xlsx")
focus <- c (71,65,53,63,1)
focus
focus_label <- c
("Citizen_data_and_information_security","National_Defence_and
Security","Economic_Security_development","Protecting_Human_Rights","Econo
mic_cybercrime ")
focus_label
survey_frame
summary(survey_frame$Q3)
summary(survey_frame$Q4)
summary(survey_frame$Q6)

table (survey_frame$Q7)## function to see how a factor variable is distributed
table (survey_frame$Q9)
table (survey_frame$Q8)
install.packages(c("grid", "Matrix"))
library (survey)
survey_design = svydesign(
  ids =~1,
data = survey_frame,
  weights = ~Q3
)
svymean (~ Q9,
         design = survey_design)
```

국가 사이버 보안 전략에 관한 연구

미래의 사이버 보안 전략 개발을위한 기능 분석

2020.
석사학위논문
테렌스 네마이레
국제학과
지도교수: Joshua I. James, 장윤식

국가, 조직 및 개인의 정보 통신 기술을 활용하는 힘은 필연적으로 일상의 일부가 되었다. 많은 시스템 상호 연결 및 디지털 기술에 대한 의존도가 높아짐에 따라 사이버 위협의 종류, 양 및 궤도가 기하 급수적으로 증가했다. 사이버 보안 환경을 개선하기위한 전략적 조치, 절차 및 솔루션인 국가 사이버 안보 전략 (NCSS)을 채택하는 것이 국가 차원에서 필수적이되었다. ITU (International Telecommunications Union)의 최근 연구에 따르면 상당수의 국가에는 여전히 국가 사이버 안보 전략이 없지만 사이버 안보 환경은 놀라운 속도로 발전하고 있다.

다른 한편으로, 개도국은 다른 선진국에 비해 국가 차원에서 사이버 위협에 대한 경쟁에서 뒤쳐져있다. 그러므로 개도국이 자신의 환경과 필요에 내재 된 위협을 다루는 새로운 방법을 채택하기 시작해야 한다. 따라서 본 연구는 개발 도상국의 문제, 필요 및 요구 사항을 확인하고자 한다. 이 연구는 이 연구에서 식별 된 특징들을 고려하여 채택 될 수있는 하이브리드 프레임 워크를 제안했다. 주요 특징은 강력한 인프라, 입법, 문화 및

기술 통제에 의해 지원되는 다중 이해 관계자 접근 방식의 다른 기능인 시민의 인식, 교육 및 참여 등이다.

주제어 : 사이버 안보, 개발도상국, 모델, 사이버 위협, 아프리카, 국가 사이버 안보전략 (NCSS).

A Study on National Cybersecurity Strategy

Feature Analysis for Future Cybersecurity Strategy Development

2020.
Master's Degree
Terrence Nemayire
Department of International Studies
Advisor: Prof. James I. Joshua. Prof. Jang Yunsik

National, organisational and, individual's harnessing power of information and communication technology has inevitably become part of daily routines. With the prolific system interconnection and growing dependence on digital technologies the varieties, volume and, trajectory of cyber threats have exponentially increased. It has become imperative at the national level to adopt strategic measures, procedures and, solution to improve the cybersecurity environment: the National Cyber Security Strategy (NCSS). Recent studies by the International Telecommunications Union (ITU) revealed that a significant number of countries are still without a national cybersecurity strategy, yet the cybersecurity landscape is evolving at an alarming rate.

On the other hand, developing nations have lagged behind in the race against cyberthreats at the national level as compared to other developed nations. It is therefore imperative for developing nations to start adopting new ways of dealing with the vice natured within their setting and needs. This study therefore seeks to ascertain the challanges, needs and, requirements for developing countries. The research work has proposed a hybrid framework that can be adopted taking into considerations the features identified in this study. The main features includes; citizen's awareness, education and, involvement, the other feature in multistakeholder approach supported by robust infrastructure, legislative, cultural and technical controls.

Keywords: Cybersecurity, Developing Nations, Model, Cyber Threat, Africa, National Cybersecurity Strategy (NCSS)