Towards an aligned South African National Cybersecurity Policy Framework

by

JOEL CHIGADA
(Student Number: CHGJOE001)

Submitted in accordance with the requirements for the degree of

DOCTOR OF PHILOSOPHY

in the subject

INFORMATION SYSTEMS

in the

Department of Information Systems,
Commerce Faculty, University of Cape Town

Supervisor: Professor Michael Kyobe

2021

DECLARATION

I, Joel Chigada, hereby declare that the work on this thesis, ***"Towards an aligned South African National Cybersecurity Policy Framework"*** is my original work (except where acknowledgements indicate otherwise) and that neither the whole work nor any part of it has been, is being, or is to be submitted for another degree in this or other university. I authorise the University to reproduce for the purpose of research either the whole or any portion of the contents in any manner whatsoever.

"I also confirm that I have been granted permission by the University of Cape Town's Doctoral Degrees Board to include the following publication in my PhD thesis and where co-authorships are involved, my co-author has agreed that I may include the publication":

(i) Chigada, J. & Kyobe, M.E. (2018). "Evaluating factors contributing to misalignment of the South African National Cybersecurity Policy Framework", Proceedings of the International Conference on Information Resources Management (CONF-IRM), *2018 Proceedings 4*.: Available at: http://aisel.aisnet.org/confirm2018/4

With the help and constructive guidance of IS scholarly community, I have integrated and incorporated various ideas to develop this thesis.

Signature: **Date:** 25 August 2022

Plagiarism Score (Turnitin): 14% (green)

ABSTRACT

The purpose of this study was to measure and align factors that contribute to the misalignment of the South African National Cybersecurity Policy Framework (SA-NCPF). The exponential growth rate of cyber-attacks and threats has caused more headaches for cybersecurity experts, law enforcement agents, organisations and the global business economy. The emergence of the global Corona Virus Disease-2019 has also contributed to the growth of cyber-attacks and threats thus, requiring concerted efforts from everyone in society to devise appropriate interventions that mitigate unacceptable user behaviour in the reality of cyberspace. In this study, various theories were identified and pooled together into an integrative theoretical framework to provide a better understanding of various aspects of the law-making process more comprehensively. The study identified nine influencing factors that contributed to misalignment of the South African National Cybersecurity Policy Framework. These influencing factors interact with each other continuously producing complex relationships, therefore, it is difficult to measure the degree of influence of each factor, hence the need to look at and measure the relationships as Gestalts. Gestalts view individual interactions between pairs of constructs only as a part of the overall pattern. Therefore, the integrative theoretical framework and Gestalts approach were used to develop a conceptual framework to measure the degree of alignment of influencing factors.

This study proposed that the stronger the coherence among the influencing factors, the more aligned the South African National Security Policy Framework. The more coherent the SA-NCPF is perceived, the greater would be the degree of alignment of the country's cybersecurity framework to national, regional and global cyberlaws. Respondents that perceived a strong coherence among the elements also perceived an effective SA-NCPF. Empirically, this proposition was tested using nine constructs. Quantitative data was gathered from respondents using a survey. A major contribution of this study was that it was the first attempt in South Africa to measure the alignment of the SA-NCPF using the Gestalts approach as an effective approach for measuring complex relationships. The study developed the integrative theoretical framework which integrates various theories that helped to understand and explain the South African law-making process.

The study also made a significant methodological contribution by adopting the Cluster-based perspective to distinguish, describe and predict the degree of alignment of the SA-NCPF. There is a dearth of information that suggests that past studies have adopted or attempted to address the challenge of alignment of the SA-NCPF using the cluster-based and Gestalts perspectives. Practical implications from the study include a review of the law-making process, skills development strategy, a paradigm shift to address the global Covid-19 pandemic and sophisticated cybercrimes simultaneously. The study asserted the importance of establishing an independent cybersecurity board comprising courts, legal, cybersecurity experts, academics and law-makers to provide cybersecurity expertise and advice. From the research findings, government and practitioners can draw lessons to review the NCPF to ensure the country develops an effective national cybersecurity strategy. Limitations and recommendations for future research conclude the discussions of this study.

Keywords: Alignment, Cybercrime, Cyberlaws, Cybersecurity, Information Systems Security, National Cybersecurity Policy Framework

ACKNOWLEDGEMENTS

Education is the most powerful weapon which you can use to change the world
(Nelson Mandela, 2003).

The successful completion of this study is attributed to many people who contributed in different ways. I owe a debt of gratitude to my promoter and supervisor, Professor Michael Kyobe, Department of Information Systems at the University of Cape Town (UCT) whose immense and constructive criticism helped me to solidify my ideas regarding the Configuration Theory. To Professor Kyobe, I thank you for holding my hand throughout this tiring, painful but rewarding academic journey. Today, I am proud to stand up with an accolade that came about as a result of your invaluable guidance and desire to see an output that you are proud of. I thank you for your mentorship.

I would like to thank my colleagues in the Information Systems Department for their support and encouragement during the study. To Dr. Jacques Ophoff, Professor Irwin Brown and Mr. Pitso Siboloane, thank you for the talks we had regarding this doctoral project. Thank you, colleagues, for the words of support, jokes and above all, humour that eased pressure off my shoulders. I would like to thank Ms. Noxolo Limani for editing and proof-reading services. The grammatical idiosyncrasies envisaged editorial and proof-reading attention. It was imperative to correct, condense, organise and perform some modifications with the intention of producing correct, consistent, accurate and complete work that has been presented in this report.

I extend my sincere appreciation and heartfelt thanks to all respondents for their consent to participate in this study. For, without your time, cooperation and input, this study would not have been accomplished. I would like to express my gratitude to various institutions for their contributions towards the completion of this study. The insights and contributions were invaluable. Lastly, I express my profound appreciation to my wife, Lillian, children, Faith, Joel Jr. and Charmaine for their unwavering support during the study. To them, it was a repeat of past experiences when a similar process was embarked. I thank you for the confidence and patience during this difficult journey. To my friends, students and colleagues, I thank you for all your input and criticism during the period of the study. To everyone who contributed towards this study, I extend my deep appreciation. I owe you all a debt of gratitude.

DEDICATION

It would be grossly unfair to ignore the support provided by my wife, Lillian (my pillar of strength; my loving children: Faith Rue; Joel Jnr and Charmaine Nokubonga, my sisters and friends who offered encouragement and inspiration throughout the course of this study. The period of this study was characterised by loss of a dear mother who was very inspirational and motivational in her own right. To you mom, Mrs Sarah Chigada, I say, rest in peace. I will forever cherish the good time well-spent together in this world. Not only were you my mother, but, you were my confidant and foundation for who I am today. The melodious voice when you sang those gospel hymns reminisces in my mind when I write this epistle in remembrance of a great mother you were.

In loving memory of my siblings, Albert, Thomas and Evermary, my father, Mrs Bumhira, for their pride and contentment with this achievement would have been indescribable. I dedicate this thesis to all of you. How time has flown very quickly, since your departure from this world, have I suddenly become a force to reckon with within the academia fraternity.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LEGISLATION IN SOUTH AFRICA

I. Broadband Infraco Act 33 of 2007
II. Common Law
III. Consumer Protection Act 68 of 2008
IV. Copyright Act 98 of 1978
V. Critical Infrastructure Protection Act (CIPA) 8 of 2019
VI. Cybercrimes Bill of 2019 (waiting for assent by the President)
VII. Cyber Warfare Strategy
VIII. Electronic Communications Act 36 of 2005
IX. Electronic Communications and Transactions Act (ECTA)25 of 2002
X. Financial Intelligence Centre Act (FICA) 38 of 2001
XI. Interception and Monitoring Prohibition Act (IMPA) 77 of 1995
XII. Independent Communications Authority of South Africa Act 13 of 2000
XIII. King Code IV
XIV. National Archives and Records Service of South Africa Act 43 of 1996
XV. National Cybersecurity Policy Framework
XVI. National Prosecutions Act 32 of 1998
XVII. Prevention of Organised Crime Act 38 of 1999
XVIII. Protection of Constitutional Democracy against Terrorism and Related Activities Act 33 of 2004
XIX. Protection of Personal Information Act 4 (POPI) of 2013
XX. Protection of State Information Bill
XXI. Protection from Harassment Act 17 of 2011
XXII. Regulation of Interception of Communications and Provision of Communications (RICA)

LIST OF ACRONYMS

ABSA	:	Amalgamated Banks of South Africa
AIS	:	Association for Information Systems
ANA	:	Africa News Agency
ATMs	:	Automated Teller Machines
BASA	:	Banking Association of South Africa
BBC	:	British Broadcasting Corporation
BYODs	:	Bring Your Own Devices
CAB	:	Copyright Amendment Bill
CECC	:	Council of Europe's Convention on Cybercrime
CIO	:	Central Intelligence Organisation
CIPA	:	Critical Infrastructure Protect Act
CNP	:	Card-Not-Present
COBIT	:	Control Objectives for Information and Related Technologies
COVID-19	:	Corona Virus Disease-2019
CS	:	Cyber Security
CSC	:	Cyber Security Culture
CSIRT	:	Computer Security Incident Response Team
CPD	:	Continuing Professional Development
DDoS	:	Distributed Denial of Service attack
DHA	:	Department of Home Affairs
DNA	:	Deoxyribonucleic Acid
ECTA	:	Electronic Communications and Transactions Act
EGCL	:	Existence of many Global Cyberlaws
EU	:	European Union
FATF	:	Financial Action Task Force
FBI	:	Federal Bureau of Investigations
FICA	:	Financial Intelligence Centre Act
FNB	:	First National Bank
FTP	:	File Transfer Protocol
GBV	:	Gender-Based Violence
GDP	:	Gross Domestic Product
HOIC	:	High Orbit Ion Cannon
ICASA	:	Independent Communications Authority of South Africa
ICT	:	Information and Communication Technology
IDASA	:	Institute of Democracy in South Africa
IDs	:	Identity Documents
IMPA	:	Interception and Monitoring Prohibition Act
IODSA	:	Institute of Directors South Africa
IS	:	Information Systems
ISACA	:	Information Systems Audit and Control Association
IT	:	Information Technology

ITU	:	International Telecommunications Union
JCPS	:	Justice Crime Prevention and Security Cluster
KIS	:	Knowledge and Information Sharing
LOIC	:	Low Orbit Ion Cannon
LMPRE	:	Law-Making Process and Regulatory Environment
M & G	:	Mail and Guardian
MAIS	:	Multiple Agencies and Information Systems
MC	:	Monitoring and Control
NA	:	National Assembly
NCAC	:	National Cybersecurity Advisory Council
NCII	:	National Critical Information Infrastructure
NCOPs	:	National Council of Provinces
NCS	:	National Cybersecurity Strategy
NPA	:	National Prosecuting Authority
PCS	:	People-Centric Security
PI	:	Principal Investigator
PICL	:	Pace of Implementation of Cyberlaws
PIN	:	Personal Identification Number
PIRLS	:	Progress in international Reading Literacy
POPIA	:	Protection of Personal Information Act
POS	:	Point-Of-Sale
PSP	:	Parliamentary Support Programme
RBV	:	Resource-Based View theory
RICA	:	Regulation of Interception of Communication Act
SA	:	South Africa
SABC	:	South African Broadcasting Corporation
SABRIC	:	South African Bank Risk and Information Centre
SADC	:	Southern African Development Community
SA-NCPF	:	South African National Cybersecurity Policy Framework
SAP	:	Systems Application Products
SARS	:	South African Revenue Services
SIC	:	Skills in Cybersecurity
SMEs	:	Small and Medium Enterprises
SSA	:	State Security Agency
SQL	:	Structured Query Language
UCT	:	University of Cape Town
UK	:	United Kingdom
UN	:	United Nations
USA	:	United States of America
USD	:	United States Dollars
UWC	:	University of the Western Cape
WEF	:	World Economic Forum
WHO	:	World Health Organisation

WiFi	:	802.11 x standards
Wits	:	University of the Witwatersrand

PART I

CHAPTER ONE: INTRODUCTION AND BACKGROUND

"Connecting any strategic infrastructure to the Internet makes it vulnerable to security threats, attacks and most government systems connected south are extremely vulnerable to hacking, data leakages and hijacking" (Khan, 2019:12)

1.1 Introduction

Advancements in technology are pushing businesses, big and small and individual members of society to use information and communication technologies to transact and communicate (International Telecommunications Union [ITU], 2019). Over-reliance on technology facilitates faster communication, information and knowledge sharing as well providing efficient and reliable services and products. Schwab (2019) states that technological advancements can facilitate the achievement of millennium development goals of poverty reduction and improving the standard of living. As firms embrace and adopt new technologies as part of their value chain, there is an emerging and worrisome scourge- of cybercrime. Quade (2020) states that due to the World-Wide-Web [WWW] (International connection of computers), the use of cloud computing services pushes firms to connect their strategic infrastructure to the Internet, thus, exposing the firm to cyber-attacks and threats. Cybercrimes are criminal activities carried out by cybercriminal syndicates on the Internet through the use of computers, smartphones, laptops and other Internet-enabled devices (Schwab, 2019).

The emergence of the global Corona Virus Disease-2019 (Covid-19) pandemic has contributed to the exponential growth of cyber-attacks on critical public and private information technology infrastructure resulting in loss of billions of USD (World Health Organisation [WHO], 2020). Given the recent surge and gravity of cyber-attacks on information technology (IT) infrastructure, cybersecurity has become a topical policy issue globally. Governments are challenged to provide the requisite regulatory and legislative frameworks and instruments to protect personal, private and public sector IT infrastructure against threat actors (Schwab, 2019).

Change and Coppel (2020) assert that the exponential growth of cybercrimes is not a government responsibility alone but everyone's responsibility. This calls for concerted efforts from all stakeholders to ensure that cybercrime is mitigated and combated. A comprehensive approach that includes the development of effective and relevant legislation, intervention strategies and appropriate punishment should be put in place to protect the integrity of national IT infrastructure (Chang & Coppel, 2020). The ITU (2019) argues that in order to prevent, respond and recover from cyber-attacks and threats, governments should develop a national information infrastructure protection strategy. For example, South Africa has developed the National Cybersecurity Policy Framework (NCPF) as part of the country's efforts towards a coordinated approach to fight cybercrime. The effectiveness of the NCPF envisages a coherent multi-stakeholder strategy approach considering the role of each stakeholder within the framework to facilitate international cooperation (ITU, 2019). Bote (2019) acknowledges the importance and objectives of the NCPF, but is cautious that the SA-NCPF is not effective due to a myriad of elements that interplay resulting in complex relationships that hinder the NCPF's objectives. Pokwana and Kyobe (2016) assert that complex relationships between influencing factors affect the alignment of the NCPF to national, regional and international cyberlaws, which gives cybercriminals some leverage. Though cyber-legislation and other interventions are required to address cybercrime, human behaviour is the nexus to all cybercrimes (Malatji, Marnewick & von Solms, 2021).

Currently, South Africa's cyberlaws are coordinated by different government agencies, creating windows of opportunities for inconsistencies, fragmentation and misalignment, thus, weakening initiatives for an effective national cybersecurity strategy. Mahlobo (2015) also acknowledges that different government agencies have overlapping mandates resulting in information asymmetries and poor coordination. Pokwana and Kyobe (2016) posit that civil society, public and private sector institutions are not well-versed with cybercrimes, let alone understanding and interpretation of legislation. Thus, firms and individuals fail to comply with cyber legislation. With reference to the prevailing circumstances, this study also analyses the gaps in the country's cyberlaws and ascertain if the substantive laws criminalise and successfully prosecute cybercrimes. Furthermore, the researcher states that in order to successfully investigate and prosecute cybercriminals, the legal fraternity, cyberlaws and well-equipped and trained well-trained law enforcement agencies should be pooled together and work harmoniously.

1.2 Contextual Setting of the Study

The nexus of this study is the South African Cybersecurity Regulatory Environment which developed the country's national cybersecurity policy framework. Most companies and civil society adopt and utilise ICTs to access the global markets, thus, company information systems, data, people, information and computing resources are exposed to cyber-attacks and threats (Schwab, 2019). The recurring and growing threats to cyberspace should not deter economic growth, rather cyber-threats and all forms of data breaches should be a source of motivation for innovation for the information society (Khan, Brohi & Zaman, 2020). Every economy is concerned about the escalating rate of cybercrime; therefore, various intervention strategies are put in place to mitigate these challenges. It is acknowledged that single intervention strategies might not be adequate or effective deterrents, therefore, a series of interventions should be implemented simultaneously to determine which combinations of strategies are effective. The researcher acknowledges that though, it is welcome to implement different interventions, the challenge is to determine which interventions yield the desired results-vis-à-vis mitigating cybercrime. The main limitations confronted include a lack of human skills, financial resources and know-how to manage a two-pronged intervention approach. For example, South Africa's has developed and implemented various pieces of e-legislation to combat cybercrimes and these efforts should be complemented by other intervention approaches through public, private sector organisations and civic society support. As pointed above, the country faces an acute shortage of skilled cybersecurity professionals, thus, pose challenges to the whole cybersecurity strategy. In addition, the pieces of legislation are managed as silos resulting in information symmetry. However, cyber criminals are becoming sophisticated and evading detection or arrests, therefore, complex information security strategies are required now more than ever. Misaligned and complex regulatory systems compound the challenges and posit more headaches for governments and organisations fighting all forms of Internet mediated criminal activities.

Johnson (2017) states that fragmented national cybersecurity policy e-legislations are fraught with inconsistencies and it is the prerogative of government to put contingency measures in place to ensure these laws are effective. The ITU (2019) states that development and implementation of national cybersecurity laws is not the panacea to addressing cybercrimes, but, civil society, public and private sector firms should be part of the nation's information security strategy. This active participation is feasible if there is a good level of understanding

of cybercrimes. With reference to the South African context, the coordination of different pieces of e-legislation creates complexities to understand, resulting in non-compliance by many firms (Malatji *et al.,* 2021). Attributable to these challenges is the aspect of inconsistencies found in the country's e-legislation (Mahlobo, 2015; Bote, 2019). Fragmentation violates the principles of Systems theorists who advocate for tightly interdependent elements that work together to achieve a desired outcome (Bertalanffy, Rapoport & Gerard, 1956). Bertalanffy *et al.* (1956) state that various elements in an organisation interact with each other forming patterns or relationships that can determine the behaviour of the organisation. Therefore, these patterns or relationships work towards unity. Malatji et al (2021) states that due to the level of fragmentation and misalignment of South Africa's cyberlaws, perpetrators of cybercrimes know that the risk of being detected and prosecuted is very low. People committing cybercrimes in different countries may not be investigated in other countries due to the fragmentation and misalignment of cyberlaws between member states (van der Merwe, 2016; Bote, 2019).

1.3 Definition of Terms/Concepts

This section defines key terms that inform the study.

Alignment: Hsiao and Omrod (1998) and Maes, Rijsenbrij, Truijens and Goedvolk (2000) agree that alignment is the synergy emanating from the coherence of various organisational components. The interplay between these organisational elements should be sustained over a period of time to an adequate level of coherence which will drive towards competitiveness.

Coherence: Given the context of strategic management, organisational elements interplay to form relationships that will lead the organisation to achieve superior performance than competitors (Mimbi, 2014). For example, coherence between strategy and organogram describes the extent to which a firm's organogram and strategy are aligned to enhance organisational performance.

Configuration: Configurations are patterns or Gestalts formed by the interaction and interplay between various organisational elements. When organisational elements achieve an adequate level of coherence over a period of time, organisational performance improves (Venkatraman,1989).

Cybercrime: The researcher defines cybercrime as any unlawful activity perpetrated by a criminal through Internet-based transactions with the intention of destroying, inflicting emotional, psychological harm, financial loss and reputational damage to a person of organisation.

Cybersecurity: Raimundo and Rosario (2022:2) state that "cybersecurity is concerned with the protection of electronics, software and data along with the procedures by which systems are accessed". Therefore, security objectives comprise privacy in terms of information not inappropriately disclosed to unauthorised devices or individuals to be destroyed or modified (Furstenau et al., 2021). The word "cybersecurity" comprises the prefix "cyber" and concept "security". Cybersecurity is a multidisciplinary approach where technological and non-technological mechanisms are pooled together to fight cyber-attacks and threats focusing on the security of assets with a presence in cyberspace. Thus, when discussing cybersecurity, one as to be cognisant that information security is contained by cybersecurity. Information Systems Security: Quite often, many people tend to confuse information systems security to have the same meaning as cybersecurity, yet the two are different by related. The World Economic Forum [WEF] (2019) defines information systems security as all interventions or proactive actions taken by an organisation to protect its information and information systems assets. Organisations use both internal and external processes to prevent destruction of company information assets (Raimundo & Rosario, 2022).

Gestalts: Patterns or configurations emanating from interactions between different organisational elements (Venkatraman, 1989). The elements should achieve an adequate level of coherence over a period of time to influence effectiveness or unity with each other.

Information Systems: In order to collect, process, store or distribute information, organisations require a set of interrelated components namely: people, task, technology and roles to achieve that. These components form an Information System. The absence of one element destabilises the functionality of the information system (Laudon & Laudon, 2017).

Knowledge: Nonaka and Takeuchi (1995) define knowledge as a state of knowing something. Therefore, people gain experiences over a certain period of time and then use that experience for to generate new insights. Knowledge is superior than information (Ngulube, 2019). A firm

with superior knowledge assets has better chance of performing better than one that does not have knowledge assets (Ngulube, 2021).

Legislation: Legislation refers to laws of the country (van der Merwe, 2016). For example, there are different pieces of cyberlaws developed to address specific types of cybercrimes.

Legislative framework: The Constitution of South Africa (108 of 1996) defines the legislative framework as a combination of the country's laws (Acts), procedures, policies and instructions put together to protect the citizens of the country. Each legislation has specific provisions and penalties for any successfully prosecuted individual.

1.4 Problem Statement

The development and implementation of South Africa's crime-related framework is impeded by many misaligned, fragmented and complex regulatory policy reforms that inhibit the country from addressing cybersecurity challenges (Mahlobo, 2015; van der Merwe, 2016; Bote, 2019). The country has been struggling to achieve key objectives of the national cybersecurity strategy because the objectives are distributed among thirty-seven (37) or more different pieces of legislation that are poorly coordinated (Malatji *et al.*,2021). Due to fragmentation and inconsistencies, the country's national cybersecurity policy framework is ineffective and misaligned to regional and international cyber laws (Bote, 2019). Furthermore, there is a paucity of studies to suggest the existence of a comprehensive approach to the development of an effective national cybersecurity strategy because civic society, private and public sector companies are not conversant with cyberlaws in the country (Ntsaluba, 2018; Bote, 2019).

Mahlobo (2015); Schultz (2016) and Bote (2019) state that misaligned and inconsistencies in cyber legislation compound the misunderstanding of cyber legislation among people and businesses as well as perpetuating national, regional and international cybersecurity challenges. Past studies have failed to address the challenge of alignment of the SA-NCPF as pointed by Malatji *et al.* (2021). The authors state that after the NCPF was gazetted in September 2015, different researchers have interrogated the merits and demerits of the NCPF, resulting in a general consensus that the development of the country's NCPF did not consider global cyber laws, thus, resulting in its ineffectiveness. The absence of a comprehensive approach to the

development and supporting legislation and policies contributes to misalignment of the NCPF (Malatji *et al.,* 2021). Therefore, the motivation for conducting this study is to determine how influencing factors contributing to misalignment can be aligned and measured to ensure an effective NCPF is achieved?

1.5 Research Questions

With reference to the discussions in the contextual setting and the existing gaps in IS research, the following research question will guide the study:

The Primary Research Question

- How can influencing factors be measured and aligned to facilitate an effective South African National Cybersecurity Policy Framework?

1.6 Aim of the Study

The aim of this study is to measure and align influencing factors to achieve an effective NCPF in South Africa. The lack of studies on the alignment of the SA-NCPF has contributed to the limited understanding of cyber legislation and its application by many people and organisations in South Africa. Measuring the extent of alignment of cybersecurity policy frameworks has been problematic for many researchers (Macintosh & Whyte, 2006) because of the complexities arising from interplays between different elements involved in the coordination of cybersecurity legislation. A new approach to measure such a complex interplay is required by the SA government, private and public sector organisations and society to demonstrate the benefits of an effective Cybersecurity Policy Framework. It is also important to identify the influencing factors because these can inform government and organisational policies.

1.7 Contributions of the Study

1.7.1 Originality/Value

For long, people and businesses have been ceased with the concept of cybersecurity and its impact on the global economy. Guetzkow and Lamont (2004) posit that research should present new discovery that adds new knowledge. This results in originality of knowledge or value of the study. In this study, the researcher has been exposed to the concept of Gestalts for the first

time and has dutifully applied the theory to understand and explain alignment of cyber laws. After reviewing a number of studies, the researcher was convinced that this study is the first attempt to measure the alignment of the South African National Cybersecurity Policy Framework. This research has resulted in new knowledge on why the SA-NCPF is misaligned. It has also developed a novel method for suing the concept of Gestalts to understand and explain alignment of cyber-laws. Chigada and Kyobe (2018) agree that measuring alignment of the SA-NCPF has been a major challenge for many scholars and researchers in South Africa because of the complexity of multiple factors interacting with each other.

1.7.2 Theoretical and Methodological Contributions

The development of the integrative theoretical framework brought together various theories that helped to explain and understand the South African law-making process and why it is a very slow process. The researcher identified nine influencing factors which continuously interacted with each other producing complex relationships. When elements at the organisational level interact, the relationships become so complex to understand by linear relationships. Hence the need to look at and measure the relationships as Gestalts. Therefore, the first major contribution of the thesis was the development of the Gestalts model for measuring alignment of the influencing factors. The extent to which these factors influence each other is not known, therefore, the conceptual model was developed to measure extent of alignment that would achieve an effective NCPF. Miller (1991) states that Gestalts view individual interactions between pairs of elements only as part of the overall pattern/configuration.

This study adopted the Cluster-based configuration perspective to distinguish, describe and predict the degree of alignment of the SA-NCPF. The cluster-based configuration provided a valid measurement of alignment of the SA-NCPF which is a major methodological contribution of the thesis. The researcher was convinced that the integrative, conceptual model and adoption of the Gestalts approach were the first attempt in South African studies to address the challenge of alignment of the NCPF. This is in line with the assertions of Malatji *et al*. (2021) who admit that past studies have concluded that the NCPF is misaligned and ineffective due to a number of reasons, some of which are the influencing factors described in this study. However, there is a dearth of studies that have addressed the challenge of alignment.

1.7.3 Practical Contribution

The misalignment of the SA-NCPF is caused by the lack of IT and cybersecurity legal skills, fragmented pieces of legislation, poor coordination of legislation by multiple government departments, slow pace in the law-making process and the fast-paced rate of sophisticated cybercrime space. In addition, the global village is grappling with Corona Virus Disease-2019 on hand and cybercriminals taking advantage of the overreliance on Information Communication Technologies (ICTs) during this pandemic. The complexity of cybercrimes during the global Covid-19 pandemic exerts pressure on governments and economies that do not have IT and legal skills in cybersecurity, effectively, exposing many countries and companies to cyber-attacks and threats (WHO, 2020; WEF, 2020). An adequate level of coherence is attained when influencing factors support and reinforce each over a sustained period of time. The study identified many areas that require interventions and revision of the NCPF. Education, awareness and involvement of everyone in society helps to develop a cybersecurity culture in South Africa.

Given the context of the global Covid-19 pandemic, it is high time that a strong partnership should be formed to fight both pandemics simultaneously. This study is important because it raises fundamental issues that the country should invest in the development of IT and legal skills in cybersecurity as well as the need for technology preparedness. The transition to online business transactions caught many people and industries off-guard, and in the midst of trying to assimilate to working remotely, windows of opportunities for cybercrimes have been rising (WHO, 2020).Whilst the global economy is focusing on the Covid-19 pandemic, cybercriminals are busy with their nefarious acts, thus, the current thesis is fundamental to what is presently happening globally, that both legal, technological, non-technological, tools, practices and interventions should be developed and implemented at a faster pace if the country is to develop and implement an effective national cybersecurity strategy. Events occurring at the time of compiling this research study, require a paradigm shift and complete overhaul of the law-making process and coordination of cyber-legislation. This thesis has drawn theories from other disciplines in order to obtain rich insights thus, the confirming the multidisciplinary approach of the thesis.

1.8 Scope of the Study

This study examines factors that impede the alignment of the South African National Cybersecurity Policy Framework. Therefore, the researcher tries to unpack the concept of alignment and how influencing factors can be measured to determine the extent of their alignment. South Africa is a developing economy but is regarded as the most advanced economy in Africa, therefore, it is revered in high esteem. This includes its influence on economic, legal, technological and political prowess in the South African Development Community (SADC). The SA-NCPF has a bearing on most SADC member states, thus, it was important to include a few of them in the study because they were development their own country's cybersecurity policy frameworks. The emphasis of this study is placed in the misalignment of the SA-NCPF with national, regional and global cyberlaws. Though the concept of information systems security is briefly discussed to demonstrates its relationship with Cybersecurity, it is not the nexus of the study.

1.9 Research Design

1.9.1 Paradigm/Design/Methodology

The study examined influencing factors that contributed to misalignment of the SA-NCPF. Thus, scholarship from various disciplines was reviewed to obtain a better understanding and explanation of the concept of alignment. Diverse theoretical works were consulted and adopted to explain the various elements existing in the concept of alignment resulting in the development of an integrative theoretical framework. The study used the integrative theoretical framework to explain and understand interactions between the influencing factors. Ntsaluba (2018), Bote (2019) and Malatji *et al.* (2021) state that researchers have been grappling with the challenge of measuring the extent of alignment of the SA-NCPF with no breakthrough. After identifying gaps in past studies and literature, the study used the integrative theoretical framework and Gestalts approach to develop a conceptual model which guided the researcher to assess and test the degree of alignment of the NCPF.

The nature of the research problem was complex to understand from a human perspective, therefore, to obtain knowledge about the phenomenon at hand, the researcher adopted an objectivist ontological stance. The focus of objectivism of the scientific neutrality stems from positivist assumptions that knowledge is derived from the experience of natural phenomena

and their attributes (Creswell, 2012). Guba (1990) states that verified data obtained from senses is based on empirical evidence which is verified through scientific methods or logical reasoning. In this study, the objectivity of scientific discourse was understood as the researcher's detachment from the object. An online and hand delivered questionnaire was used to collect quantitative data from people with knowledge and understanding of cybersecurity, thus, providing empirical, observable and measurable evidence. This empirical evidence was premised on the principles of deductive reasoning to arrive at logical conclusions (Onwuegbuzie & Leech, 2005). The ultimate goal was to integrate and systematise research findings into meaningful theory which is regarded as the truth (Creswell & Plano Clark, 2011).

A quantitative research design guided the research procedures in data collection, analysis and interpretation. Data were collected from a diverse population of people who were key leaders from academia, legal, political, policy-making, Information Technology, Information Systems, Computer Science, Cabinet with a vested interest in the SA-NCPF. The conceptual model and propositions were tested through the lens of Cluster analysis on all quantitative data gathered for the study. Chapter five (research design and methodology) of this thesis presents a detailed discussion of the philosophical stance and research methods that underpin the study.

1.9.2 Research Limitations/Implications

The study confronted methodological limitations. First, there were no previous studies on the topic under study, thus, the theoretical underpinnings of literature on alignment of the SA-NCPF were limited. The second limitation was attributed to the Gestalts approach which was used in an unpredictable environment due to the global Covid-19 pandemic. Cybercrimes are growing at an exponential rate; thus, the cyberspace is uncertain, limiting the ability of managers to make decisions (Soin & Paul, 2013). Addressing the concept of alignment should be an ongoing process because it constantly changes the contemporary business environment. The set of relationships existing between organisational elements is temporary, thus, these changes need to be studied over time. Due to interactions between organisations and the emergence of the global Corona Virus Disease-2019 (COVID-19) pandemic, measures of alignment should be cognisant of the challenges of conducting fieldwork in the context of social distancing and other health protocols, thus, a longitudinal study would be ideal.

The target population for the study were information systems professionals, legal experts, lawmakers and information systems and legal academics. This is in line with the GCSCC which

involved academia, cybersecurity experts, private & public sectors, policy-developers etc in the development of the CMM. The goal of this thesis was to obtain relevant insights from professionals working with the domain of cybersecurity. Members of civil society were excluded from study, whose responses could have changed the findings of this study. In addition, a mono-quantitative research method was used, therefore, the voice of the respondent was not heard. Ngulube (2019); Saunders et al (2019) state that the use of a mono-method has pros and cons, as has been admitted by the author of this thesis. This would have been ameliorated if a mixed method research had been adopted, where both qualitative and quantitative data were collected.

The author of this thesis identified that some of the questions probing the degree to which respondents believe the various issues identified through the survey work are relevant, use negative language, therefore, one might conclude that the results could be biased towards the preconceptions of the author. This is not true in every aspect of the survey, for example the section on cybersecurity culture has examples of positive language and reverse framing of questions where high scores indicate evidence of alignment.

1.10 Structure of Thesis

There are four parts in this thesis- Part I, Part II, Part III and Part IV. The parts are logically arranged to serve distinct areas of the thesis. Figure 1. below presents the structure of thesis indicating these four parts and their corresponding chapters.

Part I: Introduction and Background

This is the introductory chapter of the study which provides the background and problem statement. In addition, Part I presents an overview of what the study is all about. To accomplish this goal, Part I contains only one chapter which is divided into chronologically arranged subsections. The scope of the thesis, contributions, limitations and research design of the thesis are presented.

Part II: Literature Review and Theoretical Framework

Chapter 2: Cybercrimes and Cybersecurity

The concepts of cybercrime and cybersecurity are key to this study; therefore, a considerable amount of time is spent unpacking the concepts. In addition, the author of this thesis discusses

factors contributing to exponential growth of cybercrime, cybercrime in public and private sectors in South Africa, impact of cybercrime and intervention strategies to address cybercrime.

Chapter 3: The South African Regulatory Environment

This chapter highlights the historical developments and South African Regulatory Environment. The nucleus/nexus of the literature review is the law-making process and pieces of legislation enacted to mitigate cybercrime. Lessons drawn and comparisons made from the law-making processes of UK, USA and Australia will synthesise the arguments that the flaws in the South African regulatory environment which contributed to the alignment challenge.

Chapter 4: Theoretical Framework

In this chapter, the researcher discusses the Configurations/Gestalts Theory that guided the research, while determining what data will be measured and what statistical relationships will be looked for. Other theoretical works are discussed to better understand the problem under interrogation. Theoretical frameworks are imperative in quantitative research projects because they help to test/verify what is already known rather than develop new theories.

Part III-Research Design and Methodology

There are two chapters in Part III

Chapter 5: Research Methodology

This chapter discusses the research methodology employed in this study. The research plan is defined, outlined and discussed showing key tenets/concepts integrated to conduct this study to completion. The research process is a fundamental component of all research studies because it articulates the involvement, attachment or responsibility of the researcher from the inception to the end of the study. A detailed discussion of key concepts is presented in the chapter for better understanding of how the research was conducted to its successful completion.

Chapter 6: Analysis, Interpretation and Discussion of Findings

These results are analysed, interpreted and presented in a logical sequence. This is an important aspect to note because it helps the researcher to address the research questions in the ways they would have been developed and postulated in the study. The researcher links back the results to the methods of analysis to ensure a justification for their choice.

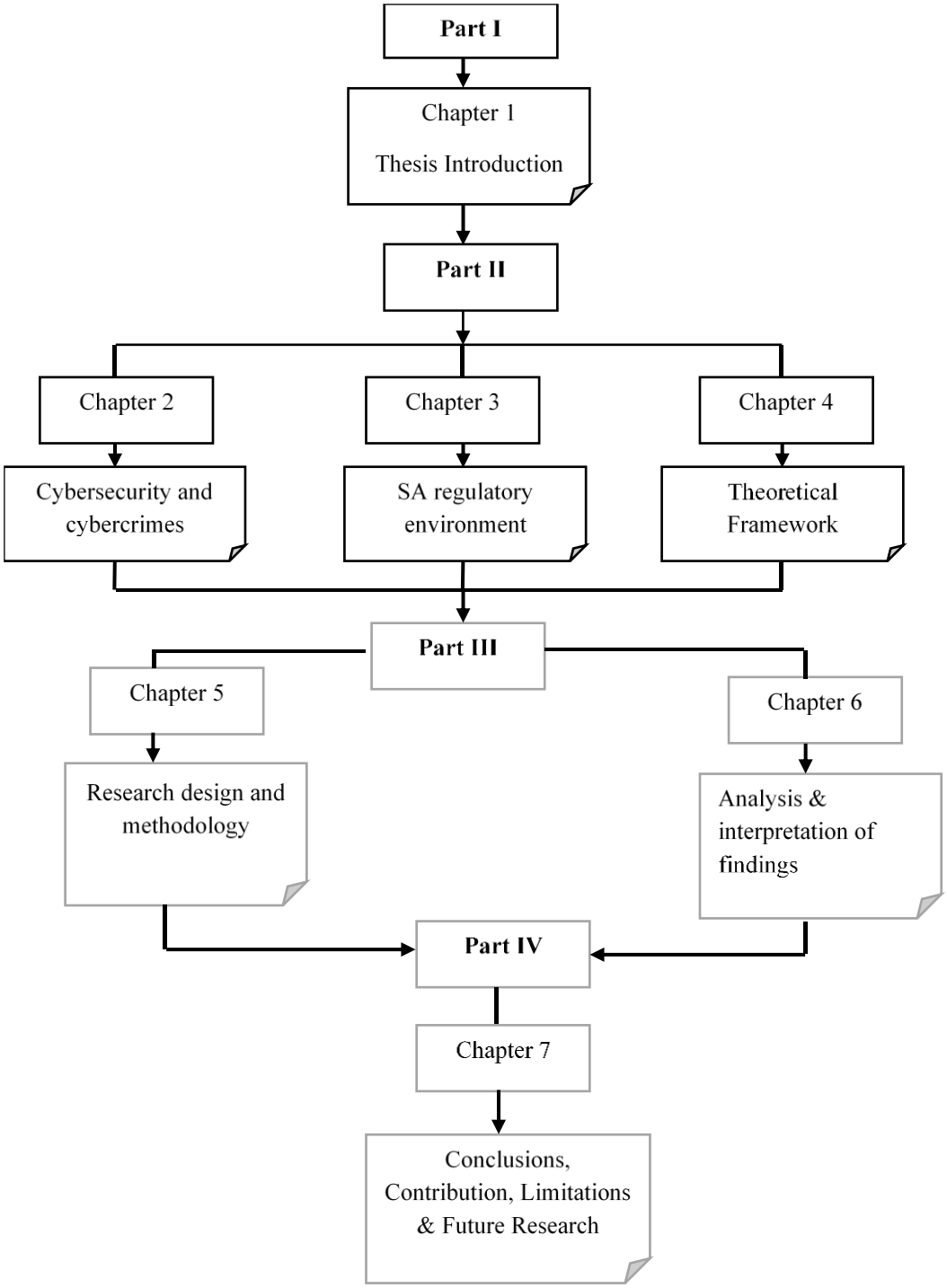

Figure 1.1: Structure of Thesis (Author, 2021)

Part IV- Conclusions, Recommendations and Research Implications

The last part of the research study comprises one chapter.

Chapter 7: Conclusions, Recommendations and Implications of Study

The last chapter of the study- chapter seven, present conclusions, recommendations, implications, limitations and major contributions of the study. For future research, the study recommends that a longitudinal study would best address the limitations faced in this study so that a better understanding of the alignment challenge can be addressed. Furthermore, future research should also interrogate interventions to address cybercrimes especially in the context of the global Covid-19 pandemic because of the exponential rise of cyber-attacks and threats when the global is grappling with deadly health pandemic.

1.11 Chapter Summary

The essence of this chapter was to present a succinct problem statement and its contextual setting why it is was worth the investigation. The alignment challenge has been there for a long period of time and past research studies have failed to address or find alternative solutions to ensure South Africa has an effective National Cybersecurity Policy Framework that would guide the development of an effective national cybersecurity strategy. Therefore, the aim of this study demonstrates clearly that the challenge of alignment should be resolved for the country to have an aligned NCPF. This would be achieved by developing an integrative theoretical framework that provides a detailed explanation of the influencing factors and their interactions. Because of the complexity of relationships that come from interplays, the thesis adopts a Gestalts approach to complement the integrative theoretical framework in the development of the conceptual model that will help measure the degree of alignment of the NCPF. The chapter also presented major contributions, limitations and delimitations and an overview of the research methods of the study. In part II, the researcher reviews literature relating to cybercrimes, cybersecurity, the South African regulatory environment and theory of alignment.

PART II

LITERATURE REVIEW AND THEORETICAL FRAMEWORK

CHAPTER TWO: CYBERCRIME AND CYBERSECURITY

In the age of cybercrime, the greater danger is not defence imperfection, but to protect first what not really matters (Nappo, 2018)

2.1 Introduction

In chapter one, the research problem, its contextual setting, objectives and methods of addressing the alignment problem were clearly presented. That discussion led the researcher to review appropriate literature pertaining to the research problem. Thus, the current chapter discusses cybercrime and cybersecurity. The chapter starts by defining cybercrime and discusses the concept of cybersecurity, types of cybercrimes and how they are perpetrated. Factors contributing to the escalation of cybercrimes in South Africa, impact of cybercrimes and cybersecurity are key discussions presented in this chapter. The discussions in this chapter are fundamental to understanding the subject (Cybersecurity) being investigated. Reviewing scholarly works from other researchers helps to synthesise ideas and arguments presented in the current study. Interrogating literature exposes the researcher to write authoritatively about the subject. In the age of cybercrime, the greater danger is not defence imperfection, but to protect first what not really matters (Nappo, 2018).

2.2 Cybercrime

The ITU (2019); WHO (2020) both agree that illegal activities perpetrated using computers or laptops, smartphones or other Internet-enabled devices define cybercrime. The objective of these illegal activities is to steal information, data, tamper, extort or delete information, data assets as well as destabilise IT infrastructure (Khan *et al*, 2020). Anastasiou, Androutsou, Costarides, Pitoglou and Giannouli (2020) state that cybercriminals use modern technologies to illegally access company networks or cellphones, resulting in cybercrime. Chang and Coppel (2020) define cybercrimes as the ability of threat actors to infiltrate a company's IT

infrastructure remotely with the intention of stealing from the company or individual. The authors further state that in many instances, friends, family and workmates share personal devices which might not be password protected, thus, exposing their credentials to criminal elements. Mohan, Gowda and Vickyath (2020) define cybercrime as "acts" punishable by the Information Technology Act. Given the different perspectives of definitions of cybercrime, the researcher concludes that there is no universally accepted definition. In light of the above, the researcher defines cybercrime as any unlawful activity perpetrated by a criminal through Internet-based transactions with the intention of destroying, inflicting emotional, psychological harm, financial loss and reputational damage to a person of organisation. This definition captures the major tenets of the above definitions and as such will be applied in this thesis.

The first recorded act of cybercrime was recorded in 1820 in France. Joseph Marie Jaqcuard developed the loom designed to perform repetitive weaving tasks in the textile manufacturing industry in France. Fear engulfed Jacquard's employees who felt their lives and jobs were threatened. In order to discourage Jacquard from improving the weaving processes, employees sabotaged the efforts and this is the first record of cybercrime. Over the last two years, cybercrimes have been increasing at an exponential rate. The emergence of Covid-19 in December 2019 has contributed significantly to the scourge. Cybersecurity experts, the World Health Organisation, Centre for Disease Control, financial and healthcare institutions and government departments are the major targets of cyber-attacks and threats because of big data. Threat actors are cognisant that large institutions process and store large volumes of client or patient information, which, in many instances contain identity documents, banking details, addresses and contact details. This information has a ready grey market with buyers prepared to pay a lot of money with the knowledge that they would get more money from their criminal acts (Bowen & Seth, 2020). Hamman, Hopkinson, Markham, Chaplik and Metzler (2017) identify two cyber typologies (cyber-attack typology and cybercrime-typology).

2.2.1 Cyber-attack typologies

Hodges and Creese (2015:34) define a cyberattack as an *electronic system, enterprise or individual that intends to disrupt, steal or corrupt assets where those assets might be digital (data, information or user account) or physical asset with a cyber component (process control system found in a building, nuclear refinement facility). Cyber-attacks seek to compromise the confidentiality, integrity or availability of digital assets; therefore, cyber security controls seek to protect these properties in some way.* Given the above definition and focus of this thesis, the

researcher chose a few cyber-attack topologies and cybercrime topologies that resonate with the foci of arguments.

2.2.1.1 Hacking

Mohan *et al.* (2020) define hacking as deliberate criminal act perpetrated by an intruder when one gains an unauthorised access to an information system. Usually hackers are computer programmers with an advanced understanding of computers and the majority of incidents are nuisance attacks rather than serious malicious attacks, victims still suffer financial losses. Mohan *et al.* (2020) emphasize that hackers have expert level skills and intrude into the privacy of systems to show-off their expertise. Some firms are hiring hackers in an attempt to find out flaws in the company's security systems and help fix them. Interesting Dennis Ritchie and Ken Thompson, founders of the UNIX operating system and Mark Zuckerberg of the Facebook (Meta) fame are good examples of computer geniuses or famous hackers (Bowen & Seth, 2020). Hackers can access systems through structured query language (SQL) injections, theft of file transfer protocol (FTP) passwords and cross-site scripting (Laudon & Laudon, 2017). At least 45 million computers, globally, were damaged by a love-bug virus that was released on the 4th of May 2000 (British Broadcasting Corporation [BBC] News, 2000).

For example, serious cases of hackings recorded to date include the Yahoo (2013-2014) where the 3 billion users' accounts were hacked into and compromised while the Internet giant was still negotiating the sell to Verizon. Yahoo (2014) admitted that this massive hacking was attributable to unacceptable user behaviour because the crime was an inside job. A robust crypt algorithm was used to steal more than 500 million users' information. This crime was committed at a time when Yahoo was in the process of disposing its stake to Verizon, thus, there was a serious financial loss of three hundred and fifty million United States Dollars from the sale price (Verizon, 2016). In November 2018, the Marriott International Group of hotels was seriously exposed to cyber thieves who stole information for more than 500 million of the hotel group's customers worldwide (Biag, Chenyshev & Zeadally, 2018). More than 400 million customers' information amassed over a 20-year period was stolen from the hotel group's six databases, resulting in cybercriminals decrypting credit card details on the Adult Friend finder information system (Quade, 2020).

eBay became a victim in 2014 when attackers accessed data for more than 145 million users. Access to the company's information system was gained by using the credentials of three

corporate employees. This breach resulted in decline of user activity (Donahue, 2017). Attackers accessed sensitive information (social security numbers, birth dates, addresses and drivers' licence numbers) for 143 million customers on the Equifax database in July 2017 (Equifax, 2017). In June 2018, South Africa, Liberty Holdings customers' details were illegally accessed by attackers who breached the email repository and started demanding a ransom so that they could release the company' information (Liberty Holdings, 2018). The South African Master Deed's database was breached in October 2017. Over 60 million South Africans' identity numbers, company directorship was compromised (ITWEB, 2017). Fin24 (2017) reports that 7 million Ster-Kinekor South African customers fell victim to data breach because the company's online booking system.

The Life Healthcare group in South Africa was hacked in June 2020, thus, the group's admissions, business processing systems and email servers were severely affected (Fleckenstein& Fellows, 2020). This demonstrates that cybercriminals invest more efforts, time and planning studying weaknesses in systems and then attack when the organisation least expects or is not prepared. Anastasiou *et al.* (2020) posit that hacking, financial fraud, identity theft and distributed denial of service (DDoS) attacks are some of the major challenges rising during the era of Covid-19 pandemic. With reference to the above incidents, it would appear cybercriminals are winning the war of cybersecurity as they put the country on the back foot- South African businesses have been put to sword. Everyone is focusing on the deadly Covid-19 pandemic which is affecting productivity and economic growth. Given the context of limited skilled human capital, organisations and government are failing to manage a double pandemic- cybersecurity on one hand and Covid-19 pandemic on the other. The WHO (2020) and United Nations [UN] (2021) concur with each other that professionals and non-professionals are dying due to Covid-19, thus, this has adverse effects on the skills development. Globally, there has been a report of a serious shortage of IT skills. The emergence of Covid-19 will exacerbate the problem (Hockey, 2020).

2.2.1.2 Virus Dissemination

Chenthara, Ahmed and Whittaker (2019) define a virus as a computer program that attacks or piggy-backs to other executable system software with the intention of causing harm. The virus attack sometimes causes severe damage to systems or file. Virus dissemination is a common cyber-attack where criminals generate and send viruses that attach themselves to infect a system or files and can easily circulate to other computers. Viruses disrupt systems operations

and can modify and delete files (Gaspereniene, Remeikiene & Schneider, 2017). System users receive email attachments that appear legitimate, yet they are viruses that replicate. Viruses can be spread through removable media, or the Internet.

Stewart, Chapple and Gibson (2018) state that several Trojan generator tools enable cyber hackers to create their own customised Trojan Horses (viruses) which can be passed from one system to the other undetected through security tools. These customised Trojan Horses can pass from system to system undetected because they do not match any known signatures. Recently, emerging Trojan kits include: Senna Spy Generator; Trojan Horse Construction kit v2.0; Progenic Mall Trojan Construction Kit and Pandora's Box (Chenthara *et al.,* 2019). Cybersecurity experts acknowledge that malicious activities involving viruses are affecting systems whilst allowing hackers gain access to the system. Viruses are classified according to what and how they infect. Viruses can infect the following: systems sectors; files; Macros; companion files like DLL and INI; disk clusters; batch files and source code (Arewa, 2018). Trojan Horses are different from worms and viruses in their manner of propagation. Trojan Horses masquerade as legitimate files (for example an email attachment to a friend), then intended recipient opens the attachment, meanwhile, will be installing a Trojan Horse program (Chenthara *et al.,* 2019). In addition, viruses have infection techniques which include: polymorphic; stealth; fast and slow; sparse; armoured; multipartite; cavity (space-filler); tunnelling; camouflage and active directory. The illustration in Figure 2.1 summaries the discussion presented above.

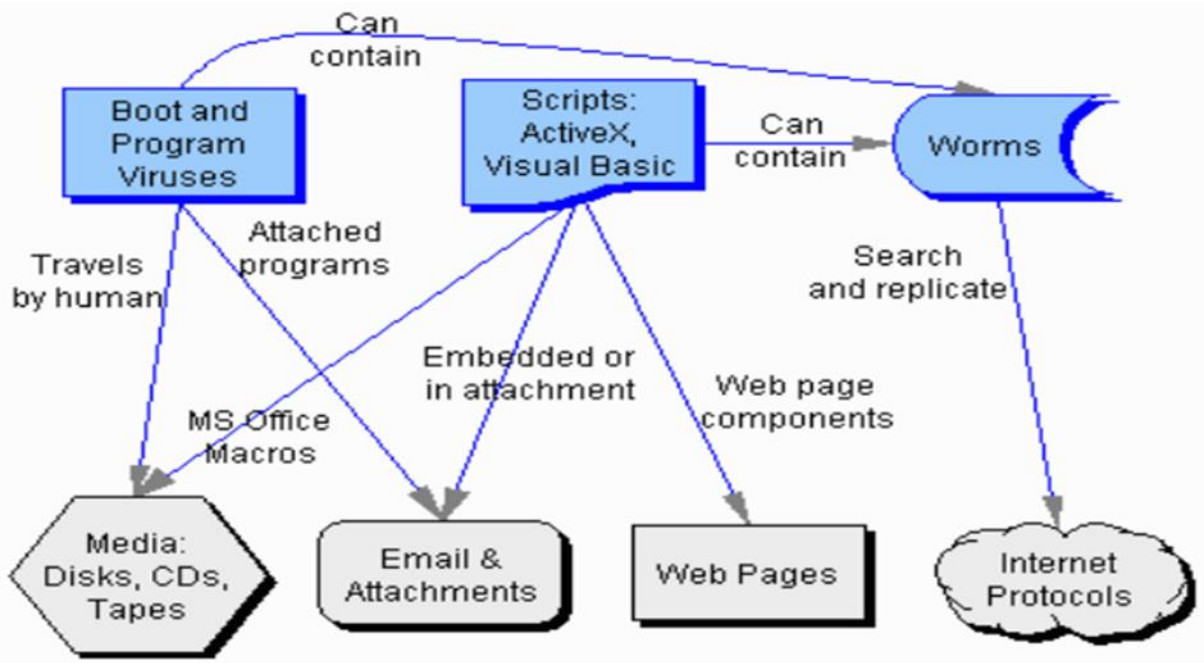

Figure 2.1 Virus Dissemination (Chenthara, Ahmed & Whittaker, 2019)

2.2.1.3 Logic Bomb

As the name implies, the slag code or logic bomb is also a deadly code that is inserted into operating and application systems and then explodes when activated under certain conditions (Chenthara *et al*., 2019). When employees are not happy with some employment conditions or disgruntled, they can engage in unscrupulous behaviour including development of logic bombs. A good example is the infamous "Friday the 13th" virus which attacks systems on specific dates (Abukari & Bankas, 2020). Hackers are known to hide pieces of code that harms the system by deleting files such as salary database trigger if the company attempts to terminate the codes from the company. Logic bombs were set off using codes on March 20, 2013 disrupting banking and broadcasting IT infrastructure in South Korea. Cybercriminals set the logic bomb so that it can dictate the date and time to explode erasing files and records from the computer (Dusane & Pavithra, 2020). All hard drives and master boot records were wiped out, putting out some automated teller machines (ATMs) out of service and disrupting all banking transactions. The logic bomb comprised files- AgentBase.exe which triggered the wiping. Inside the AgentBase.exe file was a hex string (4DAD4678) that indicated the exact timing the attack was to take place (FortiGuard Labs, 2014). When the internal clock hit 14:00:00 time, the wiper overwrote the hard drive and master boot record forcing the systems to reboot and send messages to users on their screens. The message was, "Boot device not found. Please

install an operating system on your hard disk". In a state of confusion, users who responded to the message triggered the deletion of files (Dusane & Pavithra, 2020).

2.2.1.4 Distributed Denial-of Service attack (DDoS)

The ITU (2019) indicates that Distributed Denial-of Service attack (DDoS) is perpetrated when threat actors and attackers clog the bandwidth denying legitimate users from access computing services. Computer resources are flooded with unnecessary requests that clog the bandwidth. The presence of DDoS slows down the server or crash so that no user can access it. Normal operations are disrupted creating challenges for the organisation or individual to halt business activities because the attacks are aimed at the network or server resulting in traffic congestion (Makridisa & Smeets, 2019). As shown in Figure 3 below, the attacker sends unnecessary requests to handlers- servers clogging the bandwidth with the intention of compromising the network. Users (agents) are confronted with slow speed and in some instances the servers crash due to the attacks. For this attack to be successful, cybercriminals send a ping flood attack (targeted attack on a server) in order for them to control remotely a botnet- (a collection of computers). DDoS are more damaging because modern security tools have evolved to stop traditional DoS attacks. In addition, modern DDoS attack tools are cost effective and easy to use, thus, creating an avalanche of DDoS attacks worldwide (Quade, 2020). For example, the Low Orbit Ion Cannon (LOIC) which is an open-source application for stress testing, allows attackers to use the what-you-see-is-what-you-get (WYSIWYG) interface using a web-browser. While the High Orbit Ion Cannon (HOIC) is an advancement of the LOIC in that attackers use the HTTP protocol to attack specific targets. These attacks can be mitigated by regulating the number of server requests in a specific time period, or installation of web-application firewalls that filter traffic or unnecessary requests to the server (Makridisa & Smeets, 2019).

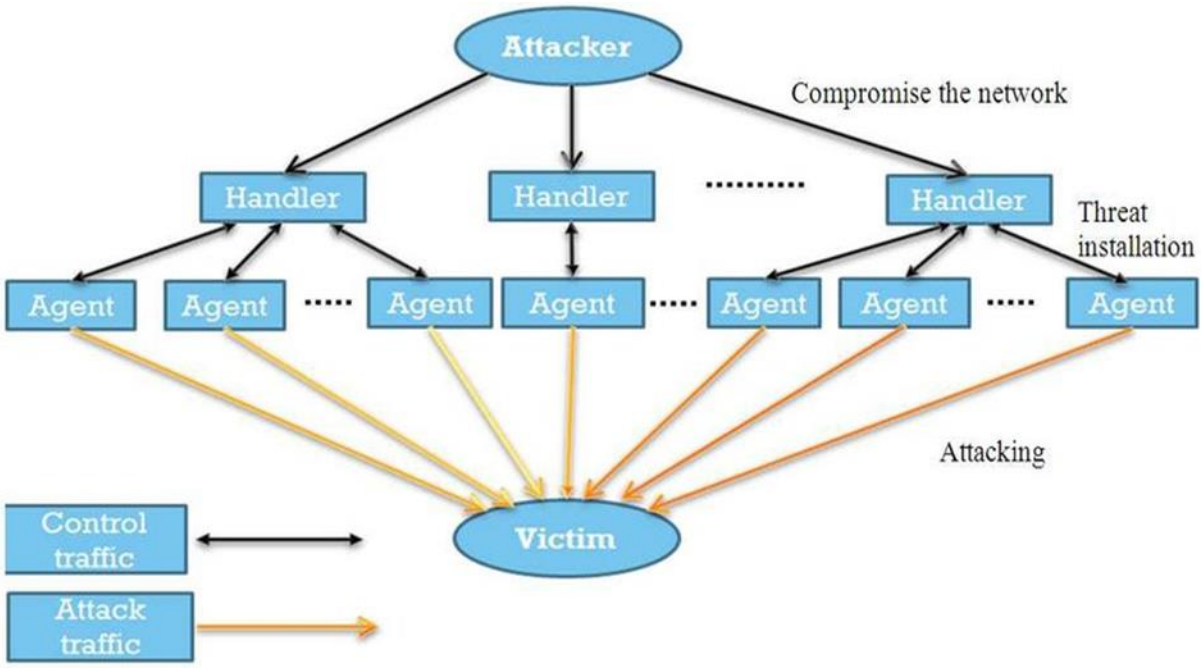

Figure 2.2 Distributed Denial-of-Service (Quade, 2020)

2.2.1.5 Phishing

Chuma and Ngoepe (2021) state that South Africa has recently become of the top countries experiencing Phishing attacks. Cybercriminals send spoofing emails designed to obtain people's personal information. Many people have fallen victim to Phishing attacks because of the belief that emails would be coming from a legitimate enterprise. For example, the researcher received emails purporting to be from the South African Revenue Services (SARS) requesting to log onto the e-Filing system and update bank details because there was "a payment due to you" type of message. As a scholar of Cybersecurity, the researcher called the SARS Contact Centre to verify if the organisation was now requesting its clients to update bank details on the e-Filing system. It only turned out that it was a well-orchestrated scheme from cybercriminals. It later turned out that some colleagues working in the same institution with the researcher, had received similar requests and had proceeded to click the email attachment, and in the process, exposing their details to cybercrime syndicates. Cybercriminals use email spoofing with links to fake websites, and if the user clicks on the link believing it is legitimate, capture private and sensitive information, the hackers will take the stolen information and sell it for their personal gains (Gaspereniene *et al.*, 2017).

Arewa (2018) states that attackers are generating emails, purporting to be a bank, send to unsuspecting Internet users with the intention to trick victims to enter their personal banking

information. This attack is well choreographed that victims fall prey to websites that look authentic yet they are fake. These “fake-authentic” sites are difficult to verify or validate with server authentication programs. The Banking Association South Africa [BASA] (2019) acknowledges that perpetrators can be cunning and call their potential victims to verify their credentials. Standard Bank South Africa (2019) has also indicated that scammers are targeting Standard Bank UCount users. An email is generated and send to UCount users purportedly originating from the bank. The message is enticing and with enthusiasm, clicking on the link exposes the customer’s details. UCount users fall prey if they click the link sent by the attackers. The fraudulent email “informs” customers that they have earned over 60, 000 UCount points. The World Health Organisation (2020) states that there are millions of fake emails sent out by threat actors purporting to be sharing Corona Virus Disease-2019 (Covid-19) related information with ulterior motives of attaching unsuspecting victims.

Osborne (2020) states that the Amalgamated Banks of South Africa (ABSA) was embroiled in a data leak with one of their employees who illegally accessed customers’ information and exposed it to third parties. The employee was alleged to have exposed clients’ personally identifiable information to external parties. Pinnock (2020) asserts that with the recent spike in data breaches in South Africa, it is a clear indication that the country’s state of readiness is put into question. This shows that there is no organisation that is immune from a data breach. With POPIA now in effect, organisations are duty-bound to report breaches. Prior (2020) posits that there has been an exponential increase of data breaches and banking scams during the period of the global Covid-19 pandemic. Given the context of the global Covid-19 pandemic, there has been a major shift to remote and hybrid work. Businesses had to reconfigure their operating models within a short space of time with little preparation for the transition.

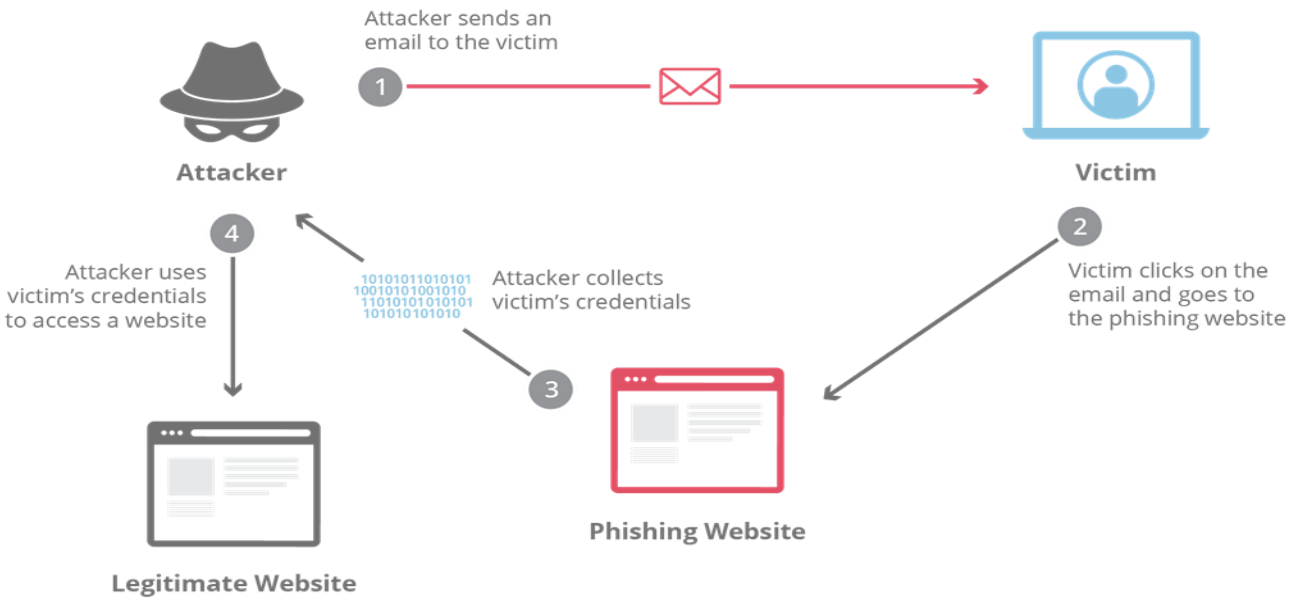

Figure 2.3 Phishing Website (Amazon, 2017)

For example, the illustration in Figure 2.3 summarises the processes followed by attackers. An email is sent to the unsuspecting victims who click on the email and the response is directed to the phishing site (step 3). The victims' credentials are collected and used by the attackers to access a genuine website for personal gains. Companies that have also fallen prey include Amazon.com, most airlines and online clothing retailers.

2.2.1.6 Email Bombing, Spamming and Cyberstalking

The WHO (2020); Chigada and Madzinga (2021) observed that during the global Covid-19 pandemic, many organisations have been experienced unprecedented levels of email bombing and spamming from fraudsters. Huge emails with fake Covid-19 vaccination or infections information are sent to mail servers with the intention of crashing servers. Usually these email messages are long and complex to understand designed to consume bandwidth resources-imitating DDoS impact. Users opening unsolicited emails expose their personal details to spammers. Internet users receive unsolicited bulk messages which when opened, expose the user's credentials to hackers. The WHO (2020) highlights that **website jacking** is a growing cybercrime especially during the global COVID-19 pandemic. An organisation's website is fraudulently controlled by hackers who are able to manipulate and change the website content to a fake similar looking page. Website hackers use the hacked site for selfish interests and might ask for ransom. For example, the WHO website has been impersonated many times and unsuspecting victims have fallen prey to threat actors. **Cyberstalking** has been reported in

many print and electronic media, where victims have complained about cyberbullying and attacks (Chuma & Ngoepe, 2021). Cyberstalkers follow victims on their online activities, while harvesting information and in some instances harassing them via emails, blogs, chat rooms, discussion for a and open publishing websites. This crime is perpetrated to inexperienced web users not well versed with netiquette and internet rules of safety through internet and computer stalking (World Economic Forum [WEF] (2020).

2.2.1.7 Other cyber-attack topologies

The researcher acknowledges that cybercriminals' intention is to steal data including Intellectual Property (IP), code sabotage, insider threat actions. These criminal activities are mostly committed by employees who are exposed to inside information and organisational processes. Nefarious acts are perpetrated through unacceptable human behaviour. Detailed discussions are presented in sub-section 2.4.5.

2.2.2 Cyber-crime typology

This section discusses cybercrime-typology. These are the actual crimes committed by cybercriminals.

2.2.2.1 Data Diddling

When data capturers are in the process of entering or just before they enter data into the computer, they can alter the original data with malicious intentions (Cotae, Kang & Velazquez, 2020). In simple terms, data diddling means fiddling with data so that crime can be committed before the data is processed. It might be difficult to track the modified output when an attacker uses data diddling to commit crime and the attacker can steal from the firm. A good example of data diddling might occur when a data capture clerk entering banking details for the firm, may change data to show their account number, or that of a family, friend and get full payment. This is an easier way of stealing money from the firm without detection. In India, Electricity Boards have been exposed to data diddling programs which were inserted when private electricity firms computerised their systems (New Delhi a contractor-a computer professional manipulated data files to show less receipts and bank remittance (Cotae *et al.,* 2020). A new wave of cyber-attacks is committed through digital systems sabotage by former and current employees. Inside threat or IT sabotage is an area of increasing concern across government, research, industry and the public sector. Malicious insiders intentionally use technical methods to disrupt or cease normal business operations of a victim organisation (Chigada, 2020). This

form of cybercrime is attributable to unacceptable human behaviour as discussed in sub-section 2.4.5.

2.2.2.2 Identity Theft and Bank Card Fraud

The ITU (2019) and Chigada (2020) report that identity theft and bank card fraud have the highest commission rate in the world. The researcher, a former banker, has worked in the card payment solutions landscape responsible for identifying and mitigating card and identity theft. The South African Bank Risk Information Centre [SABRIC], 2020) reports that identity and credit card theft cases are on the rise. Merchants (firms selling goods and services), financial industry and cardholders are losing millions of Rands yearly due to escalating identity and credit card fraud. People fall prey when they fail to get copies of their receipts after paying with credit cards. The receipts bear the credit card information. In some sophisticated environments, personal details are used to open fake accounts-loans, bank accounts for the purpose of committing fraud. South African banks are installing software solutions that monitor credit card and guard against identity (Chigada, 2020).

With reference to the South African payment card industry, credit card fraud increased by 1% in 2017 translating to R437m (SABRIC, 2017). Common types of credit card fraud include **lost and or stolen card fraud**- attackers interfering with customers while transacting at ATMs; **not-received issued card fraud**-this situation occurs when genuinely issued bank cards are intercepted by criminals before reaching the actual card-holder; **false application card fraud**-criminals open bank accounts using falsified credit applications; **counterfeit card fraud**- the most common type of card fraud perpetrated by criminals through information stolen from magnetic strip of genuine cards which are skimmed (Chigada, 2020). **Card skimming via point of sale (POS)** skimming devices were retrieved in 2014 in South Africa. Restauranteurs fell prey to card skimming when waitresses and waiters took away the customer's card for payment purposes. Taking away the card has since been stopped after customers' financial losses (SABRIC, 2020). **Account-takeover card fraud** takes place when the victims' information is intercepted by criminals who apply for replacement cards pretending to be the legitimate cardholder. Card not present card fraud (CNP) takes place over the telephone (Grobler, 2020). For example, a former Cape Town barman who cloned customers' bank cards. The barman was arrested and sentenced to five years in prison. The SABRIC (2019) states that fraudsters place online orders purporting to be genuine clients. Upon delivery of goods, the "prospective customers" turn out to be fraudsters and the merchant loses both the money and goods.

Chang and Coppel (2020) state that a good intervention strategy to mitigate credit card fraud is the adoption and use of biometric authentication. Customers do not need to carry credit cards or key-in personal identification numbers (PIN) when transacting. Merchants would have invested in biometric technologies that support biometrics authentication. Different biometrics usable in the authentication process are classified as physiological (fingerprint, face recognition, IRIS scan, hand geometry, deoxyribonucleic acid [DNA]) and behavioural (voice pitch, speaking style, typing rhythm, signature, breathe) (Pillay, 2020). A study by SABRIC (2019) revealed that biometrics authentication technologies require a huge financial, information technology [IT] and IT human resources outlay. In addition, South African banking technologies, running on Systems Application Products [SAP] operating systems were scalable and can sustain huge transaction volumes when biometrics authentication is implemented. This means that banks can adopt and implement biometrics authentication systems to augment bank card transactions. The study also revealed that the telecommunications infrastructure was stable and capable to carry large transaction volumes. However, it is only Capitec Bank that has embraced and implemented biometrics technology in its quest to serve customers efficiently, effectively and at low banking costs (Capitec, 2019). Instead of stealing the actual card, fraudsters are in the propensity of using digital technologies to apply for credit using another person's name by using fraudulently acquired information. Information can be stolen from doctors' consulting rooms, credit providers' files, hospital records or any source that might not have adequate security protocols. The South African Post Office (2020) states that cybercriminals intercepted mails with the intention of obtaining cards sent through mail. Customers are encouraged to analyse their bank statements to identify any anomalies and notify the bank immediately. Changing security details is another option that can enhance bank card transactions, if anyone suspects that their security information has been compromised.

2.2.2.3 Salami Slicing

The SABRIC (2019) also posits that Salami slicing attack is gaining popularity where fraudsters target their victims' bank accounts and steal money slowly to mitigate early detection. Thus, over a period of time, perpetrators would have stolen a lot of money in bits and pieces. The "collect-the-roundoff" technique is mostly used where the perpetrators carry out calculations in a particular currency and round off up to the nearest number. A computer program is inserted into the program and automatically makes imperceptible alterations and deductions. Insignificant amounts are deducted from customers' accounts over a period of time

(Curtiss, 2011). Curtiss (2011) states that a disgruntled bank employee, just dismissed from his job, inserted a logic bomb activated to deduct ten cents from an account he opened in the name of Ziegler. When Ziegler discovered the credited money to his account, he immediately notified the bank of this analogous fraudulent crime (Curtis, 2011:3). Software piracy has become an integral part of humankind committed knowingly and unknowingly (Fintech, 2018). The illegal use of someone else's intellectual property and passing it onto friends and relatives is rife in many societies. The WEF (2019) states that there is less research and development because governments are redirecting financial resources to fight software piracy and other forms of cybercrime. Given the gravity of sophisticated cybercrimes arising during Covid-19, there is pressure on the global economy to fight a number of challenges such as poverty, unemployment, inequality, cybercrimes and skills shortage (The World Bank, 2019).

2.2.2.4 Net Extortion

Other cybercrimes committed using electronic means are called Net extortion. Curtis (2011) defines net extortion as shakedown, outwrestling and exaction where criminals obtain property, money or services through coercion. Cyberextortion entails a perpetrator demanding money or goods, sex, or information from another person or company using the internet (Schwab, 2019). The attacker threatens to harm the victim, the victim's reputation or property by encrypting victims' systems and offer to decrypt the systems after getting a ransom usually in the form of cryptocurrencies, like bitcoin. DDoS is also used by blackmailers to get money from a company after making threats that the blackmailers will suspend leaking confidential company information if they get a ransom. Recently, South Africa reported that approximately R54 billion worth of cryptocurrency was stolen by two brothers that were running a fictitious Bitcoin Company (News 24, 2021). This is a form of net extortion because the two brothers are classified as hackers who gained access into the company's server, corrupted data and all the files to destroy evidence. It was reported that the two brothers advised their clients not to report to any law enforcement agencies (n.d. 2021) an indication that there were sinister motives or activities occurring. Schwab (2019) states that cryptocurrencies are not managed or regulated or monitored by a government institution thus, creating loopholes for cybercrime. This corroborates the most recent incidents in South Africa and the United Kingdom. Hackers illegally access the trading platforms to carry out anonymous transactions with the full knowledge that their identities will not be detected. For example, in 2018, more than US$5 billion was stolen through cryptocurrencies in Europe. The WEF (2020) posits that Bitcoin is exacerbating ransomware attacks where attackers demanded ransom payments in

cryptocurrencies. In order to access locked systems and data, many firms are compelled to pay the ransomware in cryptocurrencies. It is difficult to trace Bitcoins. Crypto phishing is also increasing at a very fast pace because fraudsters send complex emails to their victims directing them to fake versions of real cryptocurrency sites, thus, victims capture their credentials on these fake sites leading to exposure of their information and funds (Schwab, 2019). Therefore, this thesis warns the public and businesses to be cautious and vigilant when trading in cryptocurrencies.

2.2.2.5 Child Pornography

The internet is a breeding ground for child pornography. Various legislations have been enacted globally to deal with censorship of child pornography on the grounds of obscenity and abuse of minors (Sullivan, 2010). Child pornography is punishable by law because it is a serious offence that falls under the category of obscenity. Within the context of South African legislation, it is criminal to store or transmit pornographic material on any storage and transmission medium. Child pornography attracts harsh punishment in South Africa (more than 15 years in jail), (Childlinesa, 2016). Child pornography is gaining popularity as cyber pornography includes pornographic websites and magazines which use the internet or computer for transmission.

Literature states that the word "obscene" is debatable between different legal systems. What might be obscene under one legal system might not be obscene in another legal system. The Obscene Publication Act 1959 and 1964 Section 1(1) define obscene as material which tends to deprive viewers who would have read, seen or heard the material. Arewa (2018) states that child pornography now involves pornographic websites- sites wholly dedicated to pornography production. Online grooming is gaining popularity as a very serious cybercrime where cyber-attackers pose as children, entice victims and eventually agree to meet their victims in face-to-face, subject their victims to physical, sexual or emotional abuse (Magome, 2020).

2.2.2.6 Internet Fraud

Attackers use the internet (online services) to commit fraudulent solicitations, transactions and transmit these fraudulent transactions to financial institutions. Internet fraud has similar trait as cyberstalking (Khan *et al*., 2020). The Merriam-Webster Online Dictionary (2018) defines fraud as an untruthful and deceitful way where one person intentionally induces the other person and illegally part away with something of value. For example, there are reports from

airline companies that have stated that fraudsters book and pay for air flight tickets using stolen bank cards. In some instances, the transactions are detected quickly before the perpetrators get away with the fraudulent transactions. The researcher, having worked in a commercial bank, experienced and came across airlines that had been swindled by internet fraudsters. Most of the crimes were committed outside South Africa, using foreign-bank issued cards which, made it difficult to detect especially when the transactions are conducted after business hours and within the context of different time zones. Other forms of computer fraud involve altering the computer input in an unauthorised way' disrupting suppressing or stealing output; making illegal changes to stored information and amending computer programs (Alzubaidi & Abdulaziz, 2021). Computer fraud is one the most common types of cybercrime because it can be committed easily and yielding high financial gains for threat actors (SABRIC, 2019). Cyber fraudsters engage in their nefarious acts for selfish fraudulent financial gains, thus financial crimes are the most alarming that attract the largest number of causalities. The emergence of advance fees, dating and romance sites, job and employment scams are posing challenges for Internet users. Many people in South Africa and globally have been confronted with such scams at some point in their lives. Criminals using internet fraud devise sophisticated strategies to hoodwink unsuspecting consumers and other internet users.

Javiya (2017) and Arewa (2018) state nine types of computer fraud as: **Confidence fraud** is fraud perpetrated by attackers resulting in financial losses. Internet users over rely on another Internet user in a relationship of trust. Good examples included letter scams or "419" fraud. **Intellectual fraud:** one firm knowingly misrepresents/conceals the truth to another firm with the intention of defrauding the other part. **Government fraud** occurs when an Internet user conceals material fact to induce government to act to its own peril. Cybercriminals are using deceptive tactics on the Internet **creating fictitious investments vehicles** through income producing ventures such as Ponzi/pyramid schemes for capital gains. Two case studies to have hit South Africa include R330m Cape Town Ponzi Scheme of 2018 and the R380m Johannesburg Ponzi Scheme. In both instances fake investment companies created fictitious income generating ventures, that defrauded people and companies of their hard-earned income (Africa News Agency [ANA], 2018).

Insurance fraud has been gaining popularity within the insurance industry globally. This type of internet fraud occurs when either the insured or provider misrepresents in the indemnity against loss- inflating of actual claim using the Internet (Arewa, 2018). Misrepresenting or

concealing the truth to induce the business or financial institution to perform a fraudulent activity on a credit or debit card fraud constitutes **financial institution fraud.** Curtis (2011) acknowledges that the level of sophistication of money laundering in Nigeria is advanced and complex creating headaches for law-enforcement agencies and other stakeholders. This is corroborated by Arewa (2018) who states that there are highly sophisticated cybercriminals in Nigeria that specialise in money laundering.

Attackers use **communications fraud** where information is exchanged using wireless, satellite or landline services. Individuals or firms can misrepresent material facts to another company with the intention to defraud a regulated entity that performs an essential service using the Internet. Good examples of entities providing essential services include hospitals, schools, universities and municipalities. This type of internet fraud is referred to as **Utility fraud (**Ocaña & Faibishenko, 2016). The Financial Intelligence Centre (2020) reports that in 2020, during hard lockdown, South Africa experienced an increase in Internet fraud because of remote access to corporate networks using unsecured connections. People conducted banking transactions online have had their PINs, identity document numbers and bank account details stolen. These documents provide further information to Internet fraudsters which expose their victims to financial losses, access to their contacts and relatives. The advice proffered by the Financial Intelligence Centre (2020) is for people to be vigilant and continuously keep their documents safe all the time.

2.2.2.7 Cyber-bullying

Smith *et al.* (2018) define cyber-bullying as a form of cyber-harassment done through electronic means. Cyberbullying and cyber-harassment are also referred to as online bullying and this type of cybercrime is growing exponentially amongst teenagers on social media networking sites (Childlinesa, 2016). Attackers send electronic messages of an intimidating nature to another person using digital devices like cell phones, laptops, computers and tablets to intimidate and threaten their victims (Microsoft Corporation, 2018). Studies carried out in South Africa show that the country has been experiencing chilling images and videos of children bullying each other (Weekend Argus, 2018). In addition, South Africa has the highest prevalence of cyberbullying based on the parents who participated in an online survey. This high prevalence is attributed to increased use of social media among the youth (Ipsos South Africa, 2018). Most of the cyber bullying is perpetrated by classmates and this crime took place on social networks such as Facebook, Twitter, WhatsApp, Instagram and WeChat. Like any

other cybercrimes, insecure children project bullying emotions onto other children, resulting in cyberbullying, therefore, parents should openly talk and discuss with their children and let them know that unfavourable things can happen online.

Kyobe (2016) admits that cyberbullying is an aggressive crime that differs with the type of technology used. There are pure and bully victims defined within the context of cyberbullying. Pure bullies perpetrate bullying on their victims because they are assertive and not afraid of other bullies. While bully victims are the ones that have been bullied (Kyobe, 2016). Exacerbating cyberbullying is that law enforcement agencies and policy makers find it difficult to develop intervention strategies and legally binding anti-bullying legislation and policies in schools (Kyobe, 2016). A 2017 study of 12 000 South African children revealed that 42% responses indicated that they were bullied weekly, 35% were bullied monthly. These figures demonstrate that South African kids were the worst bullies amongst New Zealand, Singapore, United States of America, Egypt and Saudi Arabia who were surveyed in 2017. As shown in Table 2.1 below, the weekly statistics show SA (42%), followed by New Zealand (24%), Saudi Arabia (22%), Singapore (16%), USA (15%) and Egypt (7%). Compared to the rest of the countries, SA's never rate (23%) is the least, a demonstration that cyberbullying is high in SA schools (Progress in International Reading Literacy Study [PIRLS], 2017). The comparisons are shown in Table 1 below.

Table 2.1: Cyberbullying amongst school children

Country	Weekly %	Monthly %	Never %
South Africa	42	35	23
New Zealand	24	36	40
Singapore	16	33	51
United States of America	15	30	55
Egypt	7	18	75
Saudi Arabia	22	25	53

Source: PIRLS (2017)

2.2.2.8 Cellphone hacking

There is a growing trend arising where authoritarian regimes or governments are using spyware to target activists, journalists and politicians believed to be anti-government (Kirchgaessner, Lewis, Pegg, Cutler, Lakhani & Safi, 2021). It is reported that this form of cyber-surveillance

is an intentional approach perpetrated by oppressive regimes to silence critics. Reports show that the NSO-Group, an Israeli-based company, has developed the Pegasus software and selling it governments. Authoritarian governments are purchasing the Pegasus software (hacking software) purporting that they are pursuing criminal and terrorist elements in society. Pegasus is a malware targeted at iPhone and Android devices, by extracting messages, emails, photos, ability to record calls and secretly activate microphones (Kirchgaessner *et al.,* 2021).

The forensic analysis by the Guardian (2021) confirms the issues raised by Kirchgaessner *et al.* (2021) in that business executives, religious leaders, academics, non-governmental organisation (NGO) employees, trade union activists, cabinet ministers, presidents and prime ministers have been under cyber-surveillance for the past two years. This is how authoritarian governments access people's phones: For example, sim cards are rica'd or recorded with service provider (Vodacom, MTN, Cell C or Telkom), which is then compelled to submit a database of its subscribers to Government Communication Services, which can randomly pick-up suspicious phone calls and start monitoring the movements, conversations and activities of certain individuals. Through the services of the Secret Service Agency (SSA), the Pegasus spyware is remotely used to hack into people's phones without their knowledge. In most instances, the targeted victims do not notice that they are on a 24-hour surveillance (Kirchgaessner *et al.*, 2021). Whilst one is going about with their business, the Pegasus surveillance can copy messages (sent and received), harvesting photos as well as recording phone calls without one's knowledge. With a quest for knowledge and trying to understand how this Pegasus spyware works, the researcher discovered that it is marketed and licensed to governments by the Israeli Company-NSO Group. Billions of cellphones using either iOS and Android operating systems can easily be infected through spear-phishing. Spear-phishing are text messages or emails that trick the phone user to click malicious links. In recent times, the NSO Group is targeting manufacturers of Android and iPhone phones' when updating software to fix bugs in an operating system (zero-day vulnerability). For example, an iPhone user receives a notification on their cellphone settings requesting them for a software update. The cellphone should have at least 50% battery charge or should be connected to a charger and have access to uninterrupted Internet connection. When such messages are received, cellphone hackers infiltrate that "software update" message without the manufacturer or users' knowledge.

The WhatsApp Inc (2019) revealed that more than 1400 phones were targeted by exploiting the zero-day vulnerability strategy (see above discussion). When targeted individuals made or received WhatsApp calls, the NSO Pegasus code was secretly installed on the phones. There are reports that cellphone hackers are experimenting to hack Apple's iMessage software, through backdoor access to millions of iPhones (Apple Inc, 2021). The number of users targeted by hackers is increasing at an alarming rate because of the popularity of platforms such as iMessage and WhatsApp. In addition, it is reported that as recent as July 2021, iPhone users that updated their iOS software could be under surveillance. Compromised iPhones allow the attacker to obtain root privileges or administrative rights on the device. This means that the attacker starts controlling the device.

News24 (2021) reports that mobile phone hacking software can be bought over the internet for as little as R1000. People hack their partners phones to spite or use the evidence in divorce cases. For example, the case of Dr. Graham Hefer, a former rugby player who is being investigated for illegally intercepting his ex-wife's emails, SMSs and phone calls by installing Flexispy© software on his wife's phone (Preller, 2021). The wife discovered that her phone had been hacked by her husband who informed her of her legal representatives but she had not discussed these activities with the husband. This is atypical case which tested the effectiveness of the country's cyber legislation. With reference to POPI Act 4 of 2013 and the IMPA 77 of 1995, Dr Graham Hefer violated a number of provisions which constitute cybercrime and should be tested in a court of law. Once a person's phone is hacked, the user losses privacy and security. There are other high-profile cases of people who are alleged to have hacked detectives' phones, monitoring their movements leading their murders by crime syndicates.

The Zimbabwean government is reported to have bought the Pegasus software from the NSO Group and is used by the country's dreaded Central Intelligence Organisation [CIO] (Moyo, 2021). The intention is to target politicians, journalists and other high-profile people especially the country is preparing for the 2023 elections. It is reported that the CIO is snooping on mobile phones through enacting an enabling legislation. People's movements, activities and conversations will be spied on, including penetration of WhatsApp that has end-to-end encryption by the CIO (Moyo, 2020).

2.3 Cybercrime in South Africa

In the preceding sections, the researcher outlined the various types of cybercrimes and how they are committed giving examples from across the globe. It is imperative to provide a synopsis of cybercrime from South African and global perspectives. The researcher discusses cybercrime in the private sector, followed by cybercrime in the public sector.

2.3.1 Cybercrimes in Private Sector

SABRIC (2020) states that SA has the third largest number of cybercrime victims globally, resulting in the loss of more than R2.2 billion each year. Every time a user logs onto a smartphone, computer, open an email or Internet, the user is at a high risk of exposure to cybercrime. Common cybercrimes prevalent in SA include: identity theft, phishing and ransomware, malware, cyberbullying, cyberstalking, theft DoS Hacking Hoax email, defacement worm and bank card fraud (www.cybercrime.org.za). The Fin24tech (2019) reports that SA businesses are ill-equipped and ill-prepared to deal with emerging cybersecurity threats and attacks and most of these businesses rely on outdated protection strategies such as the implementation of firewalls. Cybercriminals have realised that most firewalls are not properly configured in line with the changing cybersecurity policies and sophisticated attacks and threats (Chang & Coppel, 2020). There is a fast paced in cyber-related risks, increasing the security gaps organisations can contend with and, thus, firms are left more exposed than ever before (Cotae, Kang & Velazquez, 2020).

There has been a recent surge in corporate cybercrime due to people working remotely and using unsecured or public Internet connection. There are many instances where Internet users share their personal devices with family or friends without password protection, thus, creating opportunities for cybercrimes (Cotae *et al.*,2020). The "hacking economy" is thriving worldwide thus, exposing organisations and individuals to sophisticated attacks and threats (Chang & Coppel, 2020). With reference to falling economic conditions, businesses are exposed to the fragile socio-economic-political environments and targeted cyber-attacks exacerbate reputational damage. Ster-Kinekor (2017) reported that 7 million of its customers' information was leaked via the company's website. Matt Cavanagh announced the flaws on Ster-Kinekor booking website and reported this to the company. The researcher notes that the discovery was made by a software developer. In 2016, Gupta-linked media and the South African Broadcasting Corporation [SABC] computer systems were hacked by Anonymous

Africa-hacktivist group (Mail & Guardian [M & G], 2016). The Gupta-linked media outlets were: The New Age, news channel ANN7 and companies: Sahara and Oakbay Investments were forced offline. The Fin24 (2016) reports that the SABC was attacked by Anonymous Africa in the same week the Gupta-linked companies were attacked. Some of the SABC websites were disrupted and stopped functioning for several hours. Anonymous Africa claimed responsibility for the SABC attack because the hacktivist was incensed by what it calls allegations of censorship at SABC (Fin24, 2016).

Banks hold very sensitive financial data and or information, therefore, they are the most highly prized targets for cybercrimes. SABRIC (2019) states that First National Bank [FNB], Standard Bank and Amalgamated Banks of South Africa [ABSA], were attacked, resulting in a combined financial loss of US $80,000. Due to the sensitivity of financial data, the three banks did not disclose the extent of damage, total amount stolen and the nature cyber-attacks (Marchetti, *et al.,* 2012). The infamous WikiLeaks group hacked South African banks in 2009 and released the uncensored Competition Commission report with the intention of creating public awareness about high banking fees and why these banks served middle-high income segments in the country (Marchetti *et al*., 2012). With the emergence of money mules- cybercriminals electronically transfer illegally acquired money (stolen in online banking fraud) to criminals (SA Fraud Prevention Services, 2019). Criminals are resorting to this type of crime after banks started using biometrics to verify account holders.

In July 2018, Liberty Holdings was attacked and the company informed its customers that their personal information (insurance policy information) had been stolen by an external party (Fin24, 2016). The severity of the attack was that the attackers threatened to release emails and attachments from Liberty to clients on the "dark web" (requires sophisticated software and sells mainly illegal products using cryptocurrencies) and customers' banking details, log on credentials and policy documents were exposed. The hackers were demanding a ransom but Liberty Holdings refused to pay ransom (Fin24, 2016). With the emergence of the COVID-19 pandemic, there has been an exponential growth rate of cyber-attacks and threats on healthcare institutions, financial sector and government departments. These institutions deal with Big Data which has become a lucrative venture for cybercriminals because accessing such data assets can be financially beneficial to their nefarious acts (The World Bank, 2020).

2.3.2 Cybercrimes in Public Sector

The Government Gazette (2021) states that there are 42 government departments in South Africa, all facing different types of cybercrime and there are challenges of mitigating cybercrimes in all these departments due to the complexity and sophistication of how cybercriminals operate. The first cybersecurity policy drafted by the former Minister of Communication, Mr Siphiwe Nyanda lacked a clear coordination process because there were various structures/apparatus in place already dealing with cybersecurity. Von Solms and von Solms (2018) agree with the then Minister of State Security-Mr David Mahlobo (2015) who states that South Africa has fragmented and inconsistent pieces of e-legislation coordinated by multiple government agencies, a point raised by Sapa (2010) and Bote (2019). The researcher states that there are limited empirical studies on cybercrime and cybersecurity in South Africa. Furthermore, there is little information that states that SA cyberlaws are aligned to national, reginal and global cyberlaws, thus, an unwelcome situation permeates the country's cybersecurity response strategy. Civil society, public and private sector firms receive most cybercrime reports from news, newspapers, online articles and at business conferences.

The Reuters News Agency (1999) reports that hackers attacked Statistics South Africa website and replaced it with that of Telkom South Africa. Visitors to the StatsSA website were confronted with comments such as "Telkom stop your…. lameless monopoly" instead of the usual consumer price index and gross domestic product information. Telkom SA (1998) also reports that a teenage boy from Rondebosch, Cape Town hacked through the security features of the company's information systems and moved money around-though not much damaged was caused. Otto (2008) states that two South African Revenues Services (SARS) employees and their accomplices were sentenced to 15 years imprisonment for defrauding the taxman of R500,000. Organised crime syndicates continue to use sophisticated strategies. The Department of Home Affairs (DHA) lost nearly R400 million in 2009 through cybercrime syndicates. The syndicates used fraudulently acquired identity documents, including passports, marriage certificates from the DHA system for the commission of further crimes.

In May 2018, personal records of 943 000 South African drivers were illegally accessed from an online traffic fine website-ViewFines owned by Aggregated Payment Systems (News24, 2018). The breach was discovered by Troy Hunt, an Australian security researcher specialising in checking whether an individual's information is safe and secure. The South African Master Deed's computer systems were breached and personal information for over 60 million South

Africans such as identity numbers, company directorships, names and addresses were illegally accessed by attackers (Mohapi, 2017). Jigsaw Holdings, a holding company for many real estate firms was responsible for the data breach of the Master Deeds' information systems, because Jigsaw Holdings had customers' information supplied by credit bureau agencies.

South Africa is the second largest target (globally) of cyber-attacks and threats (News24, 2018). The researcher's deduction and assumptions to the views by News24 (2018) are that the country has porous, fragmented, inconsistent and incoherent cyber laws. In addition, the term "cybercrime" is not well understood and defined, thus, firms and civil society might not prepare adequately to deal with cybercrime. South African firms are using old and irrelevant solutions to combat, address and mitigate cybercrime, yet, there is a new wave and complex strategies used by cybercriminals which are more advanced than the contemporary enterprise's information security strategy. There is a huge gap between a firm's information security policy and egregious modus operandi of cybercriminals, which, requires an enterprise's leadership to introspect and strategize the firm's cybersecurity preparedness and response pattern. Many firms and government departments are falling prey to cybercrimes due lack of IT and legal expertise, resistance to change, silo mentality approach to dealing with this scourge. Some firms and government departments use old tactics which have been supervened by sophisticated cybercrime syndicates, complex cybercrimes perpetrated on different firms and platforms. Having analysed cybercrime in South Africa, the researcher is convinced that there are more unreported incidents and financial losses in corporate South Africa, but, with limited studies, this type of information is not readily available to the public. One can pose a very serious question about human beings' moral fibre. What has gone wrong with people of the Fifth Industrial Revolution? Companies over rely on human intelligence for production and decision-making, while overlooking the ethical behaviour of these individuals. Given any opportunities of weak systems, people can bypass the system to commit crime.

The devastation caused by cybercrimes is not peculiar to South Africa, but the rest of the continent. However, with limited studies reporting on cybercrimes, it is difficult to measure the rate and degree of financial losses caused by cybercriminals. Wangwe, Eloff and Venter (2009) report that East Africa is hard-hit by a growing wave of cybercrimes. Lack of cyberlaws, fragmented and incoherent legislation and few mechanisms to combat and mitigate cybercrimes have been cited in literature as major contributing factors to cybercrimes in East Africa (Safaricom, 2016). Although there has been tremendous progress in e-government in

African states, focus should be on improving computing, telecommunications infrastructure as well as cybersecurity response and information security strategies. The ITU (2019) acknowledges that in the information era, society needs technologies to communicate, share, store or deliver services, the challenge is that human behaviour is stifling the purpose of these technologies. The growth of the information society is exposing governments, people and organisations to high levels of cybercrime. For example, Nigeria's 419 scam has put the country's image at reputational risk, resulting in some countries blocking email accounts from Nigeria (Arewa, 2018).

On the 29th of December 2018, the Guardian (2018) reported that cyber-attacks disrupted newspaper distribution in the USA. It is reported that hacking appeared to have originated from outside the USA, causing major printing and delivery disruptions on Saturday, 29 December 2018. The Los Angeles Times, The Times, Tribune, Sun and other newspapers sharing the production platform in Los Angeles were attacked (Guardian, 2018). This demonstrates how daring cybercriminals are and can attack even the most advanced computer systems and networks. When Tribune Publishing first detected the malware on Friday 28 December, the immediate reaction was to report to the Federal Bureau of Investigations [FBI]. West Coast editions of the Wall Street and New York Times were not spared either by the attackers. The total cost of the damage and loss could not be ascertained at the time of this study, but, in due course, the USA government is likely to make this information public as an awareness campaign against cybercrime.

Smillie (2019) reported that the City of Joburg and banks to pay a ransom after hacking and threatening to close the financial sector and local government. These demands coincided with the time when residents when paying for municipal bills and gaining access to their bank accounts. The hackers demanded ransomware in the form of two Bitcoins (R219, 000) then a DDoS attack would be launched. The other group of hackers threatened the City of Joburg to release customer information if it was not paid four Bitcoins. These threats were not taken seriously and on Wednesday, 30 October 2019, banks were hit by a wave of DDoS attacks (SABRIC, 2019).

2.4 Factors Contributing to Cybercrime

White (2020) states that cybercrime is committed by different agents in different forms, thus, there is a plethora of things that happen during the commission of the crime. Consequently, this complexity of cybercrime cannot be captured by a single theory (Bote, 2019). Theoretical perspectives that have been identified to exacerbate cybercrime include: lack of understanding of cybercrime, fragmented legislation, information asymmetries and economic factors (Cotae, Kang & Velazquez, 2020).

2.4.1 Lack of Understanding of Cybercrime

Lack of understanding of cybercrime creates confusion and hinders rapid responses in the event of violation of laws (Canhoto, 2010). Lack of understanding of cybercrime is compounded by many facets at play that hinder the process of identifying and understanding what cybercrime represents (Canhoto, 2010). In addition, Baker (2010) states that different agents commit cybercrime in different forms, thus, it becomes difficult for one to understand what cybercrime is all about. Kyobe *et al.* (2012) point out that lack of understanding of cybercrime is made worse by conflicting and ambiguous interpretations of the term "cybercrime". Lack of understanding of cybercrime can be caused by multiple agents, varying levels of electronic crimes and absence of awareness programmes, making it more complex to understand what it entails. In addition, organisations focus on crimes that affect their organisations or industries, therefore, it gets complicated to devise appropriate strategies that address cybercrimes (Canhoto, 2010).

Baker (2010) states that collecting and analysing cybercrime data is complicated because people do not understand what cybercrime is all about. Authorities in the financial industry may not understand or pay heed to other cybercrimes that are irrelevant to their industries, therefore, the process of detecting such cybercrimes may be complicated (SABRIC, 2019). Financial institutions may focus on identity theft, credit card fraud and money laundering, while schools might focus on cyberbullying related crimes. In both instances, financial institutions and schools pay attention to crimes related to their industries, whilst ignoring other forms of cybercrimes (Chigada, 2020; SABRIC, 2019).

Literature posits that firms operating in the same industry may establish a monitoring body that collects, collates and disseminates cybercrime data to its stakeholders. The establishment of

such bodies helps to impart knowledge and information to the industry and society to understand cybercrime better (BankServ South Africa, 2020). South African banks provide financial risk information, challenges and cybercrime activities to the SABRIC, which compiles and disseminates this information to all banks and society (SABRIC, 2019). A central information communication repository might help financial institutions, cardholders and merchants to share, detect and understand cybercrimes. Lack of understanding of cybercrime and its consequences is exposing the government, civil society, private and public sector organisations to cybersecurity risks and losses (Kyobe *et al*., 2012). The author of this thesis states that a few initiatives that have been done by the SA government, private & public sectors to educate civil society about cybercrime. In some instances, people discover cybercrime after falling victims and losses perpetrated by cybercriminals. University students tend to access literature and other cybercrime related materials from teaching and learning materials and some universities have incorporated information security and cybercrime modules in their syllabi (Chigada & Daniels, 2021). Awareness of what cybercrime represents, prepares government departments to respond rapidly to cyber-attacks and threats. As pointed out Kyobe *et al. (*2012) there should be efforts to address cybersecurity attacks by mobilising resources to achieve the desired information security goals, thereby, driving towards an effective national cybersecurity strategy. If the level of understanding can improve, the nation will be taking the right step towards cybersecurity capacity building (Creese *et al.*, 2021).

2.4.2 Fragmentation of Legislation and Law Enforcement

Fragmented laws create opportunities for violation and non-compliance with cyberlaws. Pokwana and Kyobe (2016) state that the country's e-legislation is fragmented and inconsistent resulting in misalignment with regional and global standards. Johnson (2017) and Bote (2019) acknowledge that the country's cyberlaws are fragmented and inconsistent with other regional and global cyberlaws, therefore, windows of opportunities are presented for the commission of cybercrimes because it becomes difficult to detect cybercrime syndicates (Kyobe *et al.*, 2012). For example, Standard Bank Zimbabwe clients' sudden change in financial transactions has prompted the bank's management to warn its clients regarding phisher men sending money through Standard Bank Zimbabwe (The Business News, 4 June, 2016). Standard Bank Zimbabwe is cognisant that there are high chances that their clients will lose money with no recourse.

Despite establishing a Ministry of Cybersecurity, the Zimbabwean government does not have a cybersecurity regulatory framework to enforce and enhance the nation's cyberlaws. ITU (2019) points out that Zimbabwe is one of the African countries that does not have cybersecurity regulatory framework, thus, criminals do not have a chance of being detected and prosecuted after committing computer-mediated crimes. This demonstrates that most cyber legislations in the Southern African Development Community [SADC] are fragmented and misaligned. Attackers from other countries can commit cybercrimes with the full knowledge that cyberlaws in the host country might not investigate the crime due to differences of legislation and bi-lateral agreements (Kyobe *et al.*,2012). The SADC Secretariat is making efforts to address Capacity Building on Cybersecurity because of the high rate of cyber-threats and attacks caused by the high internet penetration and usage of smartphones amongst the youth (SADC Secretariat, 2020). The SADC Secretariat noted with concerns the level of fragmentation and inconsistencies of cyber-legislation in the SADC region. Suggestions were made on the need to synchronise, align and develop coherent cyberlaws (SADC Secretariat, 2020).

With reference to South Africa, Mahlobo (2015); Bote (2019) and Malatji *et al*. (2021) agree that the country's legislation is fragmented and poorly coordinated by different government departments and agencies which do not share information and knowledge about cybercrimes. The SA government also acknowledges that there are many pieces of legislation focusing on different types of cybercrimes (Mahlobo, 2015, Minister of State Security). The irony of this set-up is that different government agencies and departments mandated to coordinate these laws, do not share information and strategic intent varies from one department to the other (Mahlobo, 2015). The author of this thesis asserts that coordination of legislation has been identified as an influencing factor towards an aligned NCPF.

2.4.3 Information Asymmetries

Kyobe *et al.* (2012) define information asymmetries as the process where two parties to a transaction do not wield the same type of information. One party might possess superior information compared with the other party. Literature suggests that information asymmetries occur if one party withholds information from the other. For example, a seller of a product or goods does not disclose certain information to the buyer, vital information needed by the buyer to make an informed buying decision. With reference to the current study, some South African government agencies and institutions coordinating cyberlaws, might have access to

information and knowledge, but might withhold that information and knowledge from other parties-resulting in information asymmetry (Kyobe *et al.*, 2012). Information asymmetry theorists predict that information asymmetries occur as a result of bureaucratic and hierarchical political structures and policies that impede the sharing of data security information and strategies. Globally, power play politics tends to swing in favour of the most influential and well-connected individuals wielding information-resulting in information asymmetry. For example, the law-making process in South Africa follows a series of bureaucratic processes, informed by political structures. In addition, government departments do not share "sensitive cybersecurity information" for reasons best known to them.

The SABRIC (2019) states that banks do not share information on fraud and cyber-attacks, however, the researcher argues that recently, Standard Bank reported the R300 million credit card fraud scam in Japan, an indication that banks now share information on cyber-attacks. In addition, Standard Bank Zimbabwe has warned its customers in the SADC region to be wary of cybercrimes perpetrated on the clients' accounts. The warning has been made through emails, Internet, print and electronic media. Increasing cyber-threats and attacks are pushing firms to share their challenges as a way of informing the public and other potential victims to be wary and lookout for pointers related to such crimes. Kyobe *et al*. (2012) state that some privacy acts restrict sharing of some information between government and private institutions, thus, this creates barriers for understanding common cybercrimes. The views by Malatji *et al*. (2021) are true especially in environments where the sensitivity of the information comprises State Security. The researcher states that the establishment of the Computer Security Incident Response Team (CSIRT) and the National Cybersecurity Policy Framework, are steps in the right direction to diffuse information asymmetries. However, these establishments' members are compelled to share ideas, information, knowledge and strategies in addressing cybercrimes. There are high likely chances that not all information or knowledge is shared. Individuals will always withhold information to have an upper hand over their peers- leading to expert power. Schwab (2019) states that individuals possessing expert power have an in-depth information, knowledge or expertise. Other factors contributing to government agencies' failure or reluctance to share information could be attributable to upholding the provisions of the Protection of State Information Bill. Anyone who violates the Bill can be imprisoned for 25 years (Johnson, 2017; Ncube,2019).

2.4.4 Economic Factors

Guerra (2009) in Kyobe *et al.* (2012) states that cybercrimes can be caused by economics and information security. For example, South Africa has recorded negative economic growth rates for the 2015-2017 period- leading to recession. Consequently, unemployment rose to 27% in 2018, rate of white-collar crimes has also increased exponentially (Statistics South Africa [StatsSA], 2019). With unemployment at 27%, there is a high rate of people resorting to any type of crimes such as card skimming, hi-jacking and forcing victims to withdraw large sums of money from ATMs. Individuals dismissed from employment can commit various types of crimes (such as the ones reported earlier in this chapter). Reports show that South African professionals and business are experiencing financial stress because of the prevailing economic conditions (Fin24, 2018). Businesses, individuals and government do not have money to spend on security despite the recognition that cyber threats are on the rise. Rather, businesses and government spend money on sustainability strategies. Individuals responsible for securing systems or reporting security breaches are not incentivised (because firms cannot pay higher salaries due to prevailing economic conditions) to do so nor does it affect them (or do not benefit anything reporting security breaches). Apart from lack of incentives, individuals engage in these crimes for personal gain and a desire to maintain a socioeconomic status often measured by level of education, occupation and income (Brown, 2010). Being a credit consuming society (most of the goods and services are offered on credit over a period of time), most South African youth are pushed by peer pressure to maintain some status, thus excessively borrow. They might engage in cybercrimes to remain "liquid"- financially strong, maintain their debt obligations and socioeconomic status (Cotae *et al*., 2020)

2.4.5 Human Behaviour

The financial benefits accruing from illicit and cybercrimes are driving people to misbehave and act in nefarious ways prejudicing organisations of billions of USD (WHO, 2020). Chigada and Madzinga (2021) in Khan, Brohi and Zaman (2020) state that the human factor is the biggest information security and cybersecurity threat lurking in our organisations. The lure of financial gains from illegal access to information and information assets has created demand for cyber-criminals to devise sophisticated ways of studying an organisation's information systems security protocols and pouncing on defective practices in order to gain access to information for personal gains. Siponen and Vance (2010) posit that employees fail to comply with a firm's information systems security policies, thus, it becomes a major problem for

organisations. Pillay (2020) concurs that half of all information systems and cybersecurity breaches are indirectly and directly caused by unacceptable behaviour and employee's poor Information Systems (IS) compliance. Ahmed, Sharif, Kabir & Al-Maimani (2012) attribute most cyber-attacks to human error, unacceptable human behaviour and the abandonment of the security policies that mitigate cyber threats and attacks. In their study, Wells, Camelio, Williams, & White (2014) posit how the lack of awareness when creating systems can introduce security vulnerabilities in the system. Marble, Lawless, Mittu, Coyne, Abramson, & Sibley (2015) state that the human beings are the nexus of all cybercrimes because of financial gains involved. The authors share that hackers attack systems as a way of demonstrating their capabilities. This could be a way of sending a message to the organisation to enhance its security protocols and cybersecurity astuteness. Gaumer, *et al*. (2016) details how hackers have not only become skilled in the technical aspects of cybersecurity but also at exploiting human frailties.

Keman and Pearlson (2019) state that with insider threats are perpetrated by employees who have a better understanding of the systems and thus, take advantage of the weaknesses of such systems to act unethically. The authors posit that it is difficult for organisations to understand and monitor their employees' behaviour. The only approach is to have stringent policies and penalties that might deter would-be-offenders. This is because the cultural view around cybersecurity in an organisation plays a huge role in the effectiveness of the security controls put in place and the inclination of employees to adhere to these controls. In order to guide the conduct of employees, Maja, Meyer and von Solms (2020) suggest the development of a cybersecurity code of conduct, education and awareness campaign programmes to restore moral principles so that organisations can develop sound cybersecurity strategies. Unacceptable human behaviour thrives when an organisation's cybersecurity and information systems security governance policies are ineffective and or there is an absence of awareness (Khan *et al.,* 2020).

2.5 Harms resulting from Cyber-attacks

The gravity of cybercrimes in Africa, specifically in South Africa-economic powerhouse for Africa, is disconcerting the corporate world. Technological advancements in the information society have brought an undeniable reality that the global business ecosystem is and continues to go under rapid change due to the advanced technologies and interconnection of information

systems (Singe & Signe, 2018). The 4th Industrial Revolution is welcome to the business ecosystem, but, it carries with it high exposure to cyber-attacks and threats. Cyber-threats and attacks are consequential to the global economy. The SABRIC (2019) reports that cybercrime has direct and significant impacts on **jobs, innovation, economic growth and investment** and this impact is significantly rising at an unprecedented rate. **Productivity** can be hampered by loss or theft data through cyber-attacks, resulting in recovery delays for the firm in an attempt to recoup loss or stolen data (Signe & Signe, 2018). If a firm is attacked by Trojan Worms, the only way to resolve the challenge is to halt systems in an attempt to mitigate the spreading of spyware. For example, the Renault Tanger-Mediterranee automobile manufacturing plant in Morocco, which, after the malicious code attack, was shut down for more than twenty-four hours (1 day) which affected the daily one thousand vehicle production (Signe & Signe, 2018).

Businesses experience huge **financial losses** through cyber-attacks due to the concept of globalisation which complicates regulators and law enforcements. Comizio, Dayamin and Bain (2016) state that globally, businesses leverage on technological platforms which transcend beyond the borders of many countries, but are sitting on the cloud, making it easier for cybercriminals to commit crimes. It is imperative that businesses must determine the amount to be spend on cybersecurity to prevent losses if leveraged technological platforms are risky. Firms that have been incessantly attacked and threatened or lost through cybercrimes might not attract shareholders or potential investors. This negatively affects a firm's image because potential investors would not want to invest in a firm that lacks security and stability of transactions. Vulnerability can lead to loss of market share/value due to the list of concerns (Smith *et al.,* 2018).

Perpetrators of cybercrimes are sometimes employees within the company, therefore, the recruitment and selection process of employees working with sensitive and secured information, should be thorough. The prevalence of breaches to a firm's information systems and data is consequential to the company, shareholders and more so, employees and reputational damage. These concerns cause turmoil in people's personal lives (Smith *et al.,* 2018). With a more focused approach on security, firms might safeguard information and transactions. Understanding the impact of cyber-attacks and threats on a business, reputational damage, financial losses and heart-aches, is an important step towards development of an information systems security strategy (Khan *et al.,* 2020).

Pribanic (2018) states that cybercrime can also damage **intellectual property.** A business' ideas, marketing plans, campaigns, business expansion plans or strategies can be stolen/attacked by criminals who might expose intellectual property to competitors. As soon as ideas are exposed to competitors, they become useless and sometimes cost the company months or years of valuable work (von Solms & Marnewick, 2019). Any growth and revenue gains would be damaged if the firm's data is breached.

Cybercrime is affecting civil society in as much as businesses are affected. In South Africa, people losing identity documents (IDs) through thefts only discover the losses after getting demand letters from credit providers to settle debt which they are not privy to (SABRIC, 2019). When credit providers send negative payment profile to credit bureaus, people with stolen IDs are black-listed and cannot access credit until their profiles are cleared through settlement of debts. In some instances, affected people might not get jobs because their stolen IDs are used in the commission of crime. The significant rise of cybercrime is a global challenge that envisages everyone's efforts and commitment to address the challenge. Initiatives to address cybercrimes are discussed in the next section.

2.6 Cybersecurity

2.6.1 Defining Cybersecurity

Bote (2019) and White (2020) state that the word "cybersecurity" is a culmination of the prefix "cyber" and the concept "security". Cyber threats refer to malicious conducts perpetrated in cyberspace targeted at damaging information and communication technologies (Arewa, 2018). Cybersecurity law is a branch of information technology law designed to protect ICTs, information, data and related digital technologies from malicious threats and criminal misuse (Chuma & Ngoepe, 2021). Von Solms and von Solms (2018) provide different definitions: cybersecurity is the same as information security; information security is part of cybersecurity; some cybersecurity attacks have nothing to do with information and cybersecurity is the inclusive term that replaces information security. Agrafiotis, Nurse, Goldsmith, Creese and Upton (2018) state that processes and technologies are designed to prevent unauthorised and potentially threatening actors from illegally accessing digital systems and assets. Other intrusion detection and prevention systems may be designed to limit any resulting harm. After a closer look at the two statements, the authors are defining the concept of cybersecurity. However, cybersecurity is a multifaceted endeavour that goes beyond technologies that include

people across varying roles within an organisation structure, and related processes that influence governance operation (Clark et al., 2020).

Cybersecurity covers a wide range of skills, ranges from policy, organisational security culture, network security, technical elements, and non-technical (Kevin et al., 2019; Furnell, 2020). Due to the related demand, there is no sector that does not need cybersecurity. Cybersecurity has become an important concern in the private and public sector (Kevin et al., 2019). The private sector and public sector are struggling to keep up with the required need for security in the increasingly sophisticated attacks from a variety of sources. Many organisations are increasingly concerned about cyber-attacks in the workplace and had invested a huge amount of resources to tackle this issue (Li et al., 2019). Therefore, cybersecurity is an important component for preparing society to understand the issues, deal and prevent various forms of violations (Buckley & Zalewski, 2019).

2.6.2 Motivating the need for legal and regulatory frameworks

Given the above definitions, it is clear that cybersecurity is a topical issue currently attracting global attention and consideration (Von Solms & von Solms (2018). Its importance and significance are growing daily because firms, information systems and data are vulnerable, therefore, it is concerning for leadership and information systems and information users not to take appropriate steps to preserve information assets. The PwC (2018) cyber-attacks report states that South Africa is the global radar of economies persistently vulnerable to threat actors and data breaches. Stein and Jacobs (2020) report that in the first half of 2020, after the emergence of Covid-19, there has been an unprecedented increase of security breaches to many firms and government departments globally. This indicates that cybercriminals are busy at work devising strategies to attack IT infrastructure.

With a plethora of global cyber threats and attacks affecting every state, governments should have goals to minimise crime, more specifically cybercrime. One way to address cybercrime is through the development national cybersecurity intervention strategies supported by legal and regulatory frameworks. White (2020) opines that cybersecurity is an organisation-wide concern that envisages concomitant efforts from everyone in the organisation, society and private sector to fight against cyber-crime. Safeguarding a firm's cyberspace is a more than a corporate governance responsibility, but, rather, it is everyone in the firm to take responsibility

and accountability in line with the associated legislative implications for possible negligence and or ignorance (von Solms & von Solms, 2018).

Therefore, public & private sectors, civil society, international experts, academia, cybersecurity research institutes, World Bank, ITU, the Global Cyber Security Capacity Centre (GCSCC) and courts should work together to develop strategies and interventions against cyber-attacks and threats. Cybersecurity as a high-risk problem has to be treated as such given the highly unpredictability nature of where, how, when and by whom threats may arise from (Yusif & Hafeez-Baig, 2021). A similar observation was noted by Zhang-Kennedy and Chiasson (2021) that cybersecurity is a problem that is significantly impacted by non-expert end-users who interact with online content. The aforementioned problem requires a change in the working environment and measures to guide how organisations, contractors, employees' affiliates access and use corporate networks against policies and procedures (Yusif & Hafeez-Baig, 2021). Etschmaier (2019) reports that in order to achieve cybersecurity there is a need for a holistic approach to develop a viable framework and processes that can mediate between the conflicting expectations of several actors in the cyberspace. Nevertheless, many frameworks restrict themselves to tangible effects that can be quantified and ultimately reduced to the common denominator of money. Some widely frameworks that could be used in the development of a nation's cybersecurity strategy are:

2.6.3 NIST Cybersecurity Framework

National Institute of Standards and Technology (NIST) defines information security as the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability (National Institute of Standards and Technology, 2019). Organisations require guidance on how to manage and reduce IT infrastructure security risks, therefore, the NIST provides standards, guidelines and practices which can be integrated to organisation security practices to prevent, detect and respond to cyber-attacks and threats (Schwab, 2019). The primary stakeholder of this framework should be government agencies, private sector owners and operators of critical infrastructure, users (communities and organisations). Given that the NIST CSF has been widely adopted across the globe, its major benefit is that it provides a common understanding across all staff in the organisation, at all points of the supply chain in order to develop a common and shared understanding of cybersecurity risks (Shen, 2014).

Reports also indicate that the NIST CSF helps organisations to understand cybersecurity risks, as well as how to reduce these risks with appropriate measures. Firms using the NIST CSF are able to respond and recover from cybersecurity incidents, thus, prompting them to analyse root causes and devise improvement interventions (Agrifiotis *et al.*, 2018). The NIST Cybersecurity Framework (NIST CSF) lists five core functions that must be concurrently and continuously performed in order to develop an operational culture that addresses the dynamic cybersecurity risks (Barrett, 2018). These core functions are: Identify, Protect, Detect, Respond and Recover (Shen, 2014). By integrating industry standards and best practices, the goal of NIST is to help organisations manage their cybersecurity risks, through a holistic cybersecurity program (Shen, 2014).

The five core functions are:

i) ***Identify function:*** the organisation has to understand how to manage cybersecurity risks to their infrastructure, assets people and capabilities. An asset management program, policies and risk management strategy are good examples of outcomes from the identify function. For people without any knowledge about cyber security, this governance, risk and compliance framework helps them to understand and explain cybersecurity policies. people with limited knowledge about the subject would use the laws to develop internal policies that make organisations to withstand complex cyber-attacks and threats (von Solms & von Solms, 2018; Malatji *et al.*, 2021).

ii) ***Protect function:*** Organisations require support to contain or limit the impact of cyber-attacks and threats. Therefore, the protect function outlines safeguards for critical services with potential outcomes such as Data Security protection, ensuring the security and resilience of systems is intact. Staff should also be empowered through training and development. Each firm's workforce is diverse; therefore, training and development programs should be tailored to the needs of employees' requirements while aligning with the firm's objectives (Fache, 2018). It is the responsibility of management to identify cybersecurity training needs, update cycles, risk assessment processes, intelligence gathering initiatives and loss incidents training requirements in line with the firm's cybersecurity risk management policies. The absence of cybersecurity training can expose a firm

increased risks of successful cybersecurity attacks and threats Maja *et al.* (2020) assert that cybersecurity training and awareness programmes are helping firms to proactively prepare for any cyber-attacks and unscrupulous threats targeted at their IT infrastructure.

iii) ***Detect function:*** Appropriate activities, technical controls and monitoring mechanisms should be applied to help identify the occurrence of cybersecurity events timeously. Strous, von Solms and Zúquete (2020) recommend the implementation of cogent security protocols and controls throughout the organisation's IT infrastructure. Database managers must provide effective controls regulating who access, how and for how long they access what type of data. Encryption and penetration tests are performed to identify security weaknesses (Maja, Meyer & von Solms, 2020). The effective ness of protective measures should be verified regularly in line with the organisation's cybersecurity policies. Incident response planning sets out common practices that guide security leadership in response to cybersecurity threats and attacks.

iv) ***Respond function:*** Shen (2014) assert that this function of the NIST CSF helps organisations to carry out response strategies or action plans when cybersecurity incidents are detected. The goal is to minimise the impact of cyber-threats and attacks. Kuhlman and Kempf (2015) identified the following incidents response practices: existence of regular reviews of threat intelligence; data recovery plans should be in place; client confidence plans should be in place as assurance for compensation of financial losses. Organisations ensure that response planning processes successfully executed during and after a cybersecurity event/incident and that communications are properly managed to mitigate misinformation. Stein and Jacobs (2020) agree that at the peak of the Covid-19, there was an increase of misinformation about the virus etc. All response activities should be analysed to establish their effectiveness, and if need be, corrective action should be taken.

v) ***Recover function:*** The organisation has the responsibility to identify activities to maintain plans for resilience and restoration of services disrupted during the cybersecurity events (Shen, 2014). With reference to the complexity of

cybercrimes, it is advisable that firms should periodic cybersecurity risk assessments to identify security weaknesses and likely risks posed by third-party vendors (Galine *et al.*, 2017). Cybersecurity risk assessments should also consider internal and external threats caused by BYODs (Hockey, 2020). There is a proliferation of Bring Your Own Device (BYOD) approach where some organisations allow employees to use their personal devices for work purposes. The advantage is that the company does not need to spend money buying, insuring or replacing individuals' personal devices (Dingwayo & Kabanda, 2017). However, the greatest challenge is that some companies do not have policies or monitoring mechanisms to see how devices are connected to their network. Neither is there a record to show who in the organisation has how many devices nor how many devices each person is allowed to log onto to the corporate network (Kerr, Talaei-Khoei & Ghapanchi, 2018).

2.6.4 Cybersecurity Maturity Models for Nations (CMM)

The Cybersecurity Capacity Maturity for Nations was conceptualised in 2014 by the Global Cyber Security Capacity Centre (GCSCC) in the United Kingdom. Over 200 experts from international and regional organisations, private sector and academia developed the CMM with the goal of obtaining community's knowledge, whilst extracting pertinent factors required by a nation's cybersecurity capacity and the ideal steps towards reaching the levels of maturity (GCSCC, 2021). Five dimensions of maturity were considered. Between 2015 and 2021, the CMM but has retained the five dimensions briefly discussed below:

i) *Dimension 1: Cybersecurity Policy and Strategy*: In this dimension, the focus is to explore a country's capacity to develop and deliver a cybersecurity strategy. For example, South Africa has put together a number of interventions, legal and regulatory frameworks in its quest to enhance its cybersecurity resilience. The National Cybersecurity Policy Framework has been established to improve the country's incident response, cyber defense and critical infrastructure capacities (Maja *et al.*, 2020). The GCSCC (2021) states dimensions 1maintains the benefits of cyberspace vital for government, civil society and international business through deployment of an effective strategy and policy that delivers a national cybersecurity capability.

ii) *Dimension 2: Cybersecurity Culture and Society:* This dimension explores the existence of reporting mechanisms for users to report cybercrime, the role of media and social media in how they shape cybersecurity values, attitudes and behaviour. The GCSCC (2021) asserts that dimension 2 examines elements of a responsible cybersecurity culture such level of trust in internet services, e-government, e-commerce, understanding of the protection of personal information in an online environment and cyber-related risks in society.

iii) *Dimension 3: Building Cybersecurity Knowledge and Capabilities*: This dimension examines a country's or organisation's awareness raising, professional training and formal cybersecurity programmes. That is, the availability, uptake and quality of these various programmes are vital in building cybersecurity knowledge and capabilities for various groups of stakeholders. StatsSA (2019) has reported the acute IT skills shortage in South Africa. Dimension 3 is one of the nine influencing factors contributing to misalignment of the SA-NCPF as would be discussed later in this study. Dutton, Creese, Shillair and Bada (2019) posit that capacity building requires attention across sectors, thus, more resources should be made available if the country has to build its national cybersecurity capacity. Diverse activities and action plans such as developing the managerial, technical, social, legal, policy and regulatory initiatives are a must in order to enhance its resilience to cybersecurity breaches, terrorism and cybercrime (Dutton et al., 2019). Creese, Dutton, Esteve-Gonzalez and Shilliar (2021) state that cybersecurity is a growing centrality pushing many governments and international organisations across the globe to focus on building capacity for nations to withstand cyber threats to the public and digital resources. The authors agree that capacity building is a relatively new area, but there is a large number of frameworks around to help nations with cybersecurity capacity building initiatives.

iv) *Dimension 4: Legal and Regulatory Frameworks:* This dimension examines the country's capacity to design and enact statutes directly or indirectly relating cybersecurity. Emphasis is placed on cybersecurity regulatory requirements, cybercrime-related legislation. It also focuses on how these laws are enforced,

successful prosecution and capacities of courts and law enforcement agencies. One challenge that has been widely reported in South Africa is the inability of courts to successfully prosecute cybercrimes due to misunderstanding of cybercrime. A lack of cybersecurity legal expertise and knowledge has been highlighted as an influencing factor in this current thesis.

v) *Dimension 5: Standards and Technologies*: There are different cybersecurity standards such as the Health Insurance Portability and Accountability Act (HIPAA), ISP/IEC 27001/2, ISO /IEC27031, NIST CSF, COBIT and technologies used to protect individuals, organisations and national critical infrastructure. Governments and companies are evaluated against their ability to implement cybersecurity standards and best practices, processes and controls and development of technologies to reduce cybersecurity risks (GCSCC, 2021). Figure 2.4 illustrates the five dimensions of the CMM.

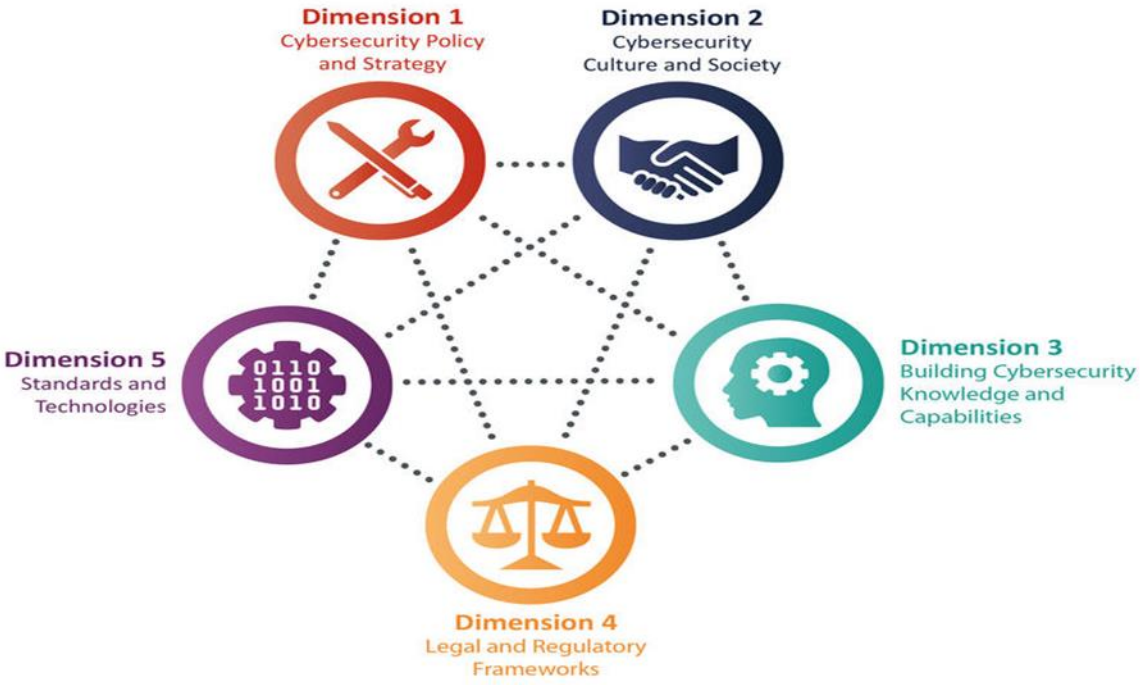

Figure 2.4 Five Dimensions of the CMM (Source: Global Cyber Security Capacity Centre, 2021)

All the five dimensions align with the tenets of this thesis on three aspects namely: 1) all the dimensions represent all influencing factors affecting the alignment of the SA-NCPF, whose interplay is complex and difficult to understand from a human perspective, 2) the objective of

the SA-NCPF is to develop a coherent and effective national cybersecurity strategy built on all the five dimensions and 3) South Africa has not achieved the CMM, given the goals of the five dimensions. However, SA has involved a wide cluster of stakeholders who are typically invited for consultations. These include academia, civil society groups, governance representatives, criminal justice and law enforcement, government departments, legislators, CSIRT, IT leaders from private & public sectors, critical infrastructure I +II, international and regional cooperation, Cyber Task force and private and business (Mahlobo, 2015; Chigada, 2020; GCSCC, 2021). The challenges of a wider cluster of stakeholders are the overlapping mandates, coordination, multiplicity of systems and silo approach resulting in misalignment of the SA-NCPF to national, regional and international cyberlaws.

2.6.5 ITU National Cybersecurity Strategy Toolkit

The International Telecommunications Union (ITU) developed a cybersecurity toolkit with the support and assistance of many global players such as Microsoft, World Bank, Global Cyber Security Capacity Centre just to mention a few (ITU, 2019). The goal of the toolkit is to help states to develop or improve their national cybersecurity strategies. For example, this thesis established that the SA-NCPF lacks alignment to national, regional and international cyberlaws and policies. The toolkit provides guidelines for any country to obtain a better understanding of National Cybersecurity Strategy in terms of how to develop a strategy, build capabilities, relevant models and resources. Developing countries like South Africa are constrained in terms of IT and cybersecurity legal skills. Therefore, the toolkit is a single resource of information.

As a single tool, national governments and stakeholders can evaluate their current status in each of the strategic areas in the reference guide (ITU, 2019). The toolkit helps governments to evaluate their current position in cybersecurity lifecycle management and identify areas for improvement. The primary focus of the National Cybers Security (NCS) is that policy developers will be able to identify the purpose and content of their country's national cyber security strategy, outline strategic areas, establish a structured process for strategy development and mobilising additional resources to support the development of strategy. The secondary focus of the toolkit is the provision of links to other best practice guidelines on how to develop the national plan, evaluate current maturity levels (similar to the CMM by the GCSCC) of their cyber security capabilities as well as comparing their strategies against peers through ranking systems. This is a very important statement in the ITU NCS toolkit which speaks to the current

study. This means aligning a nation's cyber security strategy or policy framework. In this thesis, the nexus of the problem is the misalignment of the SA-NCPF. Figure 2.5 summarises the ITU NCS toolkit.

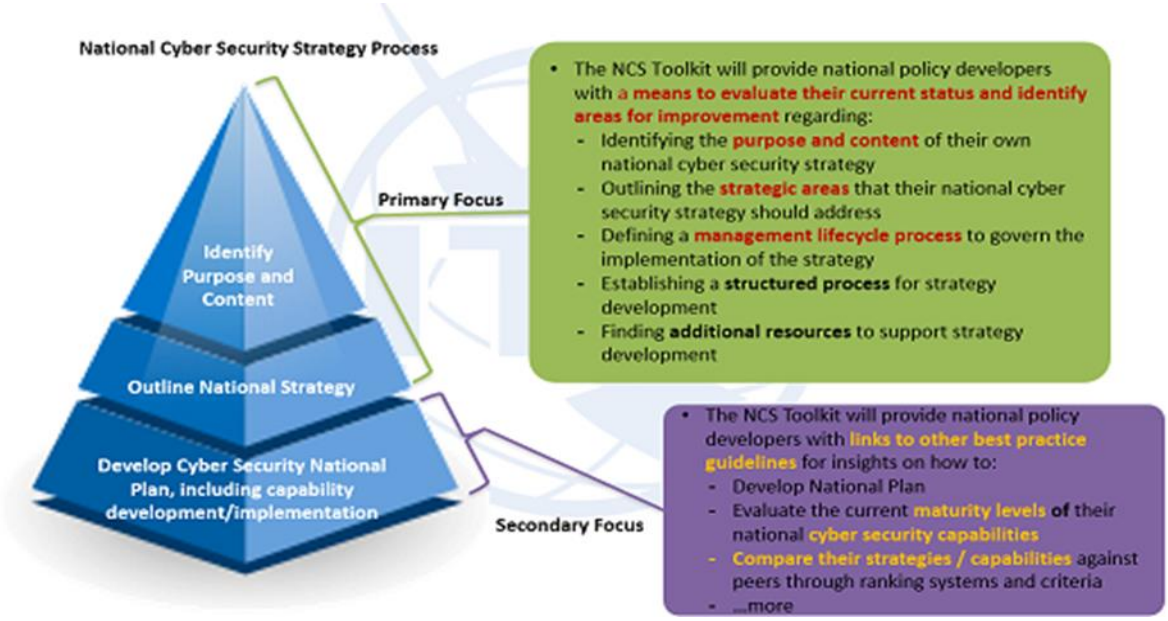

Figure 2.5 ITU NCS Toolkit (ITU, 2021)

2.6.6 World Bank Cybercrime Toolkit

The World Bank is cognisant of the effects of cybercrime across the globe, therefore, it plays an important role to develop measures and suggestions to maintain order in cyberspace. In 2014, the World Bank launched a project entitled "Combating Cybercrime: Tools and Capacity Building for Emerging Economies". When closely analysed, the title of the project brings in Dimensions 3 and 5 of the GCSCC CMM model. This indicates that the GCSCC has been recognised as an influential player in addressing cybercrime across the globe. Given that emerging economies are resource constrained and hard-hit by threat actors, the goal of the World Bank toolkit is to build capacity in order to mitigate cybercrime through a synthesis of good practices in the policy, legal and justice aspects of an enabling environment (World Bank, 2017). Policy-makers, legislators, public prosecutors and law enforcement agents would benefit a lot from the toolkit because these individuals are confronted and deal with legal and legislative issues related to crime. In this thesis, the author states that data was collected from this target population because of their proximity working with crime on a daily basis.

Given the clear goals of capacity building, the author of this thesis agrees that some cybercrimes are not detected or cybercriminals are not successfully prosecuted because of incapacitation, a lack of tools and expertise. The concept of cybersecurity is not well known among civil society because the platforms for educating and awareness are limited by lack of resources and the sensitivity of the subject matter, therefore capacity building should include training and education awareness programmes so that civil society is conscientized about cybersecurity (Malatji *et al*.,2021). Private and public sectors are not willing to share information for fear of exposing trade secrets or damaging their brands (Bote, 2019), thus, stifling efforts to understand what cybercrime is.

The toolkit synthesizes good practices in the policy, legal and criminal-justice aspects so that cybercrime can be combated (World Bank, 2017), while the assessment tools enables a country to diagnose its current capacity to combat cybercrime and identify capacity-building priorities. The World Bank along with the Global Forum on Cyber Expertise Secretariat (GFCE) and Korean Supreme Prosecutors' Office will establish a training and capacity building centre in Seoul. Drawing from the World Bank toolkit, Yoon (2019) agrees with the author of this thesis that some countries' criminal laws are either incomplete when dealing with cybercrime or they are misaligned with regional laws as far as cooperation is concerned to combat cybercrime. What is pertinent from Yoon's (2019) study is that nations are not appropriately equipped to combat cybercrime and that the different stakeholders do not expedite sharing and assistance in cybercrimes. These views have been raised in this thesis as stifling opportunities for exchanging insights about cybercrime trends. Therefore, at national level, efforts are required to develop an appropriate legal framework and at international level mechanisms should deployed to create interoperability of those national frameworks. Failure to align national frameworks to international levels can create safe havens for cybercriminals (Yoon, 2019).

The World Bank (2017) and Yoon (2019) are clear that cybercrime committed beyond territorial borders is very difficult to investigate and prosecute, therefore, cybersecurity actions should be taken through multilateral instruments rather than unilateral effort. For example, South Africa has the NCPF for combating cybercrime, therefore international cooperation is necessary to expand national territorially-based purview and build effective networks of interoperability that can function coherently and cohesively.

The deployment of any of the above cybersecurity frameworks or toolkits will not only enhance nations' cybersecurity strategies, but will serve as global best practices for combating cybercrime. Given that these toolkits and best practices have been tested for their effectiveness, it would be ideal for developing economies such as South Africa to benchmark its NCPF with global standards, hence this thesis seeks to get that solution. While the above toolkits provide guidelines on how nations can enhance their national cybersecurity strategies, the GCSCC (2021) advocates nations to evaluate their current levels of capacity building.

2.7 Chapter Summary

This literature review chapter described the concepts of cybercrime and cybersecurity. The discussions in this chapter are clear to help civic society, public and private sector organisations to understand the types of cybercrimes, whilst, putting into place, intervention strategies and mechanisms to mitigate potential cybersecurity risks, threats and attacks. It has been revealed that cybercrime is consequential to civilians, public and private sector firms globally, therefore, concerted efforts towards an information systems security strategy are required now more than ever before. Theoretical perspectives that have been identified to exacerbate cybercrime include: lack of understanding of cybercrime, fragmented legislation, information asymmetries and economic factors. The researcher discussed different interventions augmenting existing controls and mechanisms and these include: cybersecurity and others in an attempt to elucidate to readers and the larger IS community at large of different mitigation interventions that can be adopted to reduce the effects of cybercrime. The responsibility ultimate lies with the firm's security leadership to identify appropriate combinations of strategies to mitigate. In the next chapter, the South African Regulatory environment is discussed.

CHAPTER THREE
THE SOUTH AFRICAN LAW-MAKING PROCESS, REGULATORY ENVIRONMENT AND INTEGRATIVE THEORETICAL FRAMEWORK

3.1 Introduction

The preceding chapter presented detailed discussions relating to cybercrimes and cybersecurity. The study has shown that there is an exponential rise of cybercrimes and in the wake of the global Corona Virus Disease-2019 (COVID-19), organisations and individuals are attacked and threatened on a daily basis losing trillions of USD in the process (WHO, 2020). Given the extent of effects of cybercrimes in the global economy, South Africa has enacted a number of e-legislation to address escalating cybercrimes. The present chapter provides an overview of the law-making process, drawing lessons from Australia, the United Kingdom (UK) and United States of America (USA) because South Africa has adopted and implemented similar processes used in the three countries. The South African law-making process will be discussed using an integrative theoretical framework. The integrative theoretical framework comprises various theories drawn from other disciplines to help understand different aspects more comprehensively. The regulatory framework in the country is discussed through the lens of various pieces of legislation and who is responsible for coordinating them. The gaps identified in literature are outlined followed by a chapter summary.

3.2 An Overview of Law-Making Process

Bogdanoskaia (2013) defines the law-making process a form of the state activity intended for the creation or revision of legal norms. The term "law" means legislation- all acts adopted by government bodies or natural law. Therefore, the law-making process is an important activity during which an idea of law is transformed into law. Orji (2012) states that there are different forms of law namely: acts of legislative bodies (statutes), acts of executive bodies, judicial precedents and legal customs. The law-making process for each of these forms of law is distinct. For example, the state endorses or approves the created norm when legal customs are formed by the recurrence of a norm (Bogdanoskaia, 2013). Acts of legislative bodies (statutes) follow through an organised approach, but several steps are involved. Each step allows society-

public and private sector organisations opportunities to scrutinize or question each idea. However, in a Constitutional state like South Africa, the law-making process is a political process and cannot be regulated by law (Selebalo, 2014; Johnson, 2017).

Bogdanoskaia (2013) argues that when governmental bodies make laws, a more organised and structured approach is adopted, unlike the law-making process of legal customs which are spontaneous. Therefore, citizens of the country are given an opportunity to participate in these processes. Thus, involvement of diverse stakeholders prolongs the law-making process because a number of stages have to been undertaken, debating and negotiation of key issues before they are finalised as official government policy or law. The intention is to adopt and propose laws or policies that satisfy society. A legal system should reflect society's changing demands and interests. The process is achieved on democracy and science in order to project a true reflection and development of society.

The political process takes a greater portion of the law-making process. Despite legal experts formulating the main principles of this process, it is very important that authorities enforce these principles into practice. Political leaders, through Parliament and other law-makers have a Constitutional responsibility to implement the main principles, because laws are the main source of the national legal systems (Department of Justice, 2019). In democracies, statues are the main source of all national legal systems, hence it is important for the state, society, social and political groups to co-create and elaborate the laws. Laws have superior legal force after the Constitution. In some countries, it can take a few years before a proposed law or policy is implemented and its effects felt on the ground (Department of Justice, 2019).

Australia, UK, USA and South Africa have been chosen in this study to understand their law-making processes. The motivation for selecting them is: USA is a global superpower with reference to technological developments and is thus, considered the pioneer of the world's most advanced cybersecurity technologies, laws and has been exposed to terrorist threats and attacks. The UK has been chosen because of its global economic influences and technological advancements. After reading several newspapers, Internet and attending conferences, the researcher is convinced that the UK wields excessive political power over Commonwealth countries, thus, many economies develop their policies and models around the British system under the auspices of the Commonwealth banner. On the other hand, Australia has been chosen as progressive continent and has reported extensively on cybersecurity. In addition, Australia

has a Cybersecurity Policy Framework which regarded as effective by China, New-Zealand and Malaysia (Australian Parliament, 2018). The Australian law-making process has traits similar to the USA, UK and SA, therefore, it was chosen as a global benchmark. Australian law-making process is derived from the practices of the British Parliament.

3.2.1 Law-Making Process in Australia

Section 51 of the Australian Constitution gives the Australian Parliament the power to make laws in relation to certain matters. Two legislative bodies- the Senate and House of Representatives have a mandate to develop and present the Bill to Parliament. The first step is that both the Senate and House of Representatives introduce the Bill for first reading to the House of Representatives and to the Senate respectively (Australian Parliament, 2019). Members of both Senate and House of Representatives engage in the second reading of the bill (step 2), which allows debates and voting on the main ideas of the Bill.

The House Committee (House of Representatives) and Senate Committee (Senate) engage the public (society) for their inputs. The two Committees report back to the House and Senate respectively. In order to consider the Bill, House of Representatives discuss the Bill in detail, including any changes to the bill. While Senators discuss the bill in detail for consideration of the whole. The third reading commences afterwards where members and senators vote on the bill in the final form. The Bill is passed in the House of Representative and Senate respectively. The Governor General assents or signs the bill, thereby becoming an Act of the Australian Parliament-ultimately becoming law.

Given the lengthy processes involved in making laws, it is acknowledged that it may take months or years for the bill to pass through Parliament. In exceptional instances where urgent bills are passed in hours or days (Australian Parliament, 2018). Over ninety percent of Australian government bills are passed into law annually. Most of the country's Bills come from different origins. For example, a Minister can be advised by one's department about an existing specific problem which in turn might require a bill to fix the problem. Community groups, businesses or lobby groups might exert pressure to change or improve a specific area of Australian law. Thus, will approach Parliamentarians with suggestions for bills. The third origin of bills is through political parties which might have different perspectives of how the country should be governed. Therefore, political parties introduce bills in Parliament in order

to put ideas into action. Bills can originate from Parliamentary committees to examine current issues and make recommendations, usually in the form of a new bill.

3.2.2 Law-Making Process in the United Kingdom (UK)

The United Kingdom (UK) has a Parliament that operates similarly like the South African Parliament. The two legislative bodies- House of Commons and House of Lords develop and present Bills to Parliament (Telegraph, 2014). Bills presented by either legislative body are challenged by the other body, thus, the process of enactment the Bill into law is prolonged due to disagreements. The UK Parliament (2018) states that both houses (House of Commons and House of Lords) have set stages to debate, examine and suggest changes to the draft Bill. Further, the two houses should agree the final bill before it can be signed off by the monarch (Royal assent) and become an Act of Parliament-law.

The British are exposed to Parliamentary activities such as proposed Bills, therefore, the public has the opportunity to debate and resist new Bills, thus, the two legislative bodies may not pass Bills into laws if there is public rejection or there is little public input, while in the South African context, the Bill that was resisted was the Secrecy Bill. In addition, the UK law-making process is influenced by the European Union (EU)which is exerting considerable amount of pressure on EU member states, to develop legal systems that promote regional and global trade.

As pointed out, the Australian law-making process derives its practices from the British system, thus, both countries have two legislative bodies responsible for developing and introducing bills into Parliament and the law processes for the two countries follow six steps (first reading, second reading, committee stage, report stage, third reading, consideration of amendments and Assent). The only difference between the two countries approach to law processing is that the UK has three types of bills- Public bill: which affects the entire economy, thus, cabinet prepares to change the laws of the country. Private Members bill- prepared by Members of Parliament. For example, the Abortion Act. Private Bill is usually proposed by large companies or a local authority (Office of the Cabinet, 2013).

3.2.3 Law-Making Process in the United States of America (USA)

Federal laws in the US are made by the US Congress which is equated to the South African Parliament. Sullivan (2010) states that two legislative bodies-US Senate and House of Representatives) are responsible for the development and presentation of Bills to the US

Congress for consideration. Both legislative bodies present Bills for public review before enactment into law or Acts (Sullivan, 2010). American citizens are given adequate time to analyse and critique Bills through public debates, which is contrary to the South African scenario, which does not give the public adequate window period for public input (Selebalo, 2014). The US Senate and House of Representatives draft legal systems which are integrated to work together to achieve a specific goal in line with the views suggested by systems theorists. Bertalanffy, Rapoport and Gerard (1956) state that the behaviour of complex phenomena and drive towards unity can only best understood by relationships formed by various legal systems. Thus, various pieces of legislation available in the global economy should interact with each other to form patterns/configurations that provide insights into how cybersecurity challenges can be addressed. The views by Bertalanffy *et al*. (1956) resonate with the Gestalts approach adopted in this study in an attempt to understand how different elements and legislation can work in harmony (unity of science) to yield the desired goals.

3.2.4 Law-Making Process in South Africa-An integrative theoretical framework

The Integrative theoretical framework was developed to bring a better understanding and explanation to the law-making process in South Africa. This integrative theoretical framework brings together different theories that help describe the processes followed by lawmakers in Parliament. By reviewing the law-making processes of the UK, USA and Australia, the intention was to buttress that South Africa uses existing processes from developed economies. Thus, appropriate theories are drawn from different disciplines to show how laws are made in South Africa. In all instances, there are two legislative bodies responsible for developing and introducing the Bills to Parliament. The South African Parliament is the legislative body of the country with the responsibility to pass new laws, amend existing laws and repealing or abolishing old laws (Parliament of South Africa, 2019). Parliament is empowered by the Republic of South Africa Constitution- which governs and applies to all laws and conduct within the country. Sullivan (2010), Orji (2012) and van der Merwe *et al.* (2016) define law as a system of rules which are enforced through government institutions to regulate human conduct and behaviour. A country's political, economic and social systems are shaped by the country's laws. A legal system raises fundamental issues concerning equality, fairness and justice (The Human Rights Watch, 2012). The following law-making steps are discussed through the lens of theoretical works to understand the aspects comprehensively. This is illustrated in Figure 3.1.

3.2.4.1 Introduction of Bill in the National Assembly or National Council of Provinces

The first step in the law-making process occurs when the bill is introduced in the National Assembly (NA) or National Council of Provinces (NCOPs). The NCOPs is guided by Section 76 of the Constitution Act 108 of 1996, for ordinary bills affecting provinces, while the NA is guided by Section 75 for ordinary bills that do not affect provinces. The Minister, Portfolio committee or Assembly member introduces the bill in the NA for discussions and or amendments. For bills affecting provinces, they are first introduced in the NCOPs or NA and referred for debates or amendments by the committee. Further debates occur in the NA or first house and then passed for public participation. Political and Chaos theories dominate the first step in how laws are made in South Africa. For example, the deliberate democracy school of thought in ***political theory*** views exclusion of civil society from the law-making process as unfair and unreasonable resulting in conflicts and inconsistencies (Egan, 2007). South African communities have limited access to Parliamentary debates, therefore, civil society's contribution is excluded (Selebalo, 2014).

Due to poorly advertised Parliamentary events such as public hearings and debates do not give ample time to the public to participate and debate Bills resulting in low organisational knowledge conversion rate (Selebalo, 2014). This can be viewed as a deliberate strategy to exclude the public from participating in the law-making process. If the Bill is not agreed upon, disagreements will arise. The dominant House (wielding more power) will subdue the viewpoints of the other House (Eagan, 2007). It is argued that Portfolio Committee members should embrace diversity and work as unity to achieve the desired objectives of developing legislation. Harmony is not about uniformity rather it entails diversity, but when elements are in harmony, even though their individual attributes remain, they form a completely fresh feature (Isasi, 2009).

Chaos theorists assert confusion arises if there is an apparent lack of order in a system (Lorenz, 1961). Inequitable distribution and use of resources also creates conflicts between agencies resulting in confusion between systems elements in the law-making process (Lorenz, 1961). Chaos theory focuses on random and unpredicatble events.

3.2.4.2 Bill referred to relevant Portfolio Committees

Parliament establishes a range of Committees with assigned powers and functions and are compelled to report regularly to the House for debate and decision. Therefore, the law-making

process happens in committees and it is the portfolio committees that oversight of the executive is done through portfolio committees (Parliament of South Africa, 2019). Each government department is represented with a portfolio committee. Different political parties ***(Political theory)*** are represented in these portfolio committees with the objective of taking an oversight and accountability role to determine if government departments deliver on what they promise and whether they spend taxpayers' money responsibly. Conflicts are bound to arise especially where different political parties and ideologies debate Bills. This is due to scrutinization of bills that cover that department's area of jurisdiction, report on the department's budget and strategic plan (Bateman, 2013). The bills are published in the government gazette eliciting public participation and comments. The challenge that confronts South Africa is the limited access to media which affects people's exposure to legislative debates in Parliament. Thus, the law-making process is perceived to exclude citizens from participation ***[Chaos theory]*** (Selebalo, 2014). Selebalo (2014), Schultz (2016) and van der Merwe (2016) and Shaw (2017) have all raised concerns that the public is not afforded adequate time to read through and scrutinise Bills gazetted. This is further exacerbated by limited access to media and Parliamentary legal issues.

Resource-based theory contends that possession of strategic resources provides an organisation with a golden opportunity to develop competitive advantage over its competitors (Barney, 1991). The resources-based theory explains that the Parliament is a representation of an organisation with a set of resources that should be utilised to produce new legislation (Penrose, 1959). The NCOPs, NA or Parliament of South Africa require resources to produce products and services. In this instance, Bills that are enacted into Law or Acts are developed by experts drawn from the legal, IT/IS or other disciplines and civil society. The **Resources-Based Value theory** (RBV) complements the organisational **knowledge conversion theory** through the lens of optimal utilisation of resources to create knowledge assets (Penrose, 1959). IT and legal skills in cybersecurity are rare, difficult to imitate and invaluable to the long-term success of the organisation. In this study, these resources are invaluable to South Africa as a whole. The StatsSA (2019) and Bote (2019) agree that there is a shortage of these and other skills in the country because they are fundamental to providing a strategic foundation to the development of an effective national cybersecurity strategy and the NCPF to lead to superior performance over time.

3.2.4.3 Bill is debated and Amended in Committees

With reference to public participation and comments, the bill is referred back to Portfolio Committees for further debates and amendments. This is another repetitive process that stifles the enactment of Law. Given the diversity of Committee members' knowledge, skills and political affiliations, portfolio committees prolong consensus and passing of the bill. Suffice to say, this process is a repetition, thus, financial, time, human and other resources are duplicated in this and the next step where the Bill is referred to the sitting house for further debates before a vote is taken (Claassen *et al.*, 2012; PwC, 2018).

Cybercrimes are complex and require sophisticated knowledge to understand, while on the other hand the South African law-making process comprises different actors with diverse skills, viewpoints and ideologies. In addition, the regulatory environment comprises fragmented pieces of legislation coordinated multiple agencies. Given this context of systems, the cybersecurity landscape in the country presents complex adaptive systems. Bonicci (2015) states that Complex theory provides a better understanding of how different systems grow, adapt and evolve overtime. In this thesis, the researcher acknowledges the existence of relationships between members of these systems which give rise to a collective behaviour. As these systems (Parliamentary Committees) interact among each other, it should be noted that complexity arises when they interact with their environments. For example, the multiple agencies interact with society, public and private sector and international institutions, creating complex interactions. Bonicci (2015) posits that organisations should be viewed as sets of complex self-organising components made up of employees, resources and stakeholders, therefore, there is bound to be chaos in complex systems.

3.2.4.4 Bill is submitted to the House for further debate

This stage entails a further review by the sitting house to ascertain if the Bill will benefit society, political and social groupings. However, the researcher noted that this is another repetition of stage 2 and stage 3 discussed above. One would expect the input from the public, debates and concurrence of the NCOPs and NA are adequate to present and defend the Bill in Parliament before the President of the Republic assents to it into an Act of Parliament-law. Selebalo (2014), PwC (2018) and Chigada and Kyobe (2018) all agree that this stage of the law-making process defeats the logical flow from the first to the sixth stage. There is seems to

be disorder, irregularities and unpredictability which might result inconsistencies. Involving many people and departments will breed chaos from further interactions and debates.

Lorenz (1961) illustrates *chaos theory* through the analogy of a butterfly stirring in the air in Hong Kong today can change storm systems in New York the next month. Kauffman (1969) posits that chaos occurs when there are varying behavioural traits of a complex system which lacks order. The Government Gazette (2015) indicates that the Bill passes through a number of readings in the NA and NCOPs, where processes are duplicated and the logical order is difficult to understand. Lorenz (1961) conceptualised chaos theory as a result of lack of order in a system and the processes followed in the law-making can cause very complex behaviours to happen. Furthermore, Chaos theory is best explained by the self-organising formed by the subconscious rules which are followed by different government agencies coordinating different pieces of legislation. Each government agent maintains a distance from the other because they are complex systems that should grow, adapt and evolve overtime.

3.2.4.5 Bill is transmitted to the other House for Concurrence

If the Bill is not agreed upon in stage 4 above, disagreements will arise. The dominant House (wielding more power) will subdue the viewpoints of the other House (Eagan, 2007). The author posits that where Committees are involved, the probability of conflicts arising is very high (Marx, 1871), resulting in confusion or lack of harmony (Lorenz, 1961). The potential for divergent viewpoints is likely to trigger conflicts and overlapping roles and responsibilities. Though Portfolio Committees are encouraged to embrace diversity, the political landscape is polarised and characterised by hackling and lack of respect, thus, rifts are most likely to arise. If concurrence is achieved, then the Bill is sent to the President to assent.

3.2.4.6 President of the Republic Signs the Bill into an Act

The President of the Republic is empowered by the Constitution of South Africa to sign Bills into Acts of Parliament. This stage occurs if there is concurrence between different houses and within Portfolio Committees. Literature suggests that the exercise of power is accepted as endemic to human beings as social beings (Wilson, 1999). The President's actions will inform and determine the future of the country's laws (Colangelo, 2016). Laws passed without consultations and involvement of all stakeholders, will not address what they are designed to

do, therefore, a disjoint/misalignment arises (Giddens, 1984). Once the Bill has been signed, it becomes legal/an Act of Parliament/law as shown in the next stage discussed below.

3.2.4.7 Act of Parliament/Law

The Act/Law of the Land comes into being as a result of interactions between different constructs, optimum utilisation of resources and relationships between individuals and society. The President assents or signs the Bill into law or Act of Parliament and it becomes a legal system for the benefit of society, social and political groupings. Relationships between Parliament, civil society, private and public sector is imperative to develop laws that benefit everyone in the country. Businesses need laws that protect them against competition, while, civil society needs laws that protect them against substandard products, crime and other unethical conduct. Giddens (1984) states that with Structuration theory or theory of social action, different actors in the law-making process should be viewed in terms of action and structure rather than separate entities. Structuration theory acknowledges the interaction of power, standards, meaning, values and a dynamic relationship between different facets of society. Giddens (1984) stresses the need for rules and resources to create a social system.

The explanation above tallies with the law-making processes of the other three countries (Australia, UK, and USA). The author of this thesis acknowledges that South Africa, as a developing economy has made good efforts in developing its national cybersecurity legal and regulatory frameworks premised on Australia, UK and the USA. However, the effectiveness of its NCPF is doubtful given its shortcomings against the GCSCC CMM, World Bank toolkit, NIST CSF and the ITU NCS. Adopting suggestions and guidelines provided for by the above institutions would help address the law-making process in the country. Figure 3.1 summarises the SA law-making process.

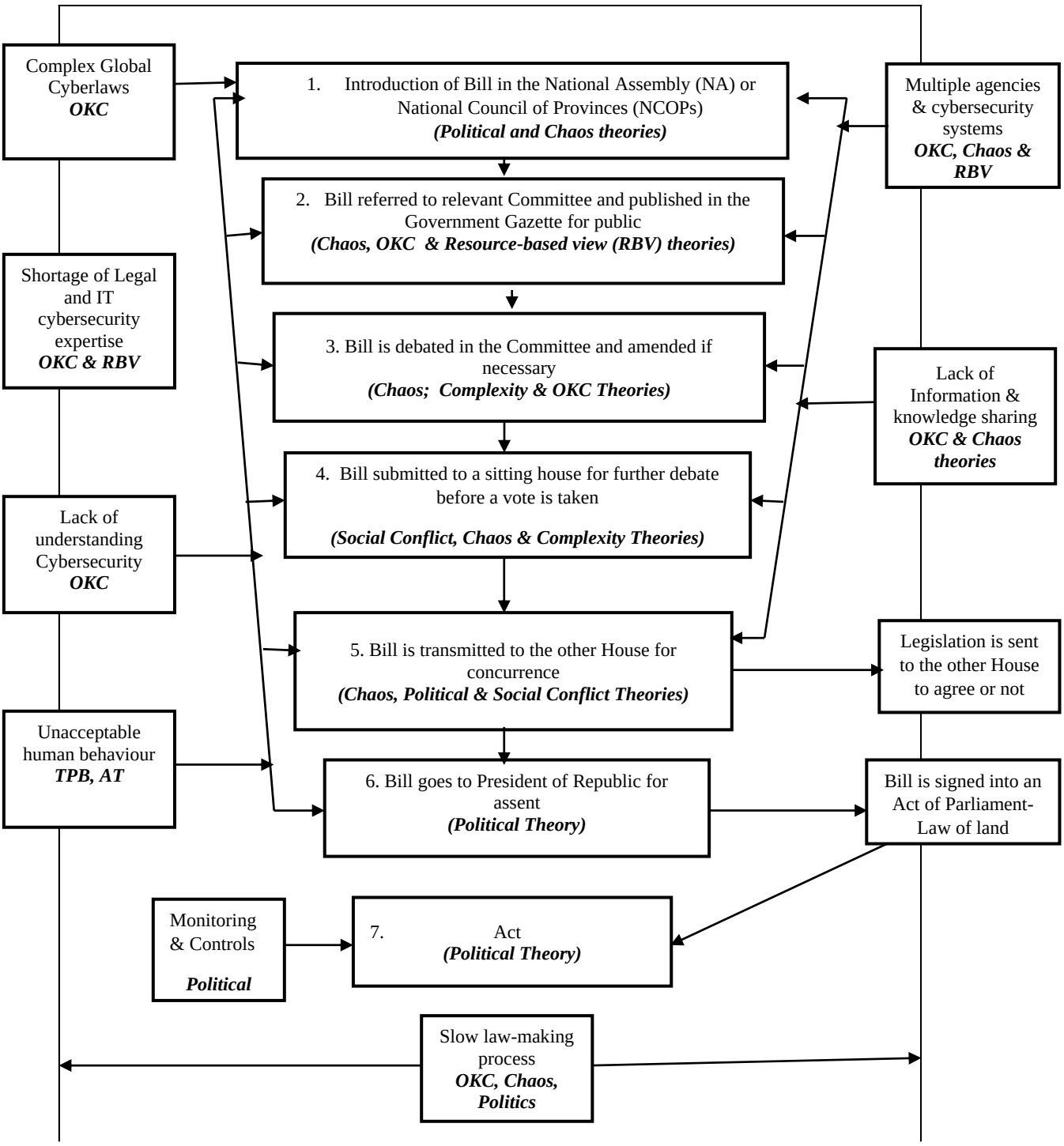

Figure 3.1: Integrative Theoretical Framework (Parliament, 2019; Author, 2021)

3.3 Weaknesses in the South African Law-Making Process

The law-making process model illustrated in Figure 3.1 above highlights seven stages that are followed in South Africa. However, the researcher has identified the following weaknesses which are considered paramount to the study:

In the first stage, the researcher established that two legislative bodies are involved in developing and presenting Bills to the NA, which involves a duplication of responsibilities and roles, thus more resources are required to ensure the next stage is achieved. In stages two and three, there are overlapping roles and responsibilities and at most, repetitive tasks which consume more resources (time, finance, human). In addition, public participation or comments to gazetted Bills is minimal due to limited access to media or communication channels that allow them to access Parliament related information. Given the limited access to internet-based resources, a huge percentage of the public is excluded from commenting and or contributing to debates on proposed Bills.

Stage four has clearly demonstrated the need for concrete approval and concurrence from the sitting house. However, this is an unnecessary repetition of stage three above because of the number of processes, diversity of viewpoints which are likely to degenerate into conflicts and lack of harmony (Eagan, 2007). Selebalo (2014), PwC (2018) and Chigada and Kyobe (2018) all agree that this stage of the law-making process is a repetition that prolongs the enactment of the Bill into law.

In stage six, the law-making process is silent if the President of the Republic has room to reject or refer back the Bill to the NA. Despite being empowered by the Constitution of the Country to sign the Bill, the President should be empowered to reject or refer back the Bill if there are issues misaligned to the Constitution of the Republic. In practice the President, through advisors and legal minds, scrutinises each Bill before signing it into an Act. This is a fundamental weakness which has not been reflected in the law-making process.

In the last stage- Bill has been signed into Law/Act of Parliament, the researcher established that there is no feedback loop to the public to inform them that the Bill has now become law. The public has a vested interest in the legal system of the country, therefore communication on

Parliament-related matters might strengthen trust issues between political leaders and civil society.

3.4 Regulatory Environment in South Africa

The researcher also acknowledges that not all subsections are on specific pieces of legislation and the subsections referred to include 3.4.5, 3.4.6, 3.4.9 and 3.4.15 respectively. The Constitution of the Republic of South Africa governs and applies to all laws and conduct within the country. All laws are governed through Parliament by passing reform policies into law or Acts, while the NCOPs focuses on provincial legislative issues (Section 76 of the Constitution Act 108 of 1996) while the NA deals with Bills not related to provinces (Section 75 of the Constitution Act 108 of 1996), which are then considered in the national sphere of government. Both the NCOPs and NA serve the people/society, public and private sector organisations, therefore, have a Constitution mandate to develop and present legal systems that work together towards the betterment of South Africa. There are various pieces of legislation (Electronic laws) enacted through Parliament, developed to focus on cybercrimes and other computer-mediated illegal activities (Chigada & Kyobe, 2018). Bote (2019) and Malatji *et al*. (2021) assert that there are more than thirty-seven pieces of legislation designed to address objectives of the national cybersecurity strategy. This demonstrates the magnitude of resources required to address the complex landscape of the country's legislation. In order to illustrate the multiplicity of these laws, how they are coordinated and what they are designed for, the following laws have been considered for discussion in this thesis. Their selection for discussion in the study is motivated by their provisions which are directly linked to cybercrimes. The discussion is not in any order of preference or importance.

3.4.1 Common Law

Claassen *et al*. (2012) define common law as the law applied to a group of people/society on the basis of their customs and legal precedents that have been developed over a period of time. Common law is derived from the Roman-Dutch law of the 17th and 18th centuries, thus, it forms the basis of modern South Africa law. For example, threat actors or online offenders committing cyber-bullying (cyber-harassment), child pornography etc should be arrested and successfully prosecuted. Hannah (2015) asserts that common law extends to the arrest and successful prosecution of offenders who defame others online, are in contempt of court or defeat the ends of justice. Smith *et al*. (2018) state that cyber-bullying involves online bullying

where attackers send electronic messages of an intimidating nature to another person (victim) using digital devices (smartphones, laptops, computers and tablets. Cyber-bullying and child pornography are common forms of online bullying in South Africa (PIRLS, 2017). In addition to online crimes, common law also includes crimes like robbery, bank card fraud, rape and murder. The major shortcomings of common law are that it can be overridden at any given time by legislation, because Parliament is superior and supreme law-making body, thus, common law is regarded as inferior (Parliament of South Africa, 2019).

However, common law has its limitations and narrows significantly when it is confronted with online crimes. For example, dealing with crimes of malicious damage to property, hand hacking or cracking or production and distribution of worms and Trojan horse viruses, common law has been found weak. In the case of *S v Howard,* the court upheld that the crime of malicious damage to property would apply to a person causing damage to an entire information system. The court used the analogy of malicious damage to property, the definition of damage to property of IT systems was applied. The major limitation of common law is the element of property which includes corporeal moveable or immovable, thus, being a limitation that hacking and cracking (computer crimes) do not entail corporeal property which has been damaged (Schultz, 2016). The weaknesses of common law have to be addressed by investigating if unauthorised access to computers and disruption of data and software applications can be adequately addressed by South African common law. If this intervention is not feasible, therefore, the courts would have to determine if a separate piece of legislation is required. Given the context of South African common law, many authors have interrogated and concluded that the country's common law has gaps and cannot adequately address cybercrimes (van der Merwe, 2016; van der Merwe, Roos, Pistorius, Elselen & Nel, 2016).

The weaknesses of common law are believed to be exacerbated by the perception that courts lack expertise about computer technology, cybersecurity experts are of the opinion that the courts would not be the best platform to develop policy on cyberlaws or resolve online crimes (van der Merwe, 2016). There is a great need to create new legislation so that South Africa can be able to prosecute offenders which is not feasible under common law.

3.4.2 The Electronic Communications and Transactions Act (ECTA)25 of 2002

Orji (2012) and Claassen *et al*. (2012) state that Chapter X111 of the ECTA 25 of 2002 addresses all forms of cybercrimes. Legal recognition of electronic transaction is provided by

the ECTA of 2002, but it prevents the abuse of information systems. In addition, Chapter X111 of the ECTA of 2002 empowers the Cyber Inspectors/Cyber Police to carry-out Cyber Inspections. The ECTA also provides for the development of a national e-strategy for the Republic, recognises the importance of the information society, promotes legal certainty and confidence in electronic communications and transactions and ensures a safe, secure and effective business environment exists for consumers, business and government to conduct and use electronic transactions (section 85). The electronic transactions environment should be conducive for the development of human resources and that the country's interests are not compromised through the use of electronic communications (ECTA 25 of 2002). In the context of the information society and advanced technological developments, most transactions are conducted electronically, thus, users of information systems are reminded to adhere to the dictates of the ECTA 25 of 2002 and other e-legislation. The researcher acknowledges that regulation of electronic communications is complex, thus, communications policy, legislation and regulation have to be continuously reviewed and developed.

Section 86 of the Act addresses unauthorised access to interception or interference with data. In section 86(1), a person who intentionally accesses or intercepts any data without authority to do so, is guilty of an offence. Section 86 (2) provides that a person who intentionally and without permission to do so, interferes with any data, which causes the modification of data, destroyed or rendered ineffective, is guilty of an offence. The ECT Act provisions (Section 87; Section 88) are explicit in terms of cybercrimes that should never be committed by any person and the penalties of such offences are provided in section 89 (1) or (2) as the case may be. For example, the case of *S v Douvenga* the court decided that Douvenga- General Manager of Rentmeester Assurance Limited contravened section 86(1) of the ECT Act. The court found Douvenga guilty of intentionally and without permission to do so, gained access to data which she knew was contained in a confidential database and sent this data by email to her fiancé. Douvenga was fined R1,000.00 fine or imprisonment for a period of three months (District Court of the Northern Transvaal, Pretoria, Case no 111/150/2003).

Provisions contained in Chapter 2 of Council of Europe's Convention on Cybercrime (CECC) (South Africa is a signatory to the CECC) are: (i) lay down common down definitions of criminal offences which allow harmonised legislation at national level; (ii) investigative powers better suited to the IT environment should be defined to bring into line criminal procedures between countries; and iii) determine both traditional and new types of international

cooperation (regional and global alignment of legislation) which help countries to rapidly arrange for investigations and prosecutions of cybercrimes. However, the ECT Act has given minimum compliance and is also lacking protocols of the CECC which other jurisdictions have made progressed significantly.

The complexity of criminalising cyber conduct is exacerbated by the fact that cybercrimes do not have borders and can be committed anywhere in the world. Threat actors need not be in South Africa when committing the offence. The challenge is the aspect of jurisdiction in that the laws are sometimes conflicting, especially when the cybercrime is committed in another country (Mahlobo, 2015; van der Merwe *et al*., 2016). South Africa as a developing country might not have specialised capabilities to address borderless nature of cybercrimes. The need for regional and international cooperation and alignment of national cyberlaws becomes pertinent to address the global nature of cybercrimes. However, some South African scholars and legal experts are calling for legislation that criminalises cybercrimes and with the enactment of the ECT Act, the law should change significantly. Though the ECT Act has made progress towards address cybercrimes, legal experts and authors believe that more should be done regarding the prosecution and penalties imposed on convicted cyber offenders (Mohan *et al.*,2020). Harsher consequences should be imposed to deter cyber criminals, because current penalties are not stringent enough. There have been promises in the ECT Act to improve specialised investigation of cybercrimes by creating cyber-inspectors and to date, this promise has not been fulfilled (van der Merwe, 2016; van der Merwe *et al.*, 2016).

3.4.3 Interception and Monitoring Prohibition Act (IMPA) 77 of 1995

This Act was the most important statutory provision regarding Interception and Monitoring before the RICA was enacted. The IMPA 77 of 1995 highlights that it is a criminal offence for any person to intentionally intercept, authorise or procure other people's communication without their knowledge and approval (Snail, 2009). The introduction of technology in the workplace has reconfigured business models and the way employees conduct their business. Given the emergence of the global COVID-19 pandemic, an employee's office is everywhere where there is internet connection and an internet-enable device. However, due to unacceptable user behaviour, corporates are constantly monitoring user activities on their network to identify vulnerabilities. The provisions of the Constitution of South Africa, 1996 guarantees an individual's right to privacy- an individual's privacy should not be infringed. This includes monitoring and interception of their emails, communication or information without their

knowledge. For example, in *Protea Technology v Wainer,* Protea Technology recorded an employee's telephonic conversations relating to the employer's affairs and the court rule in favour of the employee in that a person's right to privacy extends to situations in respect of which a legitimate expectation of privacy is harboured (Pistorius, 2009).

The IMPA was limited in its application especially criminalising cyber conduct. Cybercrime is constantly evolving and with new developments which cannot be addressed by IMPA. Cybercrimes are committed within and without the borders of South Africa. Some countries have moved to legal regulation of conduct on the cyberspace by criminalising certain forms of conduct globally (Schultz, 2016).

3.4.4 Financial Intelligence Centre Act (FICA) 38 of 2001

The FICA 38 of 2001 came into effect on 1 July 2003 as a result of the G7 summit of 1989 set-up the Financial Action Task Force (FATF) Banking Association of South Africa [BASA] (2018). The G7 economies were concerned about the effectiveness of local and international money laundering control structures. Thus, it became imperative to establish standards that promote effective implementation of legal, regulatory and operational measures to combat money laundering, financing of terrorist and other threats to the integrity of the international financial system (BASA, 2018). Given the context of the FATF, the FICA was enacted with a commitment from South Africa towards addressing money laundering, financing of terrorist activities and other related threats. This law compels financial institutions to obtain proof of identification documents (ID), proof of client's residential address which is less than three (3) months old and issued by a reputable authority. Therefore, original documents should be accessed to make copies and certify them as a true copy of the originals with a FICA endorsement. The government introduced the FICA and other applicable Anti Money Laundering and Countering of the Financing or Terrorism legislation as a direct response to acts of terrorism especially the September 11, 2001 attacks on the Twin Towers of the World Trade Centre.

3.4.5 King Code IV

The Institute of Directors South Africa [IODSA] (2018) states that the King Code IV is complete deviation of its predecessors. The first King Codes (I, II & III) were rules-based, whereas King Code IV is outcomes-based. That is, corporate governance in firms (public or private) should be concerned with leadership's ethical conduct, attitude, behaviour and

mindset. Deloitte (2020) postulates transparency and disclosures. Leadership should declare their interests or lifestyles so that when lifestyle audits are carried out, they are not found on the wrong side of law. Apart from general principles, Chapter 4, (principle 12) of **King Code IV** addresses IT governance issues where the board is required to operate, report IT security and policy issues within the auspices of Corporate Governance (COBIT) 4.1 and audit committees.

Despite the presence of a King Code IV in place, organisations grapple to deal with unacceptable human behaviour. Employees or management tend to study a system, identify its weaknesses and pounce on information infrastructure, and steal information and destabilise information systems. This is a form of planned behaviour that takes months or years to plan and intentionally engage in unethical actions (Letham, 2021).

3.4.6 SA National Cybersecurity Policy Framework

A number of interventions have been and continue to be implemented in the fight against cybercrimes resulting in the SA-NCPF. A National Cybersecurity strategy encompasses aspects of information, data, media services and technologies that can affect the security of the country's cyberspace (Government Gazette 39475, 2015). The SA-NCPF was designed to promote the establishment of the National Cybersecurity Advisory Council (NCAC) which oversees the implementation of national cybersecurity strategies and National Computer Security Incident Response Team (CSRIT). Cyberspace is brewing a lot of challenges for governments; therefore, an appropriate National Security strategy is paramount. National Cybersecurity strategy should appraise the vulnerability of south Africa's information infrastructure. One approach is to provide a legal framework to enhance public awareness against cyber-attacks, garner international and institutional co-operation as well as develop Cybersecurity training and development programmes.

The state has the mandate to implement a government-led coherent and integrated Cybersecurity approach which ensure that the country develops a cybersecurity culture and demand compliance with security standards. With this approach, partnerships between private and public sector enterprises should established because development of a national cybersecurity intervention strategy is everyone's responsibility (Khan *et al*, 2020). The WHO (2020) states that with the emergence of the global COVID-19 pandemic, countries have an added responsibility to protect National Critical Information Infrastructure (NCII). Given the

exponential growth rate of cybercrimes and threats between 2019 and 2021, a National Cybersecurity approach should be augmented by an effective judiciary system. Law enforcement agencies have a Constitutional mandate to investigate, arrest and hand over offenders to courts for prosecution, in order to deter or address cybercrime.

Chigada and Kyobe (2018) concur with Mahlobo (2015) that there are various fragmented pieces of legislation, some with overlapping mandates and poorly coordinated by different government agencies. Suffice to say that South Africa does not have an aligned legal and regulatory framework, complicates the mandate and perceived effectiveness of the National Cybersecurity approach. Thus, the purpose of the NCPF is obliterated with incoherent and fragmented legislation and poor coordination. Government has made a passionate plea to civil society, public and private sector to work together to achieve alignment of the legal and regulatory framework to address cybercrimes (Government Gazette 39475, 2015).

In order to become effective, the NCPF should have capacity to respond to Cybersecurity imperatives and work with the Justice Crime Prevention and Security Cluster (JCPS) and other government departments (for example, State Security Agency [SSA]) as well as obtain resources to support its endeavours. Appropriate consultations between the JCPS departments to share information and knowledge should be enhanced. Chigada and Ngulube (2015) posit that information and knowledge sharing are paramount to diffuse the silo mentality that permeates many organisations. When information and knowledge are shared, a better-informed Cybersecurity Response Team would proactively prepare for any cyber-threats and attacks.

3.4.7 Protection of Personal Information Act 4 (POPI) of 2013

The South African privacy law, explicitly known as the Protection of Personal Information Act, 2013 (POPI Act), came into effect on 01 July 2020. The Act fosters the security of private information by public and private organisations and sets provisions for legally processing personal data of both natural and juristic entities such as companies, living people, and trusts. The POPI Act also regulates the flow of personal information in and outside the borders of South Africa and any matters related to that information must be reported to authorities. For example, personal information as defined in section 1 of the POPI Act includes but not limited to; voice recordings, criminal records, financial records, biometric information of a person, and employment data (Protection of Personal Information Act (POPI Act), 2013).

The perceived effects of the POPIA could not be quantified at the time of conducting this study because it came into effect in July 2021, when the country was experiencing a hard lock down. Though, there was a national lockdown, this did not affect people or companies from communicating using telecommunication devices or access to personal information. For example, the POPIA is expected to fundamentally change how businesses outsource their technology operations. Section 19 of the POPI Act provides standards in respect of the implementation of security safeguards. Currently, some organisations outsource their IT operations oblivious of the exposure of people's information to third parties. The POPI Act legislates the creation and maintenance of a risk register that helps with the identification of potential risks that affect the processing of personal information in firms. Section 19 of the Act compels firms to conduct regular reviews, updates and verifications of identified risks by taking appropriate measures.

Section 21 of the POPI Act provides that firms must establish and maintain the security measures referred to in section 19. In the event that the outsource service provider believes that personal information has been breached and illegally acquired, the firm must be notified immediately. Firms should obtain a greater understanding of their IT environment because non-compliance with the provisions of the POPI Act attracts damages, claims and fine of up to R10 million (S (21) POPI Act, 2013).

3.4.8 Regulation of Interception of Communications and Provision of Communications (RICA)

Section 36 of South African Constitutions states that any fundamental right can be limited by means of a law of general application. Therefore, RICA is an Act of general application, which allows the provisions of section 36 of the Constitution. RICA allows the surveillance and monitoring of communications, however, civil society has raised concerns about law of this nature. With reference to sophisticated cybercrimes and terrorist attacks etc, RICA is necessary for South Africa.

RICA was enacted to make South Africa a safer country, by helping law enforcement agencies to identify and monitor users of mobile phones, their activities and track any suspicious criminal activities (Schultz, 2016; van der Merwe *et al.,* 2016). Though the primary focus of RICA is to assist law-enforcement agencies in the acquisition of crime-related information to mitigate crime, the Act also regulates interception and monitoring in the private sphere.

RICA has a wider jurisdiction than the IMPA, because of its applicability to the private sphere, prohibition of interception or authorisation of an interception of any communication in the course of its transmission (van der Merwe, 2016). In section 2 of RICA, no persona may intentionally intercept or attempt to intercept or authorise any other person to intercept or attempt to intercept at any place in the Republic of South Africa, any communication in the course of its occurrence. Van der Merwe (2016) defines communication in the context of RICA to include direct and indirect communication.

Section 1 of RICA defines indirect communication as the transfer of information (message or any part of a message) whether in the form of a speech, music or other sounds; data, text, visual images, signals, radio frequency spectrum; or in any form or combination of forms that is transmitted in whole or in part by means of a postal service of telecommunication system. 'Indirect communication' includes telephone calls, internet, facsimile facilities, private and personal email messages, trackers in company cars, Short Message Services (SMS) and voicemail messages. When users download information from internet sites, send/receive email messages, are considered 'indirect communication'. This takes the form of information transmission (data, text, visual images) through telecommunication systems (RICA 70 of 2002). Importantly, the concept of 'indirect communication' must be read in with section 1(2)(a) which clearly states that interception of communication takes places in the Republic if and only if, the interception is affected by conduct within the Republic. Section 86 of RICA pertaining to penalties, one can observe similarities between the RICA and ECT Act. Thus, with that relationship, there was reason to develop new legislation to address the issue.

It is noted that RICA was the first piece of legislation to address aspects of cyberlaws which could not be addressed by common law. RICA recognised laws that needed to be implemented to criminalise cyber conduct, however, due to sophisticated cybercrimes, RICA is found wanting because the constant developments of cybercrimes are a cause for concern for the global economy (WHO, 2020).

3.4.9 Privacy and Surveillance in South Africa

Overreliance on ICTs, money laundering to fund terrorism, child pornography and gender-based violence have given rise to many governments to implement surveillance technologies to curb the challenges (MacKinnon, 2011). The enactment of the POPI Act of 2013 was a way of addressing businesses and individuals from exposing personal information of people without

their consent. From 1 July 2021, the POPI Act became effective, but this does not deter would be cybercriminals from illegally accessing personal and company information for criminal activities and financial gains. Though the POPI Act prohibits sharing of information, individuals and groups of people can easily collect and manipulate information which is not directly linked to a legitimate party (section 1, POPI Act of 2013).

The South African government is aware that existing legislation is not adequate to address unacceptable user behaviour, therefore, certain individuals' behaviours and movements are monitored under surveillance processes to ensure that national security is not compromised (State Security Agency, 2015). For example, in Eswatini (Formerly Swaziland), the government has shut down Internet services to stops its citizens from communicating with the rest of the world of the extent of protests and how the country's infrastructure has been damaged. In 2021, in Uganda during the country's Presidential elections, the Internet was also shut down. In many instances, in politically volatile economies, surveillance programmes are evoked to monitor people's movements and activities. Repressive regimes control what people can and cannot see. For example, the People's Republic of China uses heavy firewalls to control its citizens and what they watch on the internet (Liu, Nikitas & Parkinson, 2021).

Therefore, it is ludicrous to even think about mobilising citizens through the Internet for policy change or organise any protests. Government would know and proactively crash any events. By creating the 50 Cent Party, where people comment and get paid for each blog they post, the objective by China is to limit democratic freedom whilst manipulating online conversations. These tactics consolidated oppressive regimes to remain in power and instil fear in their people (MacKinnon, 2011). Kirchgaessner *et al*. (2021) established that authoritarian regimes use Pegasus spyware to secretly record phone calls, extract messages and download photos without the cellphone user's knowledge. There are reports that during the African National Congress' elective congress of 2017, some politicians' cellphones were bugged or hacked without their knowledge (Daily Maverick, 2019). These acts of cellphone bugging by state agencies or government should be sanctioned in line with the Constitution of the country. If done outside the parameters of legislation, this poses challenges for the country's legislation towards the drive of addressing cybercrimes.

3.4.10 Broadband Infraco Act 33 of 2007

This Act was passed into law in December 2007 focusing on how shares are transferred, management of loan accounts, liabilities and guarantees in Broadband Infraco (Propriety) Limited from Eskom Holdings. Broadband Infraco (Pty) Ltd is a government owned enterprise mandated to improve telecommunications infrastructure in rural areas to enable access to electronic communications. In the process of infrastructure development, Broadband Infraco (Pty) Ltd would acquire land and other resources in its quest to expand network, therefore, the company requires power to expropriate land or rights, borrowing powers and issue guarantees or security in order to achieve its mandate (Broadband Infraco Act 33 of 2007, s (5)). The main issue of concern with the Broadband Infraco Act is the expropriation of land which might be abused through corrupt means; therefore, government has made a clear indication of how it can be exonerated in a court of law. The argument is the improvement of telecommunications infrastructure in under-developed areas.

3.4.11 Consumer Protection Act 68 of 2008

Legacy systems created by the apartheid regime have left an indelible mark of poverty, inequality, illiteracy and other socio-economic challenges. For example, recent protests actions that resulted in massive looting and destruction of shops and other infrastructure in Gauteng and KwaZulu-Natal in July 2021 are premised on a number of factors that include socio-economic challenges and differences in political ideologies. The Consumer Protection Act was developed to promote fairness in terms of access and a sustainable marketplace for consumers' products and services. There are incidents of service providers or manufactures who abuse or exploit consumers in the marketplace. Credit providers should desist from reckless lending. That is, after assessing a consumer's affordability, the credit provider should be open and transparent if the client can afford the credit. In some instances, some credit providers proceed to lend even if the customer does not afford-result in reckless lending (National Regulator, 2021). With the advent of technological changes, patterns and agreements, consumer rights should be protected to ensure they accessible opportunities in the economy. Given the context of the newly introduced POPI Act 4 of 2013, consumers' information should be protected, and have a right to disclosure and information.

3.4.12 Copyright Act 98 of 1978

The Act stipulates that individuals' intellectual property should be protected against piracy. For example, literary, musical, artistic, sound recordings, broadcast works should not illegally used without written or expressed permission from the owner (Copyright Act 98, of 1978, C 1, s (2). Any infringement to the Act would constitute a criminal and prosecutable offence. Globally, artists- musicians and other businesses have been raising fundamental issues regarding pircacy of music or designs. People engaged in these types of crimes affect revenue generation streams for the individuals owning the legal right to the works. Cybercriminals infringe people's right by using digital technologies to perpetrate crime with the full knowledge that they would not be easily detected because of privacy policies. The judiciary can fail to effectively enforce copyrights or delineate allowable private use if there is no legislative response in the context of new digital technologies (Pistorius, 2009; van der Merwe, 2016).

3.4.13 Critical Infrastructure Protection Act (CIPA) 8 of 2019

The Act was assented into law on the 20th of November 2019 with the objective of guiding the country on how to protect, safeguard critical infrastructure. In section 20 (1) of the Act, critical infrastructure refers to any infrastructure of national significance and should be protected against terrorist and criminal syndicates. This infrastructure includes buildings, facilities, establishments, pipelines, transoceanic cables, satellite systems etc used for national development. This infrastructure should be secured through physical, personnel, contingency plans and others against threats, ensuring information pertaining to security measures remains private and coincidental. The penalties for breaching the Act vary in terms of severity of breaches.

3.4.14 Cybercrimes Bill of 2019 (waiting for assent by the President)

Bhagattjee and Govuza (2021) state that the Cybercrimes Bill is one step-away from becoming law. The Bill was passed by the National Council of Provinces and is thus waiting for the President to assent. The new Bill is a result of the old B6-2017 bill which previously focused on cybercrimes and cybersecurity sections. Major concerns with the Old Bill were the perceived violation of rights to freedom of expression entrenched in section 16 of the Constitution. With further consultations and debates, the clauses in the Old Bill were removed, leaving the proposed Bill to focus on cybercrimes which inolve all the crimes discussed in chapter two of this thesis. Of particular interest in the new Bill is malicious communication-

which entails distribution of false data, information with intention to commit crime. Furthermore, information spread with the intention of incite violance, causing damage to property and distribution of revenge porn are key provisions in this Bill. Events of the past few days where shops were looted, perceived dissemination of inflamatory and malicious information spread to incite violence would have been a defining moment for courts to test the effectiveness of the law.

Bhagattjee and Govuza (2021) state that penalities pertaining to malicious communications include, successfully prosecuted offenders would be liable to conviction of cybercrimes- fines or imprisonment ranging from five to ten years with serious offences attracting fifteen years. In the case of the offences of cyber fraud, cyber forgery and uttering, the Bill provides for broad penalties that could be imposed for anyone found guilty of any of these cybercrimes where a court will have a discretion to impose a penalty that it deems appropriate under section 276 of the Criminal Procedure Act 51 of 1977 (Bhagattjee & Govuza, 2021).

3.4.15 Cyber Warfare Strategy

This is part of the country's drive towards the development of an effective and coherent national cybersecurity strategy through the lens of the NCPF (Selabalo, 2014; Gcaza & von Solms, 2017). South Africa establish a hub to coordinate and serve as a central point of collaboration between academia, industry, civil society. Efforts are driven towards fighting all forms of cybercrimes because of the ever increasing cyber-attacks and threats. Von Solms (2018) agrees that the shortage of IT and legal skills in cybersecurity pose challenges for the country if it is achieve its cybersecurity objectives. The shortage of skills is also combined with lack of urgency to implement measures to address cybercrimes. After analysing the The Cyber Warfare Strategy and the NCPF, the researcher of this thesis concludes that both Acts have to be read together to obtian understanding of their provisions because they are interdependent.

3.4.16 Electronic Communications Act (ECA) 36 of 2005

The ECA was enacted on the 18th of April 2006 with a focus of promoting convergence in broadcasting as well as regulating broadcasting signal distribution and the telecommunications sectors. All electronic communication services, network services and the granting of broadcasting licences are provided for by the Act. This is designed to ensure that government has a proper record and accountability of players in the telecommunications and broadcasting

industries. The ECA 36 of 2005 provides that subscribers can port their cellphones from one service provider to the other. ICASA (2020) states that telecommunications and braodcasting services are key areas of strategic national importance because if these sectors are not regulated, cybercriminals can pounce of the opportunities and broadcast information that leads to issurection and insurgency. It is pertinent for government to keep a close eye so that the country's security is not violated. In countries where there are reports of insurgency, banditry or terrorism (Nigeria, Mozambique, Somalia), if properly traced, the challenges emanate from weak electronic communications policies at governmental level (Chohan, 2020).

3.4.17 Independent Communications Authority of South Africa Act 13 of 2000

This Act came into effect on the 4th of May 2000 allowing the establishment of Independent Communications Authority of South Africa (ICASA). The establishment of ICASA paved way for the dissolution of the Independent Broadcasting Authority and the South African Regulatory Authority. Of paramount importance of the Act is its recognition of technological developments in broadcasting and telecommunications that cause rapid convergence of the two fields. People working in the telecommunications and broadcasting industries should be regulated to ensure fairness and diversity of views that represent the South Africa society (Section 92 of the Constitution). Notable achievements of ICASA have been the price warfare with service providers who were compelled to revise and reduce prices for data, cellphone costs etc in 2018. The researcher can conclude that ICASA is a government watchdog overseeing the activities of the broadcasting and telecommunications in the country.

3.4.18 National Archives and Records Service of South Africa Act 43 of 1996

The provisions of this Act are that national records should be properly archived and managed. This includes the preservation of national heritage. The disposal of records or data should be done within the auspices of law and upon approval. In the process of arching records, records management bodies can use electronic records systems for easier storage, retrieval and generation of information. Tampering or altering knowingly with an intention to commit crime is punishable with a fine or imprisonment according to the severity of the crime (Chuma & Ngoepe, 2021). Ngulube (2020) asserts that many people overlook the importance of archival and records management systems. The government places strategic importance to its heritage

as a means of sharing information and knowledge. Criminal elements can tamper with electronic records management systems in attempt to steal information for financial gains.

3.4.19 National Prosecutions Act 32 of 1998

The Department of Justice (2019) states that the NPA was developed to promote matters related to the establishment by the Constitution of the Republic, 1996 of a single national prosecuting authority. The Act provides power to institute and conduct criminal proceedings to any member of society who commits crime. All suspicious criminal activities shall be thoroughly investigated resulting in successful prosecution of offenders. This is an important point noted by this study, therefore, law enforcement agents are empowered to conduct their investigations to completion, to mitigate litigations from wrongful arrests.

3.4.20 Prevention of Organised Crime Act 38 of 1999

This Act existed before the FICA which was introduced in 2001.The Prevention of Organised Crime Act provides measures to mitigate money laundering, terrorist and criminal gang activities, racketeering etc. Anyone suspected or found to be engaged in such criminal activities is liable to imprisonment (Shaw, 2017; Johnson, 2017). South Africa has been struggling to combat Drugs and Drug Trafficking, human trafficking (StatsSA, 2020). Given the context of organised crime, the researcher can conclude that there are sophisticated syndicates involving law enforcement agencies, politicians, business executives and other influential people driving and funding these criminal activities. At law, all proceeds of crime should be punishable with hefty penalties of imprisonment.

3.4.21 Protection of Constitutional Democracy against Terrorism and Related Activities Act 33 of 2004

The country needs to put in place measures to prevent and combat terrorist and related activities. International cyberlaws on terrorism should be applied in a Sovereign State such as South Africa. The effectiveness of these laws should complement and align to existing legislation (United Nations Security Council, 2019). The September 11, 2001 Twin Towers attack in the US, is a good example where countries should continuously remind themselves that terrorists, use proceeds of criminal activities to fund their terrorist activities, therefore, appropriate punitive measures should be in place to deter-would-be terrorists (UN, 2019). South Africa is a signatory to a number of Conventions on cyber-terrorism such as the

International Convention on Suppression of Terrorist Bombings, which was adopted by the UN on 15 December 1997. From time to time the UN Security Council publishes a number of laws to help countries to fight against terrorism and other acts of banditry or insurgency.

3.4.22 Protection of State Information Bill

This replaced the Secrecy Bill. Legal experts such as van der Merwe (2016); van der Merwe *et al,* (2016); Johnson (2017) and Ncube (2019) contend that the Protection of State of Information Bill is a very controversial piece of legislation. The Bill was passed in November 2011 and then send to the President for assent. However, President Jacob Zuma refused to sign the Bill and referred it to the National Assembly for review because there are issues that were controversial such as the harsh penalties of up to 25 years in jail for leaking sensitive documents or information. Its provisions are the classification, protection and dissemination of information about the state.

3.4.23 Protection from Harassment Act 17 of 2011

The Act provides the protection against all forms of harassment, and victims of harassment should get fair reatment and appropriate remedies. The Act specifically addresses harassment of children and any person who alleges to have been subjected to harassment. The Department of Justice (2021) defines harassment as the act of instilling fear in another person. There are different forms of harassment that include sexual, emotional, physical etc. There have been several cases of sexual harassment in South Africa perpetrated by people in positions of authority while their victims were in vulnerable positions. In the contemporary information highway, perpetrators of harassment use social media, electronic communication tools to target their victims through following, accosting or engaging in verbal or electronic communication. Moyo (2021) states that cellphone spying constitutes a form of harassment in that it involves stalking of a person without one's knowledge. WhatsApp or any text messages with sexual inuendos, hand, eye signals (winking), inappropriate body language, touching another person

in a way construed to have negative connotation are viewed as forms of harassment (Department of Justice, 2021).

All the above pieces of legislation are disticnt from each other, designed to address a specific crime and coordinated by different government agent. Thus, posing serious coordination and alignment challenges.

3.5 Synthesis between the SA Regulatory Environment and multiple agencies

South Africa's Parliament follows a seven-step law-making process (See figure 3.1), which all require resources (human, technological, time, funding etc). The resources should be coordinated and managed appropriately to achieve the desired objectives such as the existing laws of the country. While the law-making process takes place, diverse stakeholders with vested interests participate in Parliamentary legislative debates (Van der Merwe, 2016). The major players are the Parliamentarians, policymakers (NCOPs, NA), politicians and the public. These diverse people interact to debate Bills and during these interactions, complex relationships are produced. Relationships could be formed in line with political ideologies, consensus or disagreements on their mis/understanding of the issue at hand. The Bills enacted into Acts of Parliament should be reviewed from time to time to ensure that they are effectively guiding the judiciary in terms of criminal procedures. With reference to the preceding discussion, at least twenty-three pieces of legislation were highlighted, thus, different agencies are mandated to coordinate them. The discussions also showed that the pieces of legislation focus on different aspects of cyberlaws and crime, creating incoherencies and fragmentation. However, courts, government agencies, policymakers and Parliament represent self-organising elements of that operate distinctly but converge on certain critical issues.

The question that one can pose is that "Are the different government agencies adequately resourced from an IT and legal cybersecurity skills perspective?". This is a fundamental question that brings the lack of IT and legal skills in cybersecurity into the limelight. When the law-making process takes place, the right IT and legal skills should be hired, consultations between the judiciary, policymakers, public and the regulatory environment should be a continuous process that never ends. Bote (2019) asserts that lack of the requisite skills,

knowledge and expertise can hinder government's vision into coherent and implementable policies that would help to align the NCPF.

From the information presented in Table 3.1 below, the author of this thesis, consulted a wide range of sources, studies and established issues fundamental to the development of an effective national cybersecurity strategy. A total of nine issues/variables were identified. This thesis observed that the issues raised by various scholars, are fundamental to the development of an effective NCPF. For example, the law-making process was cited as a key ingredient by most studies consulted. Thus, aligned to the GCSCC CMM dimension 4 which focuses on the Legal and Regulatory frameworks. The capacity to design and enact laws directly or indirectly relating to cybersecurity is important in the South African context. The law-making process should be less cumbersome, ensures that the laws are enforced, successful prosecution and capacities of courts and law enforcement agencies work coherently (GCSCC, 2021).

Table 3.1 : Issues fundamental to the development of an effective national cybersecurity strategy

Authority/study	Law making process	IT & legal skills in cybersecurity	Coordinating coherent e-legislation	User behaviour	Understanding of cybersecurity	A cybersecurity culture	Cybersecurity monitoring & controls	Coordinating Multiple global cyberlaws	Knowledge & information sharing
Selebalo (2014) Mahlobo (2015) Eagan (2007)	***x***		***x***		***x***		***x***	***x***	***x***
Claassen *et al.,* (2012) Parliament (2019)	***x***	***x***		***x***		***x***		***x***	
Chigada (2014) De (2016); Arewa (2018)		***x***		***x***		***x***			***x***
Hannah (2015) JCSE (2016)	***x***		***x***	***x***	***x***		***x***	***x***	***x***

NIST (2014)									
Smith et al (2018) Curtis (2011) GCSCC (2021) World Bank (2017)	***x***	***x***		***x***	***x***	***x***		***x***	
Selebalo (2014) PwC (2018) Chigada and Kyobe (2018)	***x***	***x***	***x***		***x***			***x***	***x***
Ahmed, Sharif, Kabir & Al-Maimani (2012) Colangelo (2016)	***x***			***x***		***x***			***x***
Eagan, 2007). Bote (2019); Malatji et al (2021)	***x***		***x***	***x***			***x***		***x***
Orji (2012) StatsSA (2019) ITU NCS (2019)		***x***			***x***		***x***		***x***

Kyobe *et al*. (2012); Ajumobi & Kyobe (2017)	***x***		***x***			***x***			***x***

3.6 Existing Gaps in IS Literature

This section discusses the existing gaps in the IS literature as postulated in Table 3.1 above and will be presented as follows:

3.6.1 General Coverage

Studies focusing on IS in developing countries, specifically in South Africa have not interrogated the extent to which the SA-NCPF has been aligned to national, let alone regional and global cyberlaws. The present study acknowledges that Kyobe (2010); van der Merwe (2016); Ajumobi and Kyobe (2017) have raised fundamental issues regarding the country's e-legislation, but have not focused on how these fundamental weaknesses would affect the development of the National Cybersecurity Strategy. In addition, some studies have ignored the law-making process and contributing factors to the poor coordination, fragmentation and misalignment of national legislation. Given the information presented in Table 3.1 above, different scholars have either focused on one or a few issues as fundamental to the development of an effective national cybersecurity strategy. The general coverage of past studies creates an opportunity for the present study to pool together the key issues into a research instrument to guide the thesis.

3.6.2 Interdisciplinarity of IS research

In the past, IS scholars have limited their studies to the effects of IT in organisations and have not engaged the IS as an interdisciplinarity research to widen theory development and knowledge sharing. In recent years, including this thesis, IS scholars are driving towards an interdisciplinarity approach to IS research to broaden the information and knowledge spectrum (ITU, 2019). With the emergence of the global COVID-19 pandemic, IT and legal cybersecurity experts have devised plans to work together to understand what constitute cybercrimes and the appropriate penalties can be imposed on prosecuted cybercriminals. These concerted efforts to address cybercrimes co-create opportunities for research collaborations (interdisciplinary).

3.6.3 Bivariate Relationship Assumptions

Past IS studies have not fully addressed the effects of cyberlaws on cybercrimes with a view to broaden IS research. Bivariate approaches assume linear relationships where one looks at the existing law against a crime, but does not consider complex interrelationships between IS, law-

making process and other factors. Table 3.1 above has summarised some of these key factors that interplay and interact forming configurations which cannot be understood from a human being perspective. The question to ask is "Does South Africa have an effective NCPF to guide the development of an effective National Cybersecurity Strategy?" Cybersecurity is paramount for the Republic to protect its information infrastructure. Thus, the present study builds on gaps identified in past studies so as to develop new knowledge, information and ideas that might be used by other IS scholars, practitioners and society.

3.7 Alignment of e-Legislation

Chigada and Kyobe (2018) state that studies by Lipton (2010) and Pokwana and Kyobe (2016) are closely related to the current studies but focused on compliance or non-compliance of legislation. A few studies that articulate misalignment, reveal three representations of misalignment of legislation through lack of Coherence; Interoperability and Harmonisation (Lipton, 2010; Pokwana & Kyobe, 2016). When organisational components operate in a synergistic and possess coherence, the end-goal is they become aligned to achieve competitive advantage (Hsiao & Omrod, 1998). Maes, Rijsenbrij, Truijens and Goedvolk (2000) define alignment as "a continuous conscious and coherent interrelation between all organisation components, human resources and IT to achieve specific objectives over time". In order to achieve an effective system, the interplays amongst the variables must be balanced over a sustained period of time. Globally, firms develop solutions to address complex organisational challenges through the lens of alignment (Portee & Siggelkow, 2008).

Schultz (2016) and van der Merwe *et al.* (2016) and other South African legal experts argue that different pieces of legislation do not adequately address cybercrimes and as such, the prosecution of cybercriminals is very low. In addition, criminals do not have to be in South Africa to commit the crime, but can be anywhere in the region, continent or world. Given the shortfalls of our national laws, it might be difficult for our courts to successfully prosecute cybercriminals because there are no specific provisions or sections that adequately align to national, regional or global cyberlaws. In addition, cybercrime is evolving at a fast pace, thus, South Africa's legislation has not moved to the legal regulation conduct by criminalising certain forms of cyber conduct globally (Schultz, 2016).

When closely looked at, South African common law, ECT Act, RICA, IMPA and other pieces of legislation have specific provisions and limitations on their implementation and application of cybercrimes. There being perceived poor coordination by different government with overlapping mandates, this shows how the country's laws operate in silos-lack of coherence. At national level, civil society, private and public sector institutions and courts should feel confident about the cyberlaws. Concerns have also been raised by legal experts about the penalties imposed on prosecutions. There is a perception that courts are lenient to cybercriminals because of lack of the courts' understanding of computer-mediated crimes.

3.8 The Concept of Effectiveness

Drucker (1987) defines effectiveness as doing the right things, whereas Nyarko (2014) defines effectiveness as the capability of producing the desired result. The intended outcome of the study is to produce a successful/aligned national cybersecurity policy framework. The researcher does not know which combination/patterns of interactions produce this desired outcome, therefore, the configuration approach will help to identify and measure that pattern/combination of constructs that provides effectiveness (Miller, 1987; Venkatraman, 1989). If the researcher can identify these constructs, their combined influences and determine their degree of coherence, the researcher should be able to tell how and when the study can achieve/align the national cybersecurity policy framework (Ventaktraman,1989). Coherent/aligned constructs help us to achieve a successful/effective national cybersecurity policy framework, attain optimum benefits and value from them as well as gain high performance. The various constructs would enable configurations to be fairly unique, tightly integrated and stable for a sustainable period of time (Ajumobi & Kyobe, 2017; Chigada & Kyobe, 2018). With reference to the perspective of alignment (Gestalts), the adequate level of alignment will be determined using cluster analysis to reveal the patterns and configurations of variables as well as their level of effectiveness. Those constructs that have attained alignment will have high level of effectiveness (Van de Ven & Robert, 1985; Ajumobi & Kyobe, 2017), while, in unlikely scenarios, it would be inferred that constructs not achieving coherence, have not attained alignment.

3.9 Chapter Summary

An overview of the law-making process was articulated and illustrated by discussing how Australia, UK, USA and South Africa managed their processes. It was revealed that all the four countries adopted a two legislative body strategy for the development and presentation of Bills. There were seven distinct steps followed in the South African process followed by a discussion of gaps that were identified. The chapter discussed the country's regulatory environment highlighting the objectives of each piece of legislation, also followed by a summary of gaps in literature review, law-making processes and weaknesses of the pieces of legislation., which resulted in the development of an integrative theoretical framework. Additional constructs were added to the original law-making process resulting in the integrative theoretical framework, a revised process of describing the country's law-making phases. The concept of alignment was discussed, supporting the motivation for adopting the Gestalts (Configuration Theory) for the study. Given the discussions presented in the integrative theoretical framework, a conceptual model with thirteen constructs was developed demonstrating how the interplay between constructs formed patterns or configurations of interest. Form a human perspective, it is difficult to understand the interplay between different constructs, therefore, cluster analysis would be used to tease out these configurations. The next chapter discusses the concept of alignment.

CHAPTER FOUR: THEORETICAL FRAMEWORKS

It is the framework which changes with each new technology and not just the picture within the frame (McLuhan, 2016)

4.1 Introduction

Chapter three discussed the law-making process, South African regulatory environment, an integrative theoretical framework that discussed concepts contributing to misalignment of national cyberlaws resulting in the development of a conceptual framework (Figure 3.3). The nexus of this chapter is to discuss the concept of alignment (Configuration/Alignment Theory) premised on the issues raised in the preceding chapter. A theoretical framework helps the research to immerse this study in the broader body of cybersecurity and information systems literature whilst uncovering pertinent issues of the research problem. It is important to set the study within the information systems security and cybersecurity scholarly discourses in order to provide a research operating tool to interpret research findings. Given the discussions pertaining to the integrative theoretical framework in chapter three, this chapter will focus on the Gestalts/Configuration theory because it is the main funnel which guided this study.

4.2 Role of Theoretical Frameworks

Various theoretical works were reviewed and assessed to determine their fit for purpose for the study. Chigada (2014:4) in Ngulube, Mathipa and Gumbo (2014) states that many quantitative research projects are theory-driven, with emphasis on testing or verifying what is already known rather than developing new theories. Ngulube *et al*. (2014) state that:

> *There is a dearth of explicating the notion of conceptual and theoretical frameworks in social and management sciences, due to the limited understanding of the development and conflation of the two terminologies. Some researchers do not fully understand the purpose of adopting either a theoretical or conceptual framework, thus, their studies are shallow because of the deficiency of understanding.*

In order to understand the coherences and interplays between constructs, the researcher used the Configurations Theory to introduce and describe the theory that explains the misalignment problem exists. Theoretical frameworks are imperative in quantitative research projects

because they help to test/verify what is already known rather than develop new theories (Ngulube, Mathipa & Gumbo, 2014). In this study, various organisational elements such as human resources, technology, strategy, vision, processes and financial resources are pooled together to achieve coherence over a sustained period of time for the organisation to attain competitive advantage and remain relevant to its market (Hsiao & Omrod, 1998). The coherence and synergistic approach of these elements leads to alignment. Therefore, the motivation of using a theoretical framework was to ensure that the study would test or verify if these elements achieved and what factors were behind their sustenance of alignment.

All phases of this thesis were driven by theories (Ngulube, 2014). As espoused by Ngulube *et al.* (2014), the research question for the current thesis was guided by theory, ultimately progressing to data collection, analysis and discussion. Babbie (2012) asserts that theory provides the researcher with a better understanding of the subject under investigation. For example, the concept of alignment of a National Cybersecurity Policy Framework is complex to understand, therefore, appropriate theoretical works were required to situate this study into a specific scholarly discourse in order to understand the research problem. Leedy and Omrod (2010) and Creswell and Plano Clark (2011) state that theoretical works help to limit the scope of relevant data by focusing on specific variables and defining the specific viewpoint that would be taken by the researcher in analysing and interpreting data gathered.

4.3 Theoretical works that shaped this Thesis

This study was shaped by a number of theories which include- **Resource-based theory** contends that possession of strategic resources provides an organisation with a golden opportunity to develop competitive advantage over its competitors (Barney,1991). Misalignment arises when an organisation's resources are not jointly exploited to achieve competitive advantage. In the Integrative Theoretical Framework, the researcher explained that lack of IT and legal skills in Cybersecurity is a major challenge confronting South Africa and other countries globally. This shortage of critical human resources is consequential to the law-making process and the country's efforts towards the development of a national cybersecurity strategy. **Organisational knowledge conversion theorists** Nonaka (1986) and Nonaka & Takeuchi (1995) posit that organisations can facilitate conducive environments for knowledge creation. Organisational knowledge creation exists when the knowledge created by individuals is made available, crystalised and is connected to an organisation's knowledge system

(Nonaka, 1986). Given the context of the South African law-making process described in the preceding chapter, the researcher highlighted that the public has limited access to media where Parliamentary issues are debated or published. Thus, with shorter window periods of time to give the public opportunities to make submissions, it is viewed as a deliberate strategy to exclude the public from participating in the law-making process (Selebalo, 2014). Therefore, individuals will not make meaningful contributions towards organisational knowledge creation. **Chaos** will arise because of the involvement of many departments, Portfolio Committees and further debates, resulting in interactions and conflicts (Marx, 1871) or disagreements regarding the Bills. Passing of Bills into Acts of Parliament can be delayed due to bickering and conflicts. With reference to the deliberative democracy school of thought in **political theory**, exclusion of civil society from the law-making process, is viewed as unfair and unreasonable, therefore, it creates conflicts and inconsistencies (Eagan, 2007).

Accountability theory focuses on the process of accountability (Lerner & Tetlock, 1999). Vance, Lowry and Eggett (2015) state that accountability theory explains how the perceived need to justify one's behaviours to another party causes one to consider and feel accountable for the process by which decisions and judgments have been reached. The President's actions will inform and determine the future of the country's laws (Colangelo, 2016) which is aptly explained by **structuration theory** that fosters informing the public about how to act, based around rules which are about the right and wrong way to do things (Giddens, 1984). IS research has widely used the structuration theory to understand the relationship between individuals and society (Jones & Karsten, 2008). The actions and behaviours of individuals in their organisations or country produce a social structure (**Theory of Planned Behaviour [TPB]).** People and businesses are embracing IT for various activities; thus, IT has played a major transformative role in people's lives. The TPB is widely used for predicting subjective norms and attitudes towards behavioural intention (Ajzen, 1985; 2006).

The ***NIST CSF*** provides guidance on how organisations should manage and reduce IT infrastructure security risks. These guidelines, practices and standards can be integrated to an organisation, security practices (NIST, 2019). Agrifiotis et al (2018) assert that organisations using NIST guidelines are able to respond and recover from cybersecurity incidents prompting them to analyse root causes and devise improvement interventions. The five core functions of the NIST CSF are Identify, Protect, Detect, Respond and Recover (Shen, 2014). *The GCSCC CMM (2021)* provides five dimensions namely i) cybersecurity policy and strategy; ii)

cybersecurity culture and society; iii) building cybersecurity knowledge and capabilities; iv) legal and regulatory frameworks; and v) standards and technologies. The main emphasis of the CMM model is for nations to evaluate their current cybersecurity capacity and maturity levels. Dutton, Creese, Shillair and Bada (2019) posit that capacity building requires attention across sectors, thus, more resources should be made available if the country has to build its national cybersecurity capacity.

The ***ITU NCS*** toolkit was developed with the assistance of the GCSCC, World Bank and other global institutions with a goal of providing guidelines to nations to obtain a better understanding of NCS vis-à-vis strategy development, building capabilities, nations can evaluate their current position in cybersecurity lifecycle management. Lastly, this thesis tapped into the provisions of the ***World Bank Cybercrime Toolkit,*** whose provisions are aligned to the ITU NCS and the GCSCC CMM that is, capacity building for emerging economies. Most importantly, this toolkit underscores the importance of nations to develop their national cybersecurity frameworks which should coherently and cohesively interoperate with international frameworks. The author of this thesis underscores the words "coherently and cohesively" because they resonate with the aim of study- measuring and aligning influencing factors to achieved an effective SA-NCPF.

4.4 The Concept of Alignment

Maes *et al.* (2000) define alignment as "a continuous conscious and coherent interrelation between all organisational components, human resources and Information Technology (IT) to achieve specific objectives over time". In order to achieve an adequate level of coherence, the influencing factors must be balanced over a sustained period of time to yield the desirable outcomes (Maes *et al.,* 2000). Levy, Powell and Yetton (2001) define alignment as a combination of "synergy between strategy, organisation, technology and human resources in order to sustain the quality of interdependence to achieve competitive advantage". Chigada and Kyobe (2018) synthesise different definitions of alignment presented above into, "alignment as the sustained synergy and coherence attained by different organisational components to achieve an effective system overtime. This definition by Chigada and Kyobe (2018) will be used throughout this study because it captures fundamental issues that resonate with the present thesis because it captures key variables from various definitions. The effectiveness and relevance of an organisation are determined by the performance of the different organisational

elements, how they are aligned to produce results in a very difficult business environment (Middleton & Harper, 2004). Thus, firms use alignment or strategic fit to identify problems and develop appropriate solutions for all problems in the firm (Camponovo & Pigneur, 2004).

Many scholars use terms such as “fit”, “balance”, “coordination”, “linkage” or “harmony” as reference to alignment (Maes *et al.,* 2000). With reference to the synthesized definition above, these terms refer to the same concept- alignment. Miller and Friesen (1977); Venkatraman (1989) posit that organisations can achieve success if all organisational components are in harmony or coherent. Venkatraman (1989) states that alignment can be measured through six perspectives, which are discussed in the next subsection.

4.4.1 Fit Perspectives Topology in Strategy Research

The six (6) perspectives of alignment are shown in Figure 4.1 below and these are fit as Moderation, Mediation, Matching, Profile Deviation, Covariation and Gestalts (Venkatraman, 1989).

4.4.1.1 Fit as Moderation

The concept of fit as moderation defines the relationship between two or more variables that predict an outcome. For example, the relationship between availability of internet-based resources (Laptop, tablet) and data to allow the student to attend online/virtual classes. The interaction between the predictor and criterion variables depends on the moderator (Venkatraman, 1989). In an organisational set-up, the interaction between organisational strategy (predictor variable) and performance (dependent variable) is moderated by the organisational structure (moderator variable).

4.4.1.2 Fit as Mediation

This has similar traits as the fit as Moderation in the relationship between two or more variables (antecedent and consequent) where a mediator (third variable) exists to produce an effect on both variables (Venkatraman, 1989). A mediator (service provider-MTN, Vodacom, Cell C) provides data to university staff members and students to enable them to connect to the internet and access online learning, research and training materials. During the period of conducting this Doctoral Research Project, the student was a beneficiary of data from the UCT. Though fit

as mediation and moderation can be used simultaneously, managers are cautious about the overlap and how they can easily mislead judgment.

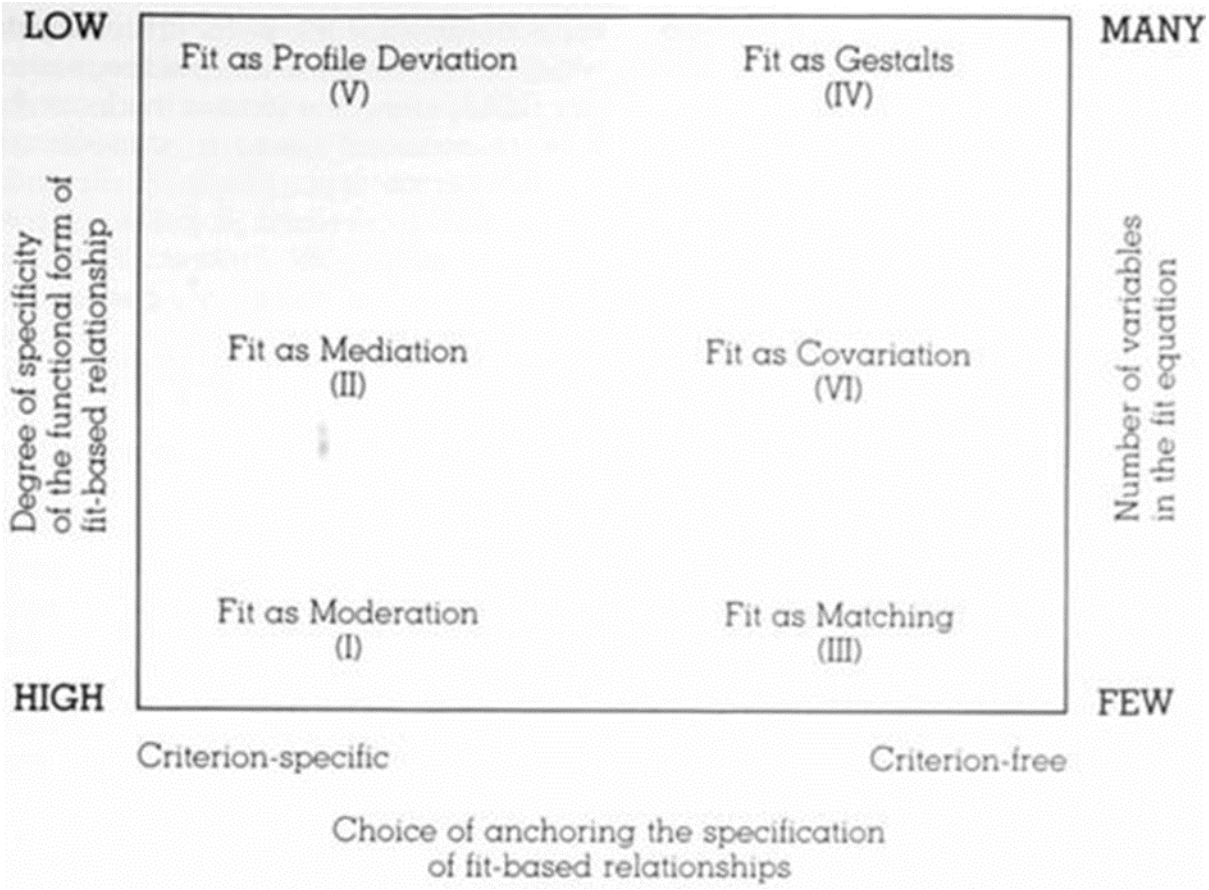

Figure 4.1: A Classificatory Framework for Mapping the Six Perspectives of Fit in Strategy Research (Venkatraman,1989)

4.4.1.3 Fit as Matching

This entails the match between two related variables (Miller, 1987). This perspective is different from fit as mediation and moderation because it does not involve a reference criterion. It is possible to estimate the effect of fit between two variables. For example, a criterion variable such as organisational performance is not referred to, management can estimate the effects of fit between two variables. Grinyer, Yasai-Ardekani and Al-Bazzaz (1980) assert that in order to develop fit relationship in a matching perspective, the theoretical proposition would be the most appropriate method.

4.4.1.4 Fit as Profile Deviation

This is defined as the degree to which a firm adheres to external variables (Venkatraman & Prescott, 1990). For example, a firm's strategy may be designed and applicable to a specific

situation, but during the course of execution, some unlikely changes occur, thus, the strategy should be flexible to fit change. However, the results from deviation are always below the expected performance levels. Venkatraman (1989) posits that adherence of a business unity to the environment can produce two scenarios: a) when the level of environment-strategy co-alignment is high, a positive performance is achieved and b) when the level of strategy co-alignment is low (deviation) the performance is negative.

4.4.1.5 Fit as Co-variation

Factor analysis is used to model Fit as Co-variation. Alignment can be viewed as a pattern of internal consistency among a set of variables related to a common objective (Venkatraman, 1989). Venkatraman (1989) notes that:

> *"If a business-unit strategy in a particular context is best represented as the pattern of consistent, concurrent resource allocations to the areas of research and development, design, manufacturing, and marketing, any one area is insufficient for an effective strategy, which requires consistent attention to all areas"* (p. 435).

Venkatraman (1989) posits that all four-dimensional areas of the business unit should be specified if the organisation is to achieve fit as Covariation.

4.4.1.6 Fit as Gestalts

Venkatraman (1989) defines Gestalts as configurations or patterns of organisational elements, constructs or variables that have attained adequate level of coherence, fit or unity with one another over a sustained period of time. Therefore, fit as Gestalts involves more than two variables. Jung (1971) postulates that "Gestalts" has its origins in psychology and it is a German word that has a shared meaning with "a pattern", constellation or configuration. Gould and Kolb (1964) define a configuration as an "organised entity or whole which the parts, though distinguishable, are interdependent; they have certain characteristics produced by their inclusion in the whole and the whole has some characteristics belonging to none of the parts" (p.234).

Gould and Kolb (1964); Drazin and van de Ven (1985) and Venkatraman (1989) emphasize that Gestalts are different from the characteristics of its individual parts in the fit relationship. Gestalts are different from the other approaches to fit relationships discussed above, in that

Gestalts view individual interactions between pairs of constructs only as a part of the overall pattern. Miller (1991) a strategic alignment theorist, claims that there exists complex Gestalts among strategy, environmental and organisational constructs and these Gestalts are relatively few and unique from each other in terms of relationships among variables.

As espoused by Miller (1991) that configurations are expected to be tightly interdependent and their significance is best understood by referring to the whole than to individual parts. Thus, researchers should not look at a few variables or linear associations among such variables, but should try to find frequently recurring clusters of Gestalts (Miller, 1991:5). Drazin and van de Ven (1985) succinctly emphasize the notion of configurational equifinality of Gestalts.

This study adopted the Gestalt perspective to analyse social change and human perceptions. Gestalts principles of closure and pragnanz (law of entire configuration) are imperative to understand the process of social change (Hartmann, 1946). Whilst closure is the effect of suggesting a visual connection between sets of elements, which do not necessarily touch each other in a composition. Given the understanding of the principle of entire configuration (pragnanz), people tend to separate whole figures from their backgrounds based on one or more variables. However, Behrens (1984), Hsiao and Chou (2006) state that in complex situations, several things are noticed as people look from one to another, they become an entire figure in turn.

By adopting the Gestalts perspectives, Wilkinson (1970) and Daniels (2004) posit that multiple forces are considered to influence human perceptions leading to individuals to experience their environments in meaningful patterns. Therefore, Gestalts cannot be separated from the environment in which they appear. Perceptions represent people's experiences or viewpoints about something of concern. Perrin and McFarland (2011) assert that opinion research aims to establish shared people's mental representation about issues of public concern, which are believed to exist in the environment where society shares information and ideas about public matters. For example, the researcher indicated that both the NCOPs and NA develop and present Bills to Portfolio Committees which then publish these Bills in Government Gazette for public comments. These platforms are designed to generate debates, inputs, suggestions and solutions to Bills which will affect civil society, public and private sector companies. When the public has limited access to media and Parliamentary information, the perception is that government deliberately excludes them from participating in matters of public concern

(Koehler, 1992). In their study of human perceptions of home page design, Hsia and Chou (2006) used Gestalts perspective and observed that perception concerning home page design was attributed to the quality of content, graphics, text and language used.

Given the importance of the six perspectives of alignment discussed above, it was not easy and a clear-cut exercise to choose the Gestalts perspective (Venkatraman, 1989). The researcher borrowed some important guidelines from other scholars to identify which perspective was more appropriate and relevant to this thesis. The selection of fit was guided by the specific fit variables supported by theories in this IS field (Venkatraman, 1989). For example, there are situations were two concepts are involved, matching, moderation and mediation fit perspectives can be considered (Venkatraman, 1989:440). Whereas, situations or studies that involve more than two variables, Profile Deviation, Covariation and Gestalts could be considered (Venkatraman, 1989). When there is an ideal profile to match with the findings is available, the ideal fit perspectives would be Profile Deviation and Covariation. In this study, the researcher was confronted with a scenario where there was no ideal profile, thus, the Gestalts fit perspective was decided upon because it does not require an ideal profile match. There is no prior knowledge of how exactly the variables would be grouped, thus, the study was exploratory in nature, the Gestalts was appropriate for this thesis and it was aptly supported by the Cluster analysis technique discussed in chapter 5 and 6). By adopting the Gestalts, the researcher was cognisant that the fit perspective should be aligned to the research objectives (Venkatraman, 1989).

To achieve the objectives of alignment, the SA-NCPF has to align to national, regional and global cyberlaws. Yoon (2019) states that once a state has developed appropriate legal framework for addressing cybercrime, international cooperation is necessary to expand national territorially-based purview in order to build effective networks for interoperability tha can function coherently and cohesively. The author of this thesis has illustrated the complex and reciprocal nature of interplays and interactions between different elements to be aligned (See Figure 4.2). Chigada and Kyobe (2018) assert that at the point at which various constructs interplay or converge, there is continuous interaction that produces different combinations or patterns that measure the degree of mis/alignment. However, these interactions are not visible or conceivable from a human perspective, but should be teased out to ascertain which patterns achieve coherence over a sustained period of time. If these elements are aligned (coherence among them), an effective National Cybersecurity Policy Framework would be achieved. The

stronger the coherence among the elements, the greater would be the role of the NCPF. If the coherence is weak (that is, misalignment of elements) then the NCPF would be ineffective. Therefore, the SA NCPF, should build effective networks of interoperability so that its deployment can function coherently and cohesively with regional and international legal frameworks (World Bank, 2017; Yoon, 2019). Borders serve no hindrance to cybercriminals and with time zones often helping to cloak their illegal activities from immediate notice, effectively combating cybercrimes requires an internationally-tasked, active response network that integrates international law enforcement agencies. For the networks to operate effectively, national-point people must understand their own legal and policy framework; how domestic arrangements intersect and interact with the larger global systems function (Yoon, 2019).

4.5 Proposed Conceptual Model

The aim of this study is to measure and align influencing factors to achieve an effective NCPF in South Africa. The Gestalts fit perspective of alignment was used and the integrative theoretical framework were used to develop the conceptual framework. A recap, the integrative theoretical framework brought together different theories to give a better understanding of the law-making process in South Africa. While the Gestalts view individual interactions between pairs of constructs only as a part of the overall pattern (Miller, 1991). Therefore, the author of this thesis knew the influencing factors, but was more interested in the degree of coherence among the influencing factors (Venkatraman, 1989), which converge in the oval shape. The influencing factors represent elements that interact at organisational level, producing relationships that are complex to be understood by linear relationships. Johnson and Vaidya (2019) describe linear relationships as a relation between two distinct variables. For example, *x* and *y* in the form of a straight line on a graph. The value of *y* is derived through the value of *x*, in a linear equation (relationship), which reflects their correlation.

As shown in Figure 4.2 below, nine (9) elements are the configurational variables, while the tenth (10) combined influence and the eleventh (11) effective NCPF are outcomes of the interplays of the nine configurational variables. The influencing factors, in the proposed conceptual model are: i) ***Understanding of cybersecurity***, ii) ***A cybersecurity culture***, iii) ***Cybersecurity monitoring and controls***, iv) ***Coherent e-legislation***, v) ***IT and legal skills in cybersecurity***, vi) ***law-making process***, vii) ***user behaviour,*** viii) ***knowledge and information sharing*** and ix) ***coordination of legislation through multiple government agencies***. At the

centre of Figure 4.2 is the oval shape where the nine influencing factors converge continuously. The eleventh construct in the proposed conceptual model relates to an aligned NCPF which is the goal of this study.

The proposed conceptual model will help the author to measure the degree of influence by teasing out the configurations between the influencing factors. The oval shape of the circle represents a continuous interplay of influencing factors without an end to that interplay (e.g. the circle symbolises a pot where various ingredients are poured in and then a person stirs the ingredients continuously) (Chigada & Kyobe, 2018). The identified influencing factors in the conceptual model, converge and interact in the oval shape, thus, combinations formed inside the circle create a combined influence desirable to achieve coherence among the interacting elements. The various combinations arising from interplay (combined influence) are hidden inside the circle. If we identify these factors, their combined influences and determine the degree to which they are coherent/aligned, we should be able to tell how and when we can achieve a better/aligned National Cybersecurity Policy Framework (Venkatraman, 1989). This degree of alignment will be determined by using cluster analysis which will reveal the patterns and configurations in the NCPF. Thus, measures to overcome issues are those which would result in stronger alignment, and coherence amongst the influencing factors would further enhance the level of alignment of the SA-NCPF. If the degree of coherence is weak (elements are misaligned or not balanced), then the pieces of cyber legislation will be ineffective (Miller, 1987).

The interplay between the influencing factors is continuous forming complex relationships, it is difficult to measure the degree of influence of each factor, hence the need to look at and measure the relationships as Gestalts. Given the complexity of interplay between the factors, it is impossible to achieve alignment using the linear approach if the matching, moderation, co-variation and mediation alignment perspectives are considered, therefore, the study adopts the configuration theory to help us tease out the combinations which would achieve alignment of the national cybersecurity policy framework (Ajumobi & Kyobe, 2017:7).

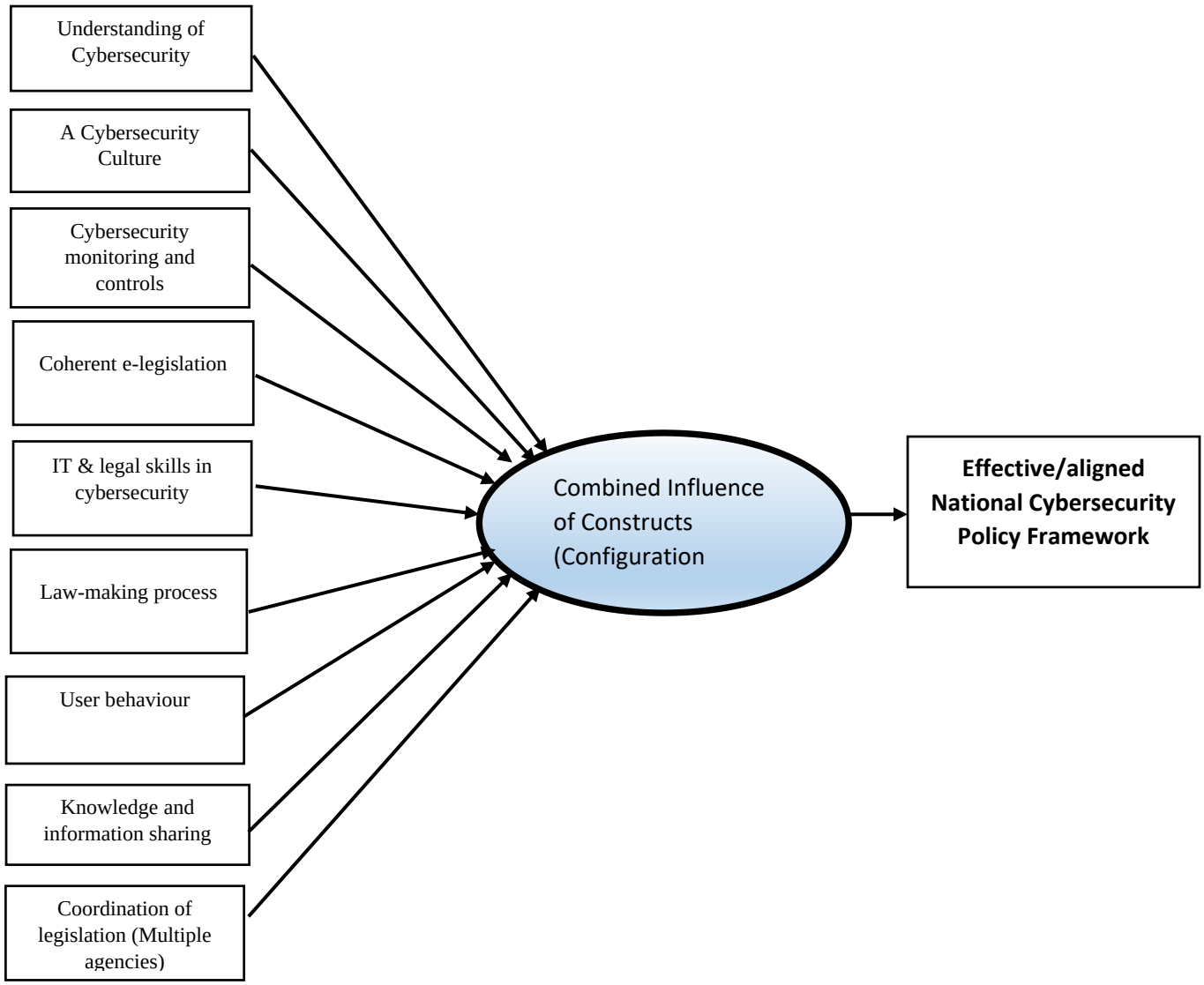

Figure 4.2 Conceptual Model of Alignment: (Author, 2021)

If, on the other hand, there is a weak coherence, then alignment will be ineffective, these constructs would have played a limited role in addressing misalignment challenges. The researcher therefore, proposes that:

- **P1:** The stronger the coherence among the influencing factors the more aligned the South African Cybersecurity Framework; and
- **P2:** The more coherent the South African National Cybersecurity Framework is perceived, the greater would be the degree of alignment of the country's Cybersecurity framework to national, regional and global cyberlaws.

The level of coherence can be determined by measuring the public's perceptions. In this study, respondents' perceptions regarding the effectiveness of the SA-NCPF may vary because of the multiplicity of factors at hand. Consistent with the Gestalts theory, there could be different groups of respondents with similar perceptions. Therefore, the researcher proposes that:

- **P3:** Groups of respondents that perceive strong coherence among the elements will also perceive effectiveness of the SA-NCPF.

4.5.1 Elements in the Proposed Conceptual Model

This section presents discussions of these influencing factors and their relationships to augment the preceding discussion (section 4.5.1 above).

i) Understanding of Cybersecurity

Bote (2019) states that civil society, private and public sector companies devise interventions to fight cybercrimes. There is no single theory that can capture cybercrimes, thus, creating challenges for people to understand cybersecurity. As pointed out by White (2020) that cybercrime is committed by different agents in different forms and at unexpected times. Many things happen during the commission of cybercrimes; therefore, confusion and chaos arises hindering rapid responses when threat actors engage in nefarious acts (Canhoto, 2010). There are many facets that contribute to lack of understanding of cybersecurity and these include lack of information and knowledge sharing platforms. For example, Parliamentary debates on Bills related to cybersecurity should provide platforms for public engagements and consultations. De Villiers (2001) asserts that the South African society has limited access to legislative debates, let alone, the media used to communicate with the public might be inaccessible to members of society.

People are confronted with conflicting and ambiguous interpretations and understanding of cybercrime, therefore, might not articulate what cybersecurity is all about. Shwab (2019) and Khan et al., (2020) posit that there is vast amount of information shared on social networking platforms, complex electronic crimes and lack of education and awareness programmes contribute to the misunderstanding of cybersecurity. Some institutions such as public funded universities offer modules in cybersecurity or information systems security, but, ironically, staff members or service providers at these institutions do not understand cybersecurity. It could be that people are engrossed in the academic project whilst overlooking the severity of

risks their IT infrastructure are exposed to. For example, a phishing email purported to be from the SARS was generated by the IT department and circulated to the university community requesting people to open a link and update their banking credentials. Many people fell prey to this hoax email, until the IT department sent out a communication email advising people that that was a phishing email. This demonstrates the extent to which people act subconsciously, exposing their personal information to phishing emails. With proper education and awareness programmes, the university community would have quickly identified that this was a phishing email and that the SARS logo was missing and the wording of the message was suspicious.

There is a possibility that large corporations might not have adequate interventions in place because these institutions only focus on cybercrimes specific to their industries. Therefore, collecting and analysing cybercrime data alien to their industries creates a barricade for understanding a holistic perspective of cybersecurity. Authorities in the financial industry may not understand or pay heed to other cybercrimes that are irrelevant to their industries, therefore, the process of detecting such cybercrimes may be complicated (SABRIC, 2019). For example, prevalent cybercrimes in the financial industry could be identity theft, money laundering, bank card fraud or internet fraud, thus, financial institutions may ignore and not pay attention to other forms of cybercrime. Threat actors study these trends, behaviours and strike unprepared sectors. In schools, school management authorities might focus on cyber-bullying, whilst threat actors might devise tactics and sexually abuse learners through explicit online pornographic material.

In order to improve the understanding of cybersecurity, sectors such as the financial and banking, establish bodies that gather, collate and disseminate information to their members as a way of imparting knowledge and information (BankServ South Africa, 2020). People should have access to a central information and knowledge repository to understand the depth and effects of cybercrimes. Lack of understanding of cybercrime and its consequences is exposing the government, civil society, private and public sector organisations to cybersecurity risks and losses (Kyobe *et al*., 2012). Awareness of what cybercrime represents, prepares government departments and civil society to respond rapidly to cyber-attacks and threats. Understanding of cybercrime should be everyone's responsibility. The more the nation's citizens are aware of cybercrimes, the higher the chances of preparedness to combat cybercrime.

ii) A Cybersecurity Culture

There is a debate as to what cybersecurity culture is. Gzaca and von Solms (2017) define cybersecurity culture as an ill-defined problem that lacks widely accepted key concepts that delimit the culture. Gcaza and von Solms (2017) and Maja *et al.* (2021) argue that a study that looks at cybersecurity culture alone is still in its infancy, but it would also need to outline how the culture can be cultivated. Boucher, Gundu and Maronga (2019) acknowledge that cybersecurity cultural issues are best addressed through a combination of human and technological aspects. There are eight critical success factors that should be embraced if an organisation aims to cultivate a cybersecurity culture and these are (a)-embracing cultural change and diversity, (b)-the commitment by top management, (c)-improving cyber attitudes of employees, (d)- administering diversity management initiatives, (e)-promoting awareness and training, (f)-enforcing information security policies (ISPs), (g)-introducing accountability and (h)- monitoring and evaluating cybersecurity culture (Boucher *et al.*, 2019).

The absence of a cybersecurity culture could be attributable to employee ignorance or lack of awareness, no prior experiences of cyber-attacks, little focus on redressing human-domain unacceptable behaviour (Boucher et al., 2019). Other issues include lack of executive buy-in, failure to adhere to changing cybersecurity policies and procedures and absence of a cybersecurity culture (Wout, 2019). Thus, employees study the weaknesses of their cybersecurity governance policies and systems before they engage in unacceptable behaviour. Gaumer, *et al*. (2016) detail how hackers have not only become skilled in the technical aspects of cybersecurity but also at exploiting human frailties. Hackers no longer hesitate to interact with their human targets through phishing, vishing or in extreme cases through real meetings in order to build trust and manipulate their victim's behaviour.

Keman and Pearlson (2019) state that most attacks and threats are perpetrated by employees who are privy to the weaknesses of the organisation's systems. Organisations that do not have effective cybersecurity cultures, policies or using legacy systems, are vulnerable because new technologies are not compatible with outdated systems, thus, are easily exposed. The cultural view around cybersecurity in an organisation plays a huge role in the effectiveness of the security controls put in place and the inclination of employees to adhere to these controls. Herath and Rao (2009) pointed out that employee's cybersecurity behaviours are influenced by their peer behaviour as either intrinsic or extrinsic motivators.

With reference to the importance and perceived effects of cybersecurity culture in the organisation, the absence of a national cybersecurity culture can be consequential to the economy especially in the era where cybercrimes are rising exponentially (Mahlobo, 2015). The development of the NCPF is help the country develop a sense of ownership, responsibility and accountability among civil society, public and private sector institutions, which should result in a national cybersecurity culture (Orji, 2012). Organisations would get motivated to build effective cybersecurity cultures if there is a national cybersecurity culture, but in the absence of such, enforcement of policies might be met with resistance or unacceptable behaviour (Keman & Pearlson, 2019). There are continuous interactions between Cybersecurity culture, development of the NCS and acceptable user behaviour. However, these interactions are not conceivable from a human perspective, but should be teased out to ascertain which patterns achieve coherence over a sustained period of time (Chigada & Kyobe, 2018).

iii) Cybersecurity Monitoring and Control

The United Nations International Crime and Justice Research Institute (2019) states that information assets (data and information systems) must be protected from security threats and attacks. Therefore, South Africa and South African companies and individuals should design, implement and maintain information security programs. The country requires safeguards or countermeasures to protect the information assets so that they meet appropriate security requirements (NIST, 2020). The protection of information involves the application of a comprehensive set of security controls that address cyber security (i.e., computer security), physical security, and personnel security. It also involves protecting infrastructure resources upon which information security systems rely (e.g., electrical power, telecommunications, environmental controls).

Thus, the application of security controls should be the nucleus of an information security management system (ISMS). An organisation or country is guided by a facility's information security plans and associated policies in the selection and application of specific security controls. If incorrect or inappropriate security controls and applications are implemented, information assets would be exposed to threats and data breaches. In addition, management should be cognisant that not all facilities can afford outright purchase of expensive security controls and related systems, however, strategic decisions should be made to balance the security risks and resources constraints.

In instances where the resources are constrained, South Africa should invest in security controls that provide the greatest overall risk reduction in line with the available resources. In Chapter 2, the researcher highlighted some of the security and technical controls as risk assessment, risk response, risk monitoring, security control implementation, incident response, monitoring and auditing and awareness and training. Given the complexity of cyber-attacks and threats, the researcher believes that security controls should be implemented in line with the type and severity of the risk. In some instances, two or more security controls might be implemented based on risk levels and resource constraint. Johnson (2017), ITU (2019) and Khan *et al*. (2020) assert that these security controls should be monitored and controlled to ensure they are appropriately used and maintained. Given the scarcity of IT and legal skills in Cybersecurity, fast-paced technological developments and incoherent legislation, South Africa might lack the capacity to monitor and control national information technology infrastructure.

Deloitte (2020) states that firms or countries fail to implement monitoring and controls because of lack of forward thinking that cyber-attacks and threats can spontaneously occur and affect the information assets. The belief that installing intelligent systems in the organisation with the hope that they will monitor and control information security protocols is a fallacy, therefore, the Chief Information Security Officer should augment these systems with human interventions through planning, daily monitoring, security management plans. Some intelligent systems might lack full visibility across the network, thus, creating windows of opportunity for attacks. Early warning signs might be missed or ignored, resulting in catastrophic data breaches.

iv) Coherent e-Legislation

Bote (2019) and Malatji *et al*. (2019) acknowledge that laws flow from different sources and with a multiplication of sources, the idea of a coherent and unitary system is disturbed. Thus, this leads to incoherent and fragmented pieces of legislation, a pertinent point that has been repeated several times by Mahlobo (2015), that South African laws are fragmented and lack synergy. Incoherence and fragmentation of legislation has been a subject of discussion in a wide of fields. The increasing globalisation, overreliance on ICTs and exponential rise of cybercrimes lead to more fragmentation because of the emergence of autonomised and specialised spheres of social action (Smits, 2010). There is no one general national or international law, but a myriad of specialised legal systems (as discussed in Chapter 3).

Incoherent and fragmented legislation directly affect the development of the NCS, coordination of these pieces of legislation ultimately affecting the country's NCPF. If the laws are fragmented, it means that diverse views and approaches are adopted which might create chaos in the development of the NCS. In addition, people with diverse backgrounds and understanding are likely to interpret the law in their own ways which might contradict the overall national objectives of addressing cybersecurity. Furthermore, fragmented laws fail to consider developments in other legislations and areas.

Schultz (2016) states that the development and enactment of the RICA was a result of the weaknesses of the IMPA due the latter's failure to address offences committed through computers. The development of the RICA did not necessarily address all the limitations of the IMPA because RICA had its shortfalls which required Parliament to enact Bills into law. Sutherland (2017) and Johnson (2017) posit that a huge factor that contributes to fragmentation of legislation is the lack of IT and legal skills in Cybersecurity and a silo mentality where information and knowledge are not shared for fear of exposing intellectual property. Incoherent and fragmented laws could be attributed to poor coordination by different agencies with overlapping mandates and in that coordination process, there is no sharing of information or strategies. The ripple effect is that poor coordination of legislation leads to fragmentation and incoherence which will ultimately affect the NCS. The combined influence of poor coordination on fragmented and incoherent legislation has on the NCS is not understandable from a human perspective (Miller, 1987).

Given the context of the South African NCS, there is lack of harmonised principles (legislation) which are coordinated by multiple government agencies, South Africa is unlikely to achieve its objectives of aligning the NCPF if this incoherence persists and if the security risks are not properly balanced with comprehensive cybersecurity strategies (ITU, 2019). If the country's NCS is fraught with inconsistencies, it would be difficult to describe the steps, programmes and initiatives undertaken to protect South Africa' cyber-infrastructure, increase its security and resilience. The number of cyber-attacks and threats reported in Chapter 2 and factors contributing to incoherencies (Chapter 3) all point to the fact that South Africa might still be battling to establish an effective NCS. Schultz (2016) and Malatji *et al.* (2021) indicate that existing cyber-laws have limited capabilities to successfully prosecute offenders of cyber misconduct. Therefore, these limitations contribute to the incoherence of an NCS (Mahlobo, 2015; Chigada & Kyobe, 2018; ITU, 2019). The researcher believes that a coherent NCS is

paramount to the identification and prioritisation of investments and resources towards cybersecurity. In addition, the NCS should provide an opportunity to align cybersecurity priorities with other ICT-related objectives (Bote, 2019). The NCS should translate government's vision into coherent and implementable policies that will help the country to achieve its objectives.

v) IT and Legal Skills in Cybersecurity

The growing reliance on digital government services, increasing ubiquity of social networks and the exponential growth of threats from foreign powers, terrorism and cybercrime, are contributing significantly to governments' attention towards cybersecurity (Sutherland, 2017). With a myriad of these challenges, governments are required to create legal frameworks and agencies to protect data and offer advice to citizens and businesses, plus ensuring sufficient supply of skilled technicians and engineers. Despite the presence of many colleges and universities and high levels of unemployment, South Africa has a shortage of ICT skills let alone in cybersecurity for a long time (StatsSA, 2020). There are number of factors contributing the shortage of IT and legal skills in Cybersecurity which include lack of a national ICT planning process that engages industry, educational institutions and providers of continuing professional development (CPD).

Many South African schools lack equipment and teachers trained in computer science and ICT, compounded by pupils with no access to computers or broadband access at home (Johnson, 2017; Shaw, 2017). Kirlidog, Van der Vyver, Zeeman and Coetzee (2016) and Shaw and Thomas (2016) state that the small and medium enterprises (SMEs) have limited budgets and capacities to develop ICT skills, yet these entrepreneurial ventures are incubators of innovation and knowledge hubs. Information security is a leading issue for many organisations where the shortage of skills is severe (Schofield, 2016). The researcher acknowledges that cybersecurity presents particular problems where the shortage of skilled individuals impedes the development of an effective NCS, defence and security sectors, banking and finance, in critical national infrastructure and other sectors. The health sector is another vulnerable sector due to Big Data and sensitive of information that is much sought after by cybercriminals (WHO, 2020; Khan *et al*., 2020; Chigada & Madzinga, 2021).

With the implementation of the POPI Act, all firms are required to bolster their cybersecurity efforts with specific focus to hiring of Cybersecurity experts. This entails hiring additional

staff, CPD, training and development (Sutherland, 2017) and attracting the right Cybersecurity skills by paying them good salaries and rewarding competitive incentives. The views presented here buttress the researcher's beliefs that lack of IT and legal skills in Cybersecurity are a cause for concern. These individuals would contribute significantly to the law-making process, development of a National Cybersecurity Strategy because of their understanding of technological and legal developments.

With reference to rapid technological developments, shortage of cybersecurity skills in IT and legal disciplines, organisations fight for these scarce resources, thus, in some instances their projects are scuppered because of unavailability of critical human resources (PwC, 2018; StatsSA, 2019). Having to keep abreast with a fast-paced technological environment would require retraining of people, reconfiguration of business models, whilst focusing on mitigating cyber-attacks and threats. This ultimately affects the financial and time resources that are urgently required so that organisation does not lose track of cybercrimes. Whilst technological innovations are welcome in the information society, there are challenges that should be addressed at both company and national level to ensure the focus remains on the development of an effective national cybersecurity strategy.

Disruptive technologies are upcoming innovations that have an effect of transforming how organisations work and communicate, rapidly displacing and disrupting existing business models (Khan *et al.*,2020). New technologies are disrupting the status quo, forcing organisations to reconfigure cybersecurity cultures, employees' behaviour, and attitudes. With the adoption of new technologies, management and employees have to rebuild a new set of cybersecurity norms and value systems (Da Veiga & Eloff, 2010). Applying old cybersecurity practices to new technologies might be outdated because the security protocols may be too complex and difficult to address prevailing conditions. Given the context in which calls for ICT uptake are growing, there is the challenge for firms to keep abreast with security requirements for these new systems. The first challenge is to train and develop their human capital to hone cybersecurity skills and the second challenge is to match the accelerated pace of technological innovations.

vi) Law-Making Process

The researcher indicated that the South African law-making process is similar to that of the Australia, UK and USA. All the processes are slow, time-consuming, thus, prolong the

enactment of Bills into law or Acts of Parliament (Selebalo, 2014). There are two legislative bodies responsible for developing and presenting Bills to Parliament. When Bills are presented to Portfolio Committees, the objective is to allow these Committees to have an oversight of the law-making process (Parliament of South Africa, 2020). Each government department is represented with a portfolio committee. For example, the Copyright Amendment Bill (CAB) was referred back to Parliament by President Ramaphosa because it did not pass the constitutional muster and may be vulnerable to constitutional challenge (Daniels, 2021). Various pressure groups such as disability activists, performers and creatives would be justified to express dismay at the NA's Trade and Industry Portfolio Committee's deliberations on the long-awaited CAB. The CAB was referred back to Parliament for review more than a year ago and to date, there is no progress in the Bill. This is a clear demonstration of how slow and time-consuming the law-making process is in South Africa and it is a setback for pressure groups to their hopes of having the Bill signed into law (Daniels, 2021).

However, given the context of the political situation in the country and in line with the Constitution of the Republic of South Africa, different political parties should be represented in these portfolio committees with the objective of taking an oversight and accountability role to determine if government departments deliver on what they promise and whether they spend taxpayers' money responsibly (Bateman, 2013). When there are multiple political party representations, interactions in these Portfolio Committees can give rise to disagreements and conflicts or differences in opinions. Considerable amount of time and other resources are spent, derailing progress in the law processes. Lack of IT and legal skills, duplication of roles and responsibilities by the NCOPs and NA, multiple regional and global cyberlaws and intention to address sophisticated cybercrimes result in complex relationships that affect the law-making process in South Africa as well as the development of an effective NCS. The law-making process in South Africa is a complex structure of different self-organising elements that tend to organise some stability without any external control, which has been explained by Chaos theory (See figure 3.1).

With a myriad of cybercrimes prevalent in cyberspace, existing e-legislation might not be at par with the level of sophistication of cybercriminal activities. This might entail a closer analysis of each cybercrime and develop an Act of Parliament that specifically addresses that crime. Given the context of the law-making process, time and other resources required, developing appropriate legislation might be a futile exercise. By the time a new piece of

legislation is enacted, cybercriminals might have been more advanced in their nefarious activities (Khan *et al.*, 2020; Chigada & Madzinga, 2021).

vii) User Behaviour

Unacceptable human behaviour is at the forefront of cyber-attacks, threats and information systems security. In addition to unacceptable behaviour, ineffective cybersecurity governance policies and the absence of awareness contribute significantly to users' unethical conduct (Chigada, 2020). The lure of financial gains from illegal access to information and information assets has created demand for cyber-criminals to devise sophisticated ways of studying an organisation's information systems security protocols and pouncing on defective practices in order to gain access to information for personal gains (WHO, 2020). Working from remote locations due to unforeseen circumstances and the global Corona Virus (COVID-19) pandemic, firms are placing greater emphasis on human intelligence than ever before. Over-reliance on human intelligence might result in firms overlooking that individual ethical behaviour creates windows of opportunities to engage in unacceptable and criminal practices that expose an organisation to cyber-attacks, threats and information systems vulnerabilities (World Economic Forum, 2020). Ahmed *et al.* (2012) and WHO (2020) attribute most cyber-attacks to human error, unacceptable human behaviour and the abandonment of the security policies that mitigate cyber threats and attacks.

Abukari and Bankas (2020) state that organisations lose information assets through unethical and unacceptable employee behaviour. Passing or sharing of log-in credentials, personal devices or trade secrets expose the organisation to criminal activities. For example, the use of BYODs allows employees to use multiple Internet-enabled devices such as smartphones, tablets, laptops, smart-watches to connect to an organisation's network, which, in some instances, are shared with friends and relatives oblivious to the fact that these devices have sensitive log-in credentials (Frost & Sullivan, 2016). Other examples where unacceptable behaviour exposed an organisation's information assets include the 2020 data breach of Experian, the world's largest credit bureau, where information for 24 million South Africans and close to 800 000 businesses' information was leaked by an employee (SABRIC, 2020). In January 2021, Absa was exposed to data breaches perpetrated by one of its employees who exposed customers' details to external parties. More than 209 000 customers' credentials were shared with cybercriminals for personal financial gain (Malinga, 2021).

User-behavioural intention to act is not build overnight but it is a calculated process where a person identifies and studies a weak process and system before acting to commit an unethical action (Malinga, 2021). There is a strong relationship between developing a cybersecurity culture and people's behaviour in an organisation or country as a whole and multiple global cyberlaws and various pieces of legislation. Governance structures and the legislative framework were developed to rein in wayward and unethical conduct- for individuals and businesses in South Africa (Abukari & Bankas, 2020). However, human beings cannot understand which of the elements (cybersecurity culture, user behaviour and multiple global cyberlaws) has more influence than the other. These elements interact with each other over a sustained period of time and that interaction requires a Gestalts to understand their combined influence on the NCS and NCPF.

viii) Knowledge and Information Sharing (Silo approach)

Silo approaches develop when people fail to share information, insights or knowledge about an event or something of substance. Lack of understanding of Cybersecurity is a very good example where information can be withheld from the public. Mahlobo (2015) and Malatji et al (2021) state that different government departments mandated to coordinate the various pieces of legislation might be faced with a similar challenge- silo approach. These institutions are bound by the Secrecy Bill which aims to regulate the classification, protection and dissemination of State Information (Schultz, 2017). Therefore, the agencies might not be at liberty to share their intellectual property with other elements, thus, they are self-organising elements (Bonnici, 2015).

In a study by de Villiers (2001), it was established that civil society had limited access to contribute to Parliamentary debates. This was compounded by the types of media used by government to communicate and share information, which, in this instance were newspapers, government gazettes that were beyond the reach of many people in South Africa. Claassen et al. (2012), Selebalo (2014) and Parliament of South Africa (2019) acknowledge that the public has limited access to the media where Parliamentary debates are published, thus, the public views this as an exclusion strategy from participating in the law-making process. Upon realisation of this shortfall, the PSP commissioned the Political Information Service of the Institute of Democracy in South Africa (IDASA) to undertake research regarding public participation in legislative and policy making process in South Africa (IDASA, 2018). Section 118 of the Constitution, stipulates that the Parliamentary Support Programme (PSP) should

facilitate public participation in Parliament and provincial Legislatures (de Villiers, 2001). The PSP is a financing agreement signed between the South African Speakers' Forum and the European Union in November 1996. The objective is to ensure good governance and a stable democracy which strengthen the role of Parliament and all the provincial legislatures. In addition to fulfilling functions of policy formulation, facilitation of constituency work, the PSP has a mandate to engage in public participation and education. Legislatures should facilitate and enable the active involvement of civil society in the law-making process which include promotion of access of the public to the legislature buildings, Constituency Offices, Committee meetings and Public Hearings (Constitution 108 of 1996, s (118)).

Given this mandate, the Promotion of the legislature should take place in both rural and urban areas, specifically giving attention to vulnerable members of society (women, youth, disabled and poor communities). Using appropriate strategies and mechanisms, the PSP should be able to educate, communicate, arrange community events, public hearings, special Parliament, advertise and media coverage. The objective is to increase civil society's capacity to serve their constituencies, promote a better understanding of the legislative process, foster a participatory form of communication, transparency and participation in the legislative process (Selebalo, 2014). Van der Merwe et al. (2016), Schultz (2016) and van der Merwe (2016) all agree that the objectives of the PSP are noble and for a good cause. The importance of public participation in the law-making process should not be overlooked because these laws affect the well-being of civil society, private and public sector entities.

The researcher posits that disjoints between Parliament or law-makers and the public create disharmony and mistrust because of the perception of deliberate exclusion from the legislative processes. In addition, civil society would remain in the dark regarding laws that pertain to cybersecurity or any criminal activities perpetrated on the computer. It would be a mammoth task to create an effective NCS let alone a cybersecurity culture because of the perceived exclusion of the public from law-making processes (Gzaca & von Solms, 2017; Boucher, Gundu & Maronga, 2019). Given the public's limited access to Parliamentary debates and legislative process, this affects the level of knowledge and understanding among society on how to react to certain crimes when perpetrated in their communities.

A silo approach occurs when Parliament fails to provide feedback to the public after all inputs and debates have been concluded and the Bill is an Act of Parliament. Citizens have a

Constitutional right to know if their inputs were considered (Bateman, 2013; Schultz, 2016). There is a dearth of information that articulates how Parliamentary legislative debates or enactments are shared with the public. Thus, the public has the perception that government strategically excludes them from the legislative processes, yet these laws affect their well-being (Selebalo, 2014).

Limited access to information leads lack of knowledge and understanding of legislative issues, therefore, even the feedback is provided, the public would not be adequately prepared to comment on issues already debated. When people are educated and adequately informed, their state of readiness and/or awareness improves, resulting in a society that is empowered and ready to fight cybercrimes. Involving society and other stakeholders informs how people behave and develop a cybersecurity culture (Knowles, 2016; Keman & Pearlson, 2019; Wout, 2019).

ix) Coordination of legislation through multiple agencies/systems

Peters (2018) acknowledges that policy coordination is an old challenge for many governments. Candel and Biesbroek (2016) state that policies influence one another in order to produce synergy or reduce conflicts. Lindblom (1965:154) defines coordination as a "set of decisions made in one program or organisation consider decisions made in others and attempt to avoid conflict". Coordination problems arise because of a number of factors such as existence of gaps in the mandate/coverage or redundancy of the programs. Strategic coordination helps government agencies or departments to improve broad strategic goals. Thus, coordination seeks to harmonise efforts across the whole organisation, reduce duplications, contradictions, displacements, changing demands, specialisation, improve accountability and cross-cutting problems (Peters, 2018).

Given the context of coordination described above, Mahlobo (2015) admits that various state agencies mandated to coordinate different pieces of legislation, do so in a disorderly manner. While, Pokwana and Kyobe (2016) assert that South African e-legislation is fragmented and inconsistent resulting in misalignment with regional and global cyberlaws. Atoum *et al.* (2014) state that when the country's laws are misaligned and inconsistent, they perpetuate national, regional and global cybersecurity challenges. A country might not develop and implement an effective cybersecurity policy framework with a high level of inconsistence in its legislation. One of the key arguments for undertaking this study is the acknowledgement by Mahlobo

(2015) former Minister of State Security in South Africa that our cyberlaws were poorly coordinated and that causes a big challenge to the country's cybersecurity protection strategy. Different government departments/agencies have overlapping mandates, which, in most instances create confusion for the judiciary (Mahlobo, 2015). When traits of poor coordination manifest, the likely probability of misinterpreting and application of the laws are very high.

Gumbi (2018) points out that after analysing South Africa's cyber laws and policy framework, the results point to an outdated legislation and in desperate need of revision. Schultz (2016) and van der Merwe *et al.* (2016) coordination should promote collaboration if the country is to achieve a coherent NCS. Poor coordination diffuses the opportunity of interactions and information sharing among the actors (Chigada, 2014). Mandating different government agencies, sometimes with little expertise, knowledge or resources exacerbates poor coordination, which will ultimately lead to different ideas and interpretation of government's goals. Malatji *et al.* (2021) posit that poor coordination demonstrates that different government agencies do not reach the basic agreement on the Cybersecurity problem and perhaps the means of addressing the problem and then a more effective policy may emerge. Addressing poor coordination can be time-consuming and difficult because of the deeply embedded ideas about policy that should be reconciled across multiple agencies.

Selebalo (2014); Colangelo (2016) and Schultz (2016) all state that cybersecurity is a shared responsibility which requires coordinated action for prevention, preparation, response and incident recovery on the part of government authorities, civil society and private sector. This would require a comprehensive legal framework or strategy developed through a multi-stakeholder approach – National Cybersecurity Strategy (NCS). The NCS should be premised on an aggregated and harmonised set of principles and good practices (ITU, 2019). Other elements that might contribute to poor coordination of legislation could be the lack of IT and legal skills in Cybersecurity, rapid technological developments and complex global cyberlaws.

x) Multiplicity of Global Cyberlaws

There is a rapid technological development rate that is driven by the desire to improve business transactions and standard of living for human beings. However, with rapid technological developments is the challenge of rising and sophisticated cybercrimes that confront governments globally. Cybersecurity has become a topical issue globally especially its exponential rise during the emergence of the global COVID-19 pandemic (WHO, 2020; United

Nations [UN], 2020). South Africa has written the NCPF to guide the country's Cybersecurity protection strategy (NCS). However, Freedman (2016) and McLeod (2016) assert that the development of the NCPF has not been thoroughly planned in terms of its implementation. The diffusion of policy elements and ideas from Europe, USA and Asia has exposed the weaknesses of the SA-NCPF. There is little evidence of these global cyberlaws having been adapted to South African national circumstances, especially the absence of any public assessment of the risks or of the potential impact of the proposed measures, or consideration of the ability to implement (Freedman, 2016; Schultz, 2016). Compounding this perception of failure to adapt global cyberlaws into the SA-NCPF, is government's failure to publish its analyses of the responses to its drafts of law and policy, raising questions about how effectively it makes use of such material and pointing to a serious weakness in governance.

The complexity of emerging cybercrimes requires governments to develop new legislation in tandem with cybercrimes. Thus, a new crop of Cybersecurity IT and legal skills is required. This poses challenges for developing countries like South Africa that does not have adequate IT and Legal skills in Cybersecurity, thus, the implementation of the NCS and NCPF might be jeopardised. Furthermore, the law-making process in South Africa is slow and the drive to align national legislation with international cyberlaws might not be achieved as required by all stakeholders (Freedman, 2016; van der Merwe, 2016). The pace at which technology is evolving is a huge challenge for global cyberlaws because in trying to keep abreast with new cybercrimes, multiple laws will be developed in the process, thus, create more confusion to many countries that might be struggling to develop and enact one piece of legislation.

Given this narrative, there is an interaction between multiple global cyberlaws, rapid technological developments, shortage of IT and Legal skills in Cybersecurity, slow law-making processes, sophisticated cybercrimes, incoherent and fragmented legislation that is poorly coordinated by agencies with overlapping mandates. As pointed out by Ajumobi and Kyobe (2017) and Chigada and Kyobe (2018) that the interaction between organisational elements is continuous and the degree of influence cannot be understood from a human perspective, thus, the interactions between these elements would be best understood through a Configuration approach. The researcher does and would not know which of these elements influence or are influenced by which one.

4.6 Chapter Summary

The concept of alignment and the six perspectives (moderation, mediation, matching, profile deviation, co-variation and Gestalts), effectiveness and the conceptual model were discussed in the present chapter. The chapter discussed the interplay between influencing factors (See Figure 4.2) the proposed conceptual model. There are nine influencing factors converging in the oval shape, thus, interact with each other forming interplays. The oval shape postulates a pot where different ingredients are poured then one continuously mixes them, forming complex relationships. In the oval shape, shown in Figure 4.2, the interplay between influencing factors is difficult to measure the degree of influence of each element, therefore, the need to look at and measure the relationships as Gestalts. The chapter also describes the influencing factors and their relationships. The next chapter presents the research plan and procedures that were adopted to gather, analyse, interpret and use research data.

PART III
RESEARCH DESIGN & PRESENTATION AND DISCUSSION OF FINDINGS
CHAPTER FIVE: RESEARCH DESIGN AND METHODOLOGY

5.1 Introduction

This chapter describes the research methodology. The chapter provides an overview of Information Systems field, thereafter, the rest of the discussion in this chapter is guided by the research methodology map shown in Figure 5.1 below. At the apex of Figure 5.1 is the introduction followed by a description and application of the positivist research paradigm. The assumptions of positivism are articulated in the form of ontological, epistemological, axiological, rhetorical and methodological. A quantitative descriptive research design is discussed followed by the research methods-target population, instrument development, pre-testing, data collection, analysis and chapter summary.

5.2 Overview of Information Systems Research

As a transdisciplinary, the Information Systems (IS) field has its roots in social science disciplines such as computer science, organisational behaviour, sociology (Walsham, 2012). IS encompasses a cross-cultural phenomenon of organisations, societies, individuals, ethical and policy issues, thus, with this diversity, many scholars have debated if Information System is a discipline or not (Cordoba, Pilkington & Bernroider, 2012). With reference to the IS debates, scholars have not agreed to the nature and domain of IS research. Orlikowski and Iacono (2001) argue that IS researchers have concentrated on theoretical significance of the context where technology is seen to operate and the processing power of IT artefacts. For example, developing a computer program, which, once tested, is installed and used to achieve organisational goals. IS scholars imply that IT is not part of natural science, but always embedded in the contexts of time, discourse, place and community, thus, IT is regarded to as transitive- passing through different stages (idea generation, development and modification (Orlikowski & Iacono, 2001).

Benbasat and Zmud (2003) criticise Orlikowski and Iacono (2001) by stating that such views limit the growth of IS as a discipline. IS scholars publishing on an IS subject, they bring new theories, insights and methodologies that enrich the IS discipline (Benbasat & Zmud, 2003). For example, this current study embeds law, organisational behaviour and Information Systems within the auspices of the IS discipline. Therefore, the richness in the current study brings out new theories and insights. Agarwal and Lucas Jr (2005) posit that the transformative capabilities of IT have been experienced in areas such as organisational services, customer services, national, regional and global economics. The views by Agarwal and Lucas Jr (2005) are echoed by Obiatade (2019) who states that IS scholars have diversified research into areas like governance, Cybersecurity and civil society. The researcher to this study asserts that IS research encompasses all facets business, science and social science disciplines because the world is operating in an information society. The diversity of IS research has and continues to contribute to the use of mono-methods (quantitative or qualitative) or mixed methods research.

5.3 Research Philosophy

This study measures the extent of alignment of influencing factors and their interactions to achieve ana aligned SA-NCPF. Past studies have failed to address the concept of alignment using linear approaches, thus, this thesis used the Gestalts approach. Prior to the use of the Gestalts approach, various multidisciplinary literature and theories were consulted leading to the development of an integrative theoretical framework (see Figure 3.2). The integrative theoretical framework brings the theories together so that one can understand the various aspects involved more comprehensively. The integrative theoretical framework and Gestalts approach were used to develop the conceptual model that measured the alignment of the SA-NCPF.

In order to conduct this study, the researcher's philosophical assumptions were considered and clearly articulated because these assumptions informed the entire research (Guba, 1990; Creswell & Plano Clark, 2011). The five fields of enquiry for this thesis were ontology, epistemology, axiology, rhetorical and methodology. Guba and Lincoln (1994) state that when addressing questions relating to the forms of reality, researchers use ontology to answer what can be or not be observable about reality. While epistemology focuses on "how" reality can be observed (that is, if it can be observed) and the relationship between the researcher and this reality (Guba, 1990; Gela, 2012). Axiology addresses the role and value of the researcher in

the study (Bryman & Bell, 2015). Rhetorical means the use of language when describing this reality (Chalmers, 2002). Guba and Lincoln (1994) and Chalmers (2002) state that the methodological field of enquiry describes the research procedures, tools and techniques used to investigate and discover this reality. In the next sections, the researcher describes the philosophical stance and the assumptions that guided this thesis.

This thesis adopted an objectivism ontological stance. Objectivism portrays the position that social entities exist in reality external to the social actors concerned with their existence (Guba & Lincoln, 1994). That is, an objectivism ontological position in this study asserted that the relationship between the social phenomena and their meanings was independent of social actors. Given (2008) asserts that information obtained from sensory experience which is interpreted through reason and logic, underpins the exclusive source of all certain knowledge. Positivists believe that positive facts (verified data) obtained from senses is based on empirical evidence (Onwuegbuzie & Leech (2005). This study viewed that all knowledge should be verified through a scientific method- logical or mathematical proof. Creswell and Plano Clark (2011) assert that scientific methods provide empirical, observable and measurable evidence which are subject to the principles of logic and reasoning. Tashakkori and Creswell (2007) further state that positivism describes that valid knowledge is found only in posterior knowledge (that is, knowledge based on experience). Frey (2018) corroborates the views above by stating that, through the lens of positivism, only scientifically and empirically verifiable facts are knowledge. In support of theories and hypotheses, verifiable empirical evidence was gathered in this study (Neil, 2019). The ultimate goal was to integrate and systematise research findings into meaningful theory which is regarded as the truth.

The scientific strength of positivism is the vigorous process of setting hypotheses (Ngulube & Ngulube, 2015). Bryman and Bell (2017) state that there is a vigorous process of empirical experimentation of testing hypotheses and a deep analysis to measure and codify the results in a set of predictions. Positivists state that the study should aim to explain and predict the outcome, the research should be empirically observable via human senses (Gela, 2012; Leedy & Omrod, 2015). In the social sciences, positivism has been a dominant philosophical stance because researchers have been able to study a social activity in a scientific way. Chalmers (2002) argues that positivism does not provide a clear criterion for choosing among multiple and competing explanations it produces. Popper (1983:12; Dowding, 1995:138) state that the other weakness of positivism is its failure to consider of the subjectivity of individual life and

interpretation of the phenomenon for the subject and community of the subject. These drawbacks of positivism may lead to intellectual incoherence in research. The discussions in this chapter are guided by the illustration in Figure 5.1 below- Research Methodology Roadmap.

5.3.1 Ontological Assumption

Chalmers (2002) defines ontology as the study of being, that is, reality is constructed within the human mind. Different people perceive reality in different ways, thus, there is no one "true" reality. Deng, Tang, Zhang, Yang and Chen (2012) state that ontology is an explicit formal specialisation of a shared conceptualisation. Holden and Lynch (2004) assert that in any research, two spectrums of ontology (objectivism and subjectivism) guide the view of reality. Reality is out there and is independent of the human mind. Thus, an objectivism ontology was adopted for the current thesis with the knowledge that the researcher's beliefs or opinions cannot influence the nature of reality (Ngulube, 2021). While, proponents of subjectivism ontology believe that the view of reality dependents on the mind and it is socially constructed (Neil, 2019).

With reference to the objectivism ontological perspective of this study, the reality of nature was made up of immutable objects and structures that existed independently of an observer's perceptions, opinions or beliefs (Ngulube, 2021). The observer can observe reality objectively, thus, a value-free approach to knowledge acquisition from such views. Positivists seek to understand the causation- cause and effect of factors. For example, influencing factors interplay and produce complex relationships, which can be observed to derive knowledge. In addition, these structures exist independently of the observer's opinions, beliefs or perceptions. Given this context, an objectivism ontological spectrum of positivism guided the process of gathering knowledge for the study.

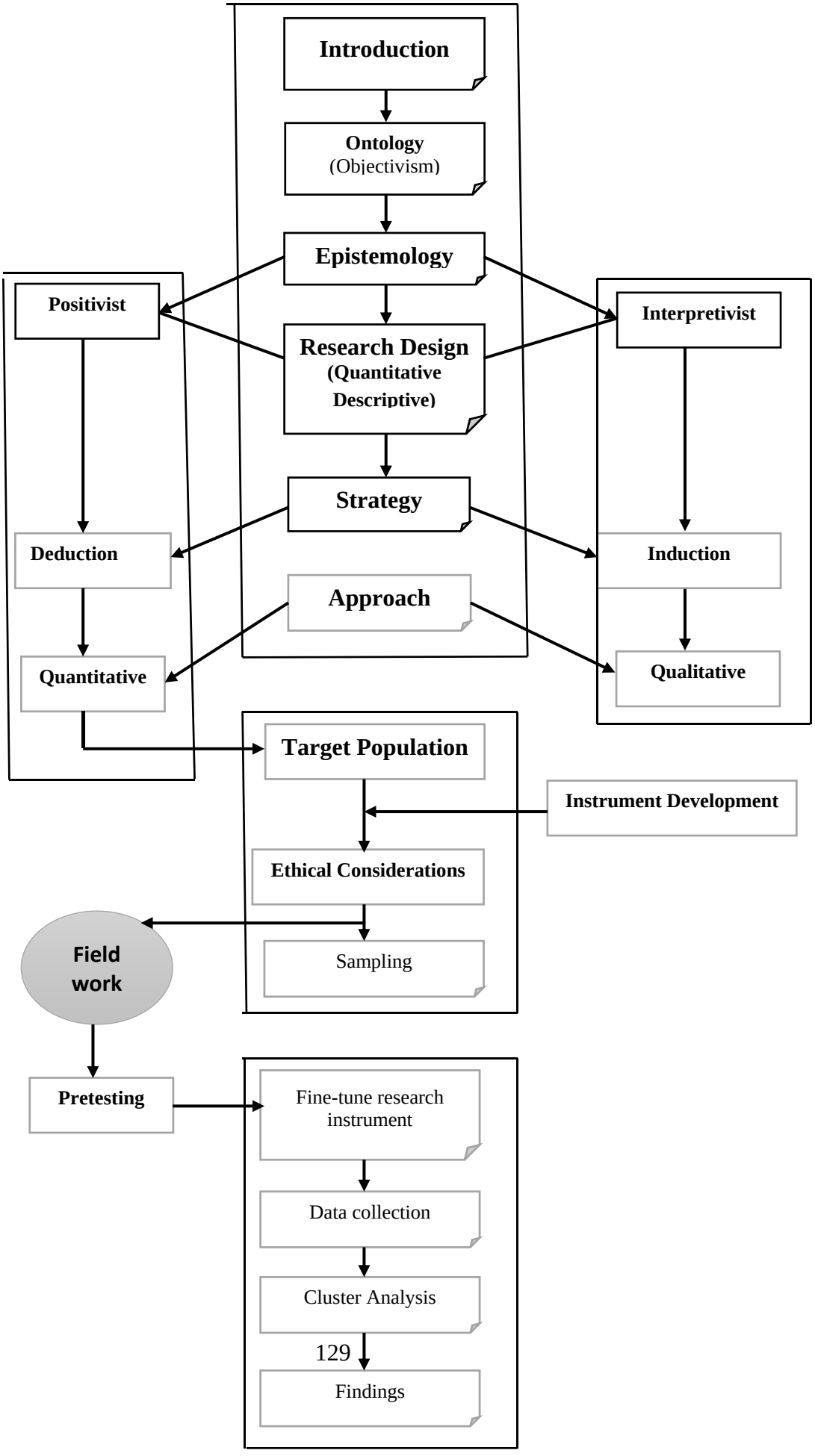
Introduction
Ontology
(Objectivism)
Epistemology
Positivist
Interpretivist
Research Design
(Quantitative
Descriptive)
Strategy
Deduction
Induction
Approach
Quantitative
Qualitative
Target Population
Instrument Development
Ethical Considerations
Field
work
Sampling
Pretesting
Fine-tune research
instrument
Data collection
Cluster Analysis
129
Findings

Figure 5.1: Research Methodology Map (Author, 2021)

The concept of alignment of the SA-NCPF has not been widely interrogated in South Africa, therefore, there was a paucity of literature. Scarcity of information and prior studies situated this study into an exploratory nature, thus, the researcher decided to adopt an objective approach to unpack knowledge about alignment of the NCPF and how its effectiveness could be beneficial to the development of a national cybersecurity strategy. With the available literature, the thesis consulted theories from other disciplines to develop an integrative theoretical framework to explain and understand the complex relationships produced by interplays from influencing factors. A conceptual model was developed by combining the integrative theoretical framework and Gestalts approach to measure the extent of alignment of the NCPF, which is a structure that exists and is a product of interrelated factors that interplayed to produce it. Literature consulted confirmed that the interactions and interplays between influencing factors can be determined objectively. The worldview of what an aligned NCPF is like, already exists, but an understanding of this phenomenon was not premised on the observer's perceptions, opinions or beliefs. This phenomenon was understood independently of the human mind and perceptions; thus, an objective inquiry was applied in the study. Given this context, the thesis adopted an objectivist ontological stance to address the overall research.

5.3.2 Epistemological Assumption

Denzin and Lincoln (1994) and Chalmers (2002) define epistemology as the theory of knowledge and the relationship between the observer and this reality. Nel (2019) posits that the philosophy of knowing (epistemology) focuses on "how" reality can be observed (that is, if it can be observed) and the relationship between the researcher and this reality (Guba, 1990). Saunders, Lewis and Thornhill (2019) state that epistemology is a fundamental assumption that describes the processes of creating, acquiring and communication of knowledge. There could be multiple methods of acquiring this knowledge from a phenomenon (Krauss, 2005). In this study, the researcher believed that positive facts (verified data) obtained from senses were based on empirical evidence (Onwuegbuzie & Leech (2005). The epistemological view of the researcher was that all observed knowledge should be verified through a scientific method, that is, through logical or mathematical proof. Therefore, the study adopted a positivism epistemology philosophical stance.

The other key consideration for the epistemological perspective of the study was the relationship between the researcher and what is being researched (Scotland, 2012). Given that positivism epistemological philosophical assumption was adopted, the researcher was detached from variables under study. The researcher wanted to ensure that the research findings depended on the phenomenon studied rather than the researcher's personality, beliefs or values. The adoption of an objectivism ontology in scientific studies helps one to get closer to the truth (Creswell & Creswell, 2017).

5.3.3 Axiological Assumption

Bryman and Bell (2017) and Saunders, Lewis and Thornhill (2016) converge on the understanding that axiology relates to the role and values of the researcher in the study. The aim of the research should be clearly articulated; therefore, the researcher should be conversant with the research procedures such as designing the research plan, instrument development, obtaining gatekeepers' permission, ethical clearance, conducting the survey and performing data analysis. In this study, the researcher was the principal investigator (PI), undertook all steps from inception to the end of the research study. In addition, the researcher acted in a value-free and unbiased manner, that is, personal opinions, beliefs or experiences did not influence the reality of nature. A number of strategic decisions were made by the researcher to ensure the study was successfully conducted. These include choosing an appropriate research design fit for the purpose, ensuring that a representative sample is selected for the study and ensuring that research findings were valid and reliable.

5.3.4 Rhetorical Assumption

Guba and Lincoln (1989) state that the use of language is imperative in research because it helps the audience to decipher between personal and impersonal and context-based language. Rhetorical means the use of language (Chalmers, 2002). In support of the concept of a value-free and unbiased manner, the researcher was careful in the selection and application of words and language in this study. Therefore, impersonal, formal and rule-based language was used in this study. A professional writing style using the English language was used. The researcher did not use colloquialisms, or first-person pronouns, which ultimately produced this final report.

5.3.5 Methodological Assumption

Le Grange (2018) and Ngulube (2021) define a research methodology as the specific techniques that are used to identify, select, process and analyse data about a phenomenon. Different research methods such as qualitative, mixed methods research or quantitative could have been used to gather, analyse and interpret research data. Positivism supports the use of quantitative methods with the objective of identifying causal relationships. Le Grange (2018) states that if the study is exploratory nature, then empirical evidence should be gathered and scientifically tested with a mathematical method. The quantitative method emphasized objective measurements, statistical and numerical analysis of data collected through the survey using computational techniques. The researcher took note of the short-fall of the quantitative methods of failing to explain the mechanisms that give rise to causal relationships and the conditions under which these relationships are bound to hold. In addition, the quantitative methodology did not obtain the vice of the participant, which could have strengthened the findings from the survey. However, this was discussed as a limitation of the study and an appropriate recommendation is made in Chapter 7.

5.4 Research Design

Teddlie and Tashakkori (2008), Babbie (2010) and Creswell (2015) all concur that every research study requires a plan or strategy that allows the researcher to conduct the study by examining specific testable research questions. Saunders, Lewis, Thornhill and Bristow (2019) define a research design as a blueprint that describes how data are gathered, measured and analysed. Leedy and Omrod (2014) states that there are various research designs at the disposal of social scientists. **Causal-comparative research designs** allow researchers to investigate the effect of an independent variable on a dependent variable. This is achieved by comparing two or more groups. When conducting an informal or unstructured research where there is no past data or there are limited studies for reference, the **exploratory research design** would be appropriate (van Wyk, 2012).

Explanatory research designs are suitable in studies where the problem has not been well researched before. Researchers use explanatory research designs to provide detailed explanations of the study (Creswell, 2013). When measuring the outcome and exposures of participants at the same time, it is appropriate to use the **cross-sectional design** because the researcher can also observe the participants. While studies that involve repeated observations

of the same variables over a short or long period of time, are referred to as **longitudinal research designs** (Leedy & Omrod, 2014). Dulock (1993) states that research designs are influenced by the available knowledge in the specific area under study. Having looked at various research designs, this thesis adopted a quantitative research design as shown in Figure 5.1.

5.4.1 Quantitative Descriptive Research Design

A quantitative descriptive research design was adopted for the study because the study systematically and accurately described the characteristics of a given area of interest. Descriptive research designs provide accurate portrayal of the situation, whilst describing what exists (Dulock, 1993; Ngulube, 2014, Creswell, 2018). A quantitative descriptive research design is also a dominant positivist approach in IS research because it helps to answer questions based on prevailing events of the study. Importantly, the research study sought to discover the associations or relationships among variables which were deemed to be the factors contributing to misalignment of the SA-NCPF. The current study involved "what" type of questions rather the "why" it happened type of questions (Pinsonnault & Kraemer,1993). This study collected quantifiable information for statistical analysis of the sample, of which data could be used for further research using different research techniques (Bryman & Bell, 2015). Past studies that have used descriptive research designs reported that high quality data, thorough information, quick to perform and a means for decision-making have been proven to be unique selling propositions (Salkind, 2018).

The flexibility of using different data collection methods (observational, case study and survey methods), ability to conduct the study in a natural environment and involvement of a large sample size, the descriptive research design was best suited for the current study (Saunders *et al.,* 2019). Furthermore, it was shown in past studies that descriptive research designs offered structured approaches that improved efficiency and effectiveness at gathering, analysing and processing of research data (Leedy & Omrod, 2019). Many academic institutions tend to adopt descriptive designs because of the benefits that were outlined in this section. The researcher's value-free position accorded by the survey method was appropriate for hypothetic deductive theory testing studies such as the current thesis (Venkatesh *et al.,* 2013). It also enhanced generalisability of research findings (Le Grange, 2018).

5.4.2 Research Strategy

Saunders et al. (2019) define a research strategy as a clearly outlined set of procedures that give the researcher directions to one's thought and efforts, enabling a systematic approach to conduct research. The objective of the research strategy is to produce quality results and detailed reporting. Creswell and Creswell (2017) state that induction and deduction are the most common research strategies available. Induction or inductive reasoning is an approach to logical thinking that involves making generalisations based on specific incidents one would have experienced or observations made. Researchers make observations to reach a conclusion, which might not always be true, but should be reasonable based on evidence. Ngulube (2019) defines deductive reasoning as a form of valid reasoning because it starts with a general statement or proposition and examines the possibilities to reach a specific logical conclusion. This study adopted a deductive strategy to complement the positivism epistemological stance and other overall research design. The researcher used a deduction strategy to test propositions(hypotheses) and theories. Three propositions (hypotheses) were formulated and tested in this study. In deductive inference, the study was premised on a specific theory (Configurations) and based on that theory, prediction of its consequences was made. The conclusions were based on the concordance of multiple premises which are generally assumed to be true.

5.5 Target Population

Research involving human beings should identify the target population from whom research data would be collected (Creswell, 2014). The target population entails a group of people or objects of interest to the researcher (Ngulube & Ngulube, 2015). A critical question in the research process is where research data are collected. This study focused on the South African National Cybersecurity Policy Framework, therefore, by default, South Africa emerged as the suitable country for conducting the research project. Data was collected from adults (above 18 years old) living in and outside South Africa. These individuals were drawn from IS, law, Computer Science and IT disciplines. Ngulube (2019) states that researchers should endeavour involve adults- that is people who are 18 years old and above in their studies because these individuals would have reached an age of maturity, can make independent decisions and in many countries, are eligible to vote. Thus, the age limit was of paramount importance in this thesis.

Yin (2014) posits that at the start of the study, it is important define the units of analysis to avoid data collection from respondents that do not add value to the study. Trochim (2020) defines a unit of analysis as the major entity that would be analysed in the study. For this thesis, the units of analysis were individuals with a vested interest in the SA-NCPF. The Association for Information Systems (AIS) database was used to reach out to respondents occupying various positions in Information Systems Security, Cybersecurity, Legal and academic brains in cybersecurity. In addition, legal experts were selected from the database supplied by the law clinics of UCT, University of the Witwatersrand (Wits) and University of the Western Cape (UWC), Parliamentarians, politicians and Ministers were also selected for the study. The logic for inclusion of Parliamentarians, politicians and Ministers; was premised on their roles as policymakers in Parliament (National Assembly and National Council of Provinces). The level of education and current position of respondents were a major consideration because of the complexity of issues that were examined. One was expected to have been acquired a certain level of education and working experience to understand the concepts under investigation. After identifying the site where the study would be conducted, the next concern was to develop an appropriate research instrument which was pertinent to get ethics approval.

5.6 Instrument Development

Two stages were involved in the development of the research instrument for the current study: (1) reviewing past studies to establish if there are existing questionnaires designed to measure constructs of the conceptual framework. Past studies provided insights and guidelines of developing the instrument regarding which issues were relevant to the development of an effective national cybersecurity strategy through the lens of an aligned NCPF (see Table 3.1). (ii) The research instrument was pre-tested to ensure validity (discussed in the next subsection).

The instrument comprised the introductory section about the purpose and objectives of the study. An overview of the research title and ethical issues was provided to assure respondents that study was approved by the University of Cape Town, Commerce Faculty Committee on Research Ethics. Section A: Demographic Information of respondents. This section was paramount to describe the characteristics of sample elements to ensure there were representative of the population for generalisation. The variables that were considered include gender, age, highest qualification, current position/title, number of years of working experience and ethnicity. A 7-point Likert Type Scale was used throughout the research instrument for a

consistent data collection and response process.1=Strongly disagree; 2=Disagree; 3=Somewhat disagree; 4= Neutral; 5=Somewhat agree; 6=Agree and 7=Strongly agree (See Appendix A).

Section B- Cybersecurity: This section sought to elicit respondents' level of agreement or disagreement with the concept of cybersecurity from a national perspective. Cybersecurity has and is a topical issue globally that should be given utmost attention if economies and firms are to protect their valuable information and knowledge assets.

Section C-Factors contributing to alignment of e-legislation. There are nine (9) constructs identified in the study are fundamental in developing an effective NCPF as well as the Republic of South Africa's national cybersecurity strategy and these are:

i) **Understanding of Cybersecurity:** The nexus of this thesis is cybersecurity and its effects on individuals and businesses in the country and globally. Citizens and businesses should be aware that cybersecurity is a shared responsibility because the over-reliance on ICTs is brewing a plethora of cybercrimes (ITU, 2019). An effective national cybersecurity strategy manifests the level of understanding, commitment and astuteness of citizens and business.

ii) **Law-making process:** In order to understand the law-making process, respondents indicated how the pace of the law-making process contributed to the growth of cybercrimes. A myriad of fragmented pieces of e-legislation coordinated by multiple government agencies play a significant role in the mis/alignment process of the SA-NCPF. Past studies by Orji (2012); Ncube (2014) and Government Gazette (2015) on the National Cyber Security Policy Framework provided insights into this construct. Chapter 3 of the study provided an elaborate discussion of the law-making process and regulatory environment in South Africa in an attempt to elucidate the perceived effects of law-making processes.

iii) **Coordination of legislation among multiple agencies (MAIS):** This variable highlighted the prevalence of multiple government agencies and the different information systems used to address cybercrimes. Given the multiplicity of agencies involved, sharing of information was inadmissible for fear of exposing intellectual

property. Claassen *et al*. (2012) and Mahlobo (2015) clearly articulated constructs i) and ii) above in Chapter 3.

iv) **Monitoring and Control (MC):** Appropriate mechanisms for monitoring and control in an information systems security strategy were considered key to the cybersecurity debates (Maja *et al*., 2020).

v) **IT and legal skills in Cybersecurity (SIC):** This issue has been topical in South Africa and the globally. National debates and statistics demonstrate that South Africa is confronted with a number of skills shortage in a number of areas of which IT/IS is one of them. This construct was derived from reports presented by Statistics South Africa regarding skills shortage (van der Merwe et al., 2016; StatsSA, 2020).

vi) **Knowledge and Information Sharing (KIS):** The extent to which multiple government agencies share or do not share information was considered key in the national cybersecurity protection strategy. Information and knowledge sharing were deemed paramount to detect trends of threat actors (Chigada, 2014).

vii) **Use behaviour (PICL):** With a fast-paced technological environment, so is the rate at which cybercriminals are outpacing existing cybersecurity interventions that the pace of implementing laws is very slow and time-consuming. There is also the element of unacceptable user behaviour stifling the implementation of cyber laws (Schultz, 2016; Johnson, 2017; Bote, 2019).

viii) **A Cybersecurity Culture (CSC):** Overreliance on ICTs requires firms to develop and implement effective cybersecurity cultures. Interactions between employees and people inside or outside their organisations can culminate in acceptable or unacceptable behaviour that expose the firm's information and knowledge assets (Knowles, 2016; Keman & Pearlson, 2019).

ix) **Coherent cyber laws (EGCL):** The global village is chasing after cyber-threats and attacks through development of cyberlaws. Developing economies are at the receiving end because they might not be familiar with new cyber-legislation, thus, compounding the pace of implementation (Freedman, 2016; McLeod, 2016). In

addition, newly implemented laws are fragmented and incoherent or might fall behind prevailing trends.

Chapters 2 and 3 of this thesis discussed all the of the above constructs in relation to cybersecurity and the South African regulatory environment. Various scholars such as Orji (2012); Ncube (2014); Colangelo (2016); Ajumobi and Kyobe (2017) and Chigada and Kyobe (2018); Bote (2019); Malatji et al (2021) to name but a few authors have concurred with each other about the effects of the above factors have and continue to play an important role in the South African cybersecurity regulatory environment. The research instrument used in this study was developed on the basis of the findings from past studies as illustrated in Table 3.1. Each of the nine elements was measured on the Likert Type Scale. Table 5.1 below presents a summary of the questionnaire constructs and related details.

Table 5 .1: Constructs, Variables and References

	Constructs	No of variables	References
Understanding of Cybersecurity	Overreliance on ICTs	1 (Q8)	Ajumobi & Kyobe (2017); ITU (2019); Khan, Brohi and Zaman (2020).
	Not well-understood	1 (Q9)	Selebalo, 2014); Keman and Pearlson (2019)
	Conflicting terminology	1 (Q10)	Schultz (2016); van der Merwe et al (2016);
	Complex cyber-attacks and threats	1 (Q11)	Mahlobo (2015); Chigada and Kyobe (2018); Bote (2019)
Influencing factors	LMPRE	4 (Q12; Q14; Q16; Q18)	Malatji et al (2021) Pokwana and Kyobe (2016)
	MAIS	5 (Q19; Q20; Q21; Q22; Q24)	(Keman & Pearlson, 2019); (Fitch, 2020).
	MC	3 (Q25; Q26; Q28)	Pokwana & Kyobe, 2016). van der Merwe (2016)
	SIC	5 (Q30-Q34)	Gumbi (2018); (PwC, 2018; StatsSA, 2019).
	KIS	3 (Q35; Q37; Q38)	Chigada (2014) (Fitch, 2020).
	PICL	3 (Q40; Q42; Q43)	Schwab (2019) Wout, 2019).
	CSC	5 (Q44-Q48)	Gzaca and von Solms (2017); Boucher, Gundu and Maronga (2019)
	EGCL	5 (Q51-Q55)	Gumbi (2018); Pistorius and Mwim (2019)

Kim (2009) states that the use of existing instruments (where possible) helps to maximise reliability and validity of the instrument, the questionnaire was validated before the actual data collection.

5.7 Pre-testing

The purpose of pre-testing the research instrument was to ensure that all the constructs were accurately captured, that the research instrument measured what it was designed to measure and there were no errors or ambiguities. Pre-testing was achieved by carrying out the following:

5.7.1 Content Validity

The first stage was to ensure that all variables in the research instrument were drawn from a universal pool of items to represent the entire domain of the construct (Straub, 1989). Legal, cybersecurity experts, lawmakers and IS academics from the University of Cape Town and University of Johannesburg, UWC, National Assembly and CSIR were consulted to review the questionnaire. A total of eleven experts reviewed the questionnaire items, instructions and language in line with the recommendations by Cronbach (1971) to ensure appropriate responses were gathered. Inputs from this panel experts were incorporated in the final research instrument. A common recommendation from the experts was to reduce the constructs from 58 by teasing out questions that appeared repetitive. This was achieved by using existing research instruments that had been used in studies closely related to the current thesis.

Given the recommendations suggested by the panel of experts, the researcher was concerned about research instrument's ability to measure what it was designed for. A pilot test was recommended. Ruel, Wagner and Gillespie (2016) describe pre-testing as a tool through which researchers validate the research instrument by ensuring that research questions are clearly articulated and response options are relevant, comprehensive and mutually exclusive. Babbie (2010) states that pre-testing is a small-scale study used as a quality assurance process by researchers. Sixty-five (65) randomly selected respondents representing the target population, were involved in pre-testing the research instrument. Bryman and Bell (2017) posit that pre-testing helps to tease errors, sensitive and harmful statements prior to gathering actual data. Ngulube (2019) posits that pre-testing the research instrument is an important process in research because the author will have second opportunity to fine-tune the research instrument (see figure 5.1). Given the nature of suggestions given by the experts and respondents, the final research instrument (Appendix A) selected some relevant variables for the research.

5.7.2 Reliability

Kumar (2012) defines reliability as the ability of the research instrument to consistently produce the same scores every time it is used to measure a constant value. Salkind (2018) posits that reliability of the research instrument is determined by its consistency and stability. Instruments that always give the same answer every time with changing its value, is deemed very reliable and can be trusted to provide accurate results (Trochim, 2020). For this study, internal consistency was used as measure of this quantitative study. The study tested internal consistency using Cronbach's alpha co-efficient (Cronbach, 1951). Cronbach's Coefficient alpha (α) is highly recommended in social science research (Straub, Gefen & Boudreau, 2005).

Four items measuring Cybersecurity had a Cronbach's alpha of 0.88; while four items measuring LMPRE had a Cronbach alpha of 0.86; five items measuring MAIS had a Cronbach's alpha of 0.87; three items measuring MC had a Cronbach's alpha of 0.78; five items measuring SIC had a Cronbach's alpha of 0.91; three items measuring KIS had a Cronbach's alpha of 0.77; three items measuring PICL had a Cronbach's alpha of 0.81; five items measuring CSC had a Cronbach's alpha of 0.79 and five items measuring EGCL had a Cronbach's alpha of 0.82.

Instruments that are not reliable receive a score of zero (0), whereas, instruments with a high level of reliability will receive a score of one (1). However, many scholars accept research instruments with a co-efficient reliability of 0.70. If the reliability of the instrument has to be improved, it is the researcher's onus to increase the number of observations, eliminate items that are not clear and maintain consistent scoring procedures (Salkind, 2018). In all cases shown in Table 5.2 above, the reliability coefficients of the questionnaire were above the recommended alpha coefficient of 0.70, which suggests that the research instrument was reliable (Schmitt, 1996; Creswell & Plano Clark, 2011; Ngulube, 2019).

A summary of Cronbach's alpha coefficient values is presented in Table 5.2 below.

Table 5.2: Cronbach's alpha coefficient Values

Construct	Cronbach's alpha coefficient
CS	0.88
LMPRE	0.86
MAIS	0.87
MC	0.78
SIC	0.91
KIS	0.77
PICL	0.81
CSC	0.79
EGCL	0.82

5.8 Ethical Considerations

Ethics in social research especially where the research involves people, is an essential component of the research project. This research study had to be approved by the University of Cape, Faculty of Commerce Research Committee because it involved human beings. The formal approval reference is **REC2018/001/005** granted on the 5th of January 2018. This approval enabled the researcher to establish ethical standards considered when conducting research involving people. The ethical issues considered were:

***Full disclosure of study information*:** The name, surname and contact details of the researcher were included in the introductory narrative to respondents. In addition, the purpose and objective of the study were clearly outlined to better inform respondents. This allowed respondents to either proceed or withdraw from the study. ***Privacy and confidentiality*:** The researcher designed the instrument so that no personal identifiable information (names, employer's name, telephone numbers or residential addresses) could be provided on the questionnaire. Disclosure of personal information is prohibited in Section 26 of the Protection of Personal Information Act (POPI) of 2013, therefore, all respondents were assured that no personal information or responses would be shared with third parties without the respondents' written or expressed approval. The information provided was for the purpose of the study and would remain private and confidential. Though all data would remain the property of the UCT,

the researcher kept the files in a secured iCloud account which was accessed through a two-factor encryption.

Free to participate or withdraw from the study: In order to ensure that respondents were not coerced to participate in the study, the researcher clearly stated that participation in the study was voluntary. There were no rewards or incentives for participation, thus, respondents were free to withdraw from the study at any given time without ramifications. ***Integrity and honest:*** It is the responsibility to safeguard respondents, build trust, while fostering honesty and avoiding misconduct and impropriety. Respondents were assured that the highest level of integrity would be the cornerstone of the current study. First, an ethical clearance was granted by the UCT Faculty of Commerce Ethics Committee. People's safety, rights and dignity were respected. This was achieved through detachment from the subjects under investigation.

Inducement to participate: Ngulube (2014) defines inducement as a form of persuasion or leading someone to do something under certain conditions. When participants are induced or incited/lured to do something, information may be biased and is not freely given. In this study, respondents' involvement in the study was freely given, specific and based on informed consent. ***Personal information:*** Bates and Cozby (2012) define personal information as that information about an individual whose identity can be ascertained or apparent. Personal information can be recorded in material form or not about an individual. The demographic constructs of participants did not contain personal information. At no point, where respondents requested to provide their names, names of organisations they worked for to mitigate exposure of personal information. This approach was done in compliance with the Protection of Personal Information Act (POPIA).

Planning the research*:** In order to avoid reporting of misleading results, the researcher drafted and properly executed a research plan. The researcher took the necessary steps to protect and ensure the dignity of respondents as well as those that participated in this study (Bryman & Bell, 2010). ***Responsibility: Ngulube (2019) states that researchers must maintain the dignity and welfare of respondents. Appropriate steps were taken to protect respondents from emotional and physical harm. Sensitive questions were eliminated during the pre-testing of the questionnaire. ***Honesty:*** The research was conducted in an honest, fair and transparent manner and the respondents were informed of the purpose and benefits of the study. The questionnaire provided a narration of the purpose and benefits of the study, thus, gave respondents with an

opportunity to participate or withdraw from the study. The respondents were randomly selected to eliminate favouritism/bias when the questionnaire was sent out.

5.9 Sampling Procedure

Sampling entails drawing objects or individuals from a population in a way that the sample is representative of the population for generalisation purposes (Creswell, 2014). There are multiple factors and role players to the SA-NCPF (academia, law, Parliament, Ministers, Politicians, private sector and civil society) with a vested interest in the country's cyberspace environment. Sample elements were drawn from Institute of Information Technology of South Africa (IITPSA), law-schools, the Association of Information Systems (AIS) databases. The total population for the study was 14801 people in various positions as indicated above. The sample size was generated by using Tejada and Punzalan (2012) formula highlighted below:

$$sample\ size = \frac{\frac{z^2 * p(1-p)}{e^2}}{1 + \frac{z^2 * p(1-p)}{e^2 N}}$$

Where *N*=population size *(14801*) and *e*=margin of error *(0.05*). The sample to be utilised was 655. There are many considerations to take when selecting the sample. Zikmund et al., (2013) define probability sampling as a technique whereby every member of the population has a known, non-zero probability of selection. In most cases, especially where selection is random, all members have an equal, non-zero probability of selection. Non-probability sampling is a sampling technique whereby members of the sample are selected from the population, based on the researcher's judgment or convenience. In non-probability sampling, the probability of any particular member of the population being chosen is unknown. In this study, probability simple random sampling was used to select respondents.

5.9.1. Simple Random Sampling

Given the nature diversity and geographic locations of respondents involved in the study, a probability simple random sampling technique to ensure that important role actors were included in the study. Tashakkori and Teddlie (2003) state that probability sampling techniques ensure that each member of the population has a known and equal chance of inclusion in the study. With a list of individuals occupying various positions (see target population), a lottery

system was used where each member was allocated a unique computer-generated number. Chigada (2014) states that the lottery system is value-free because random numbers are generated by a computer program, assigned to each member and then the computer program is run to select numbers randomly-randomisation.

5.10 Quantitative Data Collection

After identifying the target population, instrument development and obtaining ethical approval, the researcher was confronted with the "how" question of data collection. To achieve the purpose of testing propositions, quantitative data were necessary to accomplish this purpose, thus, a questionnaire was the ideal research instrument. The merits of using the questionnaire were that the researcher was able to collect data from a large sample (Rowley, 2012); same statements were provided to each respondent resulting in a consistent data collection process (Ngulube & Ngulube, 2015) and the researcher was detached from the subjects involved in the study, which is an ideal condition for studies that test propositions (Chen & Hirschheim, 2004). The only limit with the use of questionnaires is the absence of the respondent's response to some items missing from the questionnaire because the researcher cannot probe further for clarity.

5.10.1 Fieldwork

Data were collected after receiving the ethical clearance from the University of Cape Town and undertaking a number of steps described above. Respondents for this study were not known to the researcher prior, during and post data collection. When the survey was conducted, the author introduced and informed the respondents that the purpose of the study was for academic purposes and that their participation in the study was voluntary and they could withdraw from the study at any time they wished (Teddlie & Yu, 2007). It was at the point of setting up appointments with selected Parliamentarians, Ministers and Politicians that the researcher had to meet these respondents and introduce the purpose of the study. The researcher visited some of the respondents' offices in different parts of the country to ensure the questionnaires were delivered and collected.

The questionnaire was administered through Qualtrics, self-administered and shared on the AIS e-Library database and law and IT/IS schools from different universities in the country. Data were collected from 1 March 2018 to 31 May 2018 (over three months period) because some

respondents requested hand-delivered questionnaires. All completed questionnaires were saved on the Qualtrics online platform and prepared for the next statistical process. A total of 655 respondents received the questionnaires, 206 questionnaires were incomplete and thus, excluded from the analysis. The final usable questionnaires were 449 (69%) response rate which is above the recommended rate (55%) that provides high precision (Leedy & Omrod, 2019). In Cluster analysis, the minimum sample size should include no less than 2^k cases, preferably (Formann, 1984), where k= number of variables in Cluster analysis. For the nine clustering variables (See Table 5.2), the minimum sample size would have been 120 respondents. Therefore, the 449-sample size used in this study was far more than the recommended minimum sample size for 9 clustering variables. The next section discusses the quantitative data analysis process.

5.11 Quantitative Data Analysis

Numerical/mathematical raw facts collected in this study did not convey any meaning, thus, the next stage was to manipulate the facts and produce meaning- data analysis. A Statistical Package for Social Scientists (SPSS v 24) was used in the data analysis phase to identify clusters. SPSS was allowed the researcher to perform Descriptive analysis and Cluster analysis, As espoused by Chin (1998) SPSS was capable of testing a *priori* propositions against empirical data. By adopting a multivariate analysis, the researcher simultaneously analysed the relationships among the nine constructs (Babbie, 2010).

5.11.1 Cluster Analysis Technique

Punj and Stewart (1983) and Creswell (1994) state that Cluster analysis is an exploratory data analysis technique where data are organised into meaningful groups (clusters). Coghlan and Brydon-Miller (2014) assert that objects with more similar multivariate characteristics are grouped together (clusters) than those in other groups. This study involved classification and made no prior assumptions about the differences existing in the population, therefore, Cluster analysis was ideal (Chin, 1998).

The study examined configurations or patterns of interacting factors, thus, Cluster analysis was the best suited technique. Social scientists argue that when examining groupings or taxonomies, Cluster analysis and Factor analysis are commonly used. The distinction between Factor analysis and Cluster analysis is that Factor analysis reduces the number of variables into

smaller sets of factors to reveal the underlying factors, while Cluster analysis reduces the number of observations into clusters based on proximity (Burns & Burns, 2008). Cluster analysis is exploratory, therefore, with the adoption of the Gestalts/Configurations theory, the researcher performed a Cluster analysis to examine the groupings of the constructs. The researcher did not have prior knowledge of how variables would be grouped, Cluster analysis was appropriate for the Gestalts perspective.

5.11.2 Clustering Algorithms

Punj and Stewart (1983) define Clustering algorithms as procedures that guide the sorting process of observations. It is critical to select an appropriate clustering algorithm to derived optimum Cluster analysis benefits. Ketchen and Shook (1996) state that hierarchical algorithms progress a series of procedures building a tree-like structure through an add/delete elements operation. The add/delete operation, agglomerative and divisive methods are inherent in hierarchical algorithms. "Agglomerative methods are centred on adding elements to clusters while divisive methods concern deleting them from clusters. However, all hierarchical algorithms suffer from poor cluster assignment resulting from single pass through data set (Ketchen & Shook, 1996).

The second Clustering algorithm is the K-means or non-hierarchical. K-means are also referred to as iterative methods, which partition a data-set into a pre-specified number of clusters to arrive at optimal solutions (Ketchen & Shook, 1996). K-means clustering has several advantages over hierarchical algorithms. First, K-means clustering is less affected by outlier elements. This problem is corrected during subsequent pass through data set as observations switch cluster membership (Hair, Anderson, Tatham & Black, 1992). Second, K-means clustering has the capability to optimise solutions within cluster homogeneity and between cluster heterogeneity (Ketchen & Shook, 1996). Third, K-means clustering is useful when propositions are already developed for the cluster variables". Based on the above account, K-means outperforms the hierarchical algorithm; hence this study adopted the K-means technique to perform cluster algorithms.

5.11.3 KMO and Bartlett's Test

The Kaiser-Meyer-Olkin Measure of sampling adequacy indicates the proportion of variance in the variables that might be caused by underlying factors (Creswell, 2012). Scores close 1.0 indicate that the results of factor analysis are useful with research data, while values less than

0.50 indicate that results of factor analysis are not useful. Chin (1998) state that Bartlett's test of sphericity tests the propositions that the correlation matrix is an identity matrix. This means that the variables are not related and not suitable for structure detection. All values less than 0.05 of the significance level indicate that a factor analysis maybe useful to the data.

5.12 Chapter Summary

This chapter described the research design and methodology through the lens of the positivist paradigm. The researcher pointed out that social scientists share a set of beliefs in how IS research problems are understood and resolved, therefore, the positivist paradigm was used as the conduit for understanding the phenomenon under study. The ontological, epistemological, axiological, rhetorical and methodological assumptions of the positivist paradigm were discussed. A quantitative research method was adopted because the study focused on gathering quantifiable and numerical information for statistical computation. In order to put together different components of the research procedures, a research plan (quantitative descriptive research design) was decided upon and adopted in the study. Lastly the chapter discussed quantitative data analysis through the lens of Cluster analysis. A discussion of Clustering algorithms helped to clarify that the present study used the K-means to perform cluster algorithms.

The next chapter presents an analysis, interpretation and discussion of research findings.

CHAPTER SIX: INTERPRETATION, ANALYSIS AND DISCUSSION OF FINDINGS

6.1 Introduction

This chapter presents research findings which are analysed, interpreted and presented in a logical sequence, in the order in which the specific purposes of the study were formulated. The results are directly related to the methods of analysis, justification for their choice, the results of the investigation and the significance of the results. The first section of the chapter describes the Bayesian Criterion Clustering Algorithm followed by the demographic characteristics profiling of clusters. In this section, the study presents findings relating to the demographics of all respondents. The next section presents findings relating to cluster profiles of influencing factors (patterns). Lastly, the chapter is summarised.

6.2 Clustering Algorithm and Procedure

The Bayesian Criterion was used in the study where the researcher applied centroid-based algorithms to create k-partitions based on a dissimilarity function. In addition, the k-means were not affected by ordinal scales and were robust in scales and data dimensions (Punj & Stewart, 1983). The researcher used ordinal scales for the variables analysed through clusters. K-means algorithms allowed this thesis to specify the number of clusters. For example, this study established 15 clusters, which ensured that within-cluster homogeneity and between-cluster heterogeneity in the final cluster solution is optimal (Ketchen and Shook, 1996). The number of clusters established in this study helped the researcher to see if the configurations would be derived on the cases. Thus, the study ran k-means cluster analysis with variables that had ordinal scales, while variables with nominal scales were excluded to minimise inconsistencies in the distance measures of the variables (see table 6.1 below).

The BIC scores testing ration of distance measures showed significant difference across the 15 clusters as shown in Table 6.1 below. These results show interesting configurations that could provide insights and better understanding of the influencing factors and how they interplay if this revelation was to be compared to what the researcher expected to uncover. Cluster 1 (4.501) and Cluster 2(4.471) showed high ratio distance measures. However, when progressing through the other 13 Clusters, the distance measures show closeness. This is in line with the

assertions that the k-means favours groups of variables with similar means and closeness to centroids and there is a high likely that two different centroids can be selected from the same cluster (Kuo, Ho & Hu, 2002). McKeen and Singh (2007) and Chowdhary and Prakash (2007) have reported that it is possible that one cluster can combine three different groups, which one would have expected to be separately clustered. The ratio of distance measure for the total sample for each cluster are shown on the extreme right-hand side of Table 6.1 below. Cluster 1 (N=32) had a mean score for the total sample of (4.531) and Cluster 2 (N=18) mean score for the total sample was 4.471. The other 13 clusters had mean scores for the total sample of less than 1.6 as shown below.

Table 6 .1: All Continuous Variables (Auto-Clustering)

Number of Clusters	Schwarz's Bayesian Criterion (BIC)	BIC Change[a]	Ratio of BIC Changes[b]	Ratio of Distance Measures[c]
1	2900.153	-471.375	1.01	4.531
2	1922.178	-977.975	1.000	4.471
3	1788.764	-133.414	.136	1.550
4	1741.636	-47.128	.048	1.525
5	1748.545	6.909	-.007	1.388
6	1784.238	35.693	-.036	1.484
7	1844.130	59.891	-.061	1.040
8	1905.925	61.795	-.063	1.037
9	1969.436	63.511	-.065	1.521
10	2048.830	79.393	-.081	1.111
11	2131.275	82.446	-.084	1.038
12	2214.720	83.445	-.085	1.009
13	2298.396	83.676	-.086	1.060
14	2383.559	85.163	-.087	1.099
15	2470.941	87.382	-.089	1.204

a. The ratios of changes are relative to the change for the two-cluster solution

b. The ratios of distance measures are based on the current number of clusters

6.3 Demographic Characteristics Profiling of Clusters

Table 6.2 below is a summary of the frequency distribution of the demographic variables for each cluster.

6.3.1 Gender

Cluster 1(N=32) comprised 37.5% male respondents, 50% female respondents and the other 12.5% preferred not to answer. There were more female respondents in Cluster 1 compared to their male counterparts. In Cluster (N=18), 50% male respondents compared to 33%) female respondents. Cluster 3 (N=32) 56% male respondents compared to 37.5% female respondents. Cluster 4 (N=52), Cluster 5 (N=44), Cluster 6(N=41), Cluster 7 (N=36), Cluster 8 (N=28), Cluster 9(N=39), Cluster 10 (N=28), Cluster 11 (N=15), Cluster 12 (N=20), Cluster 13 (N=23) and Cluster 14 (N=18), show that more female respondents participated in the study compared to male respondents. In Cluster 2(N=18), Cluster 3 (N=32) and Cluster 15 (23), there were more male respondents compared to female respondents. Smith (2008) and Ngulube (2014) state that participants' gender helps the researcher to ascertain if all potential sample elements are included in the study. It is acknowledged that there are actual differences in the way men's and women's brains are structured and genetically affect how they react to events and stimuli. In this study, both female and male respondents reacted differently.

6.3.2 Age

Cluster 1 (22%), Cluster 4 (11.5%) and Cluster 6 (19.5%) had the largest number of respondents between 18-24 years cohort, while the clusters recorded low response rates for people in the 18-24 year age group. High responses were recorded in Cluster 1 (53%), Cluster 3 (56%), Cluster 7 (61%), Cluster 13 (65%), Cluster 14 (67%) and Cluster 15 (52%) for respondents in the 25-44 year age group. Low response rates were recorded in Cluster 2 (39%), Cluster 4 (40%), Cluster 5 (20.45%), Cluster 6(36.6%), Cluster 8 (35.7%), Cluster 9 (30.8%), Cluster 10 (28%), Cluster 11 (33%) and Cluster (45%) respectively. For respondents older than 45 years, high responses were recorded in Cluster 5 (70.55%), Cluster 8 (53.6%), Cluster 9(54.2%), Cluster 10 (68%), Cluster 11 (54%) and Cluster 12 (55%). The rest of the Clusters recorded low responses. From the illustration in Table 6.2, it is clear that the majority of respondents were in the 25-44 years and 45 years and above age group. Babbie (2010) states that the age of the sample helps to shape the perception about demographic trends, thus, the current thesis comprised all adults from 18 years and above. The minimum age of 18 years is

in line with the UCT Research on Ethics as well as other International Reporting Standards that researchers should endeavour conduct research with adults- people who have attained a legal age of maturity and can make independent decisions (Unisa Policy on Research, 2019). Leedy and Omrod (2014) state that age is an important variable to consider when analysing the target sample because individuals in the same age cohort tend share many experiences.

6.3.3 Highest Qualification

The qualifications listed include national diploma, bachelor's degree, honours, master's doctorate and certificate. As shown in Table 6.2, there were low responses for national diploma holders in all the 15 Clusters. For bachelor's degree holders, Cluster 4 (35%) and Cluster. 12 (30%) recorded high responses compared to all the other Clusters. Cluster 1 (22%), Cluster 5 (48%), Cluster 9 (41%), Cluster 10 (39%), Cluster 11 (27%), Cluster 13 (22%), Cluster 14 (28%) and Cluster 15 (48%) recorded the largest response rates of Honours degree holders. For master's degree holders, Cluster 1 (34%), Cluster 6 (32%), Cluster 7 (42%), Cluster 8(32%) and Cluster 12 (30%) recorded the largest responses. Cluster 5 (0%) did not record anything, while the rest of the Clusters recorded response rates ranging between 6%-29% respectively. Cluster 2 (28%), Cluster 5 (20%), Cluster 8(14%), Cluster 9 (13%) and Cluster 14 (17%) recorded the highest response rates of doctorate degree holders. While other clusters recorded low responses, this was to be expected because the doctorate is the highest degree conferred by a university, therefore, not many people possess the qualification. Interestingly, very low responses were recorded in all 15 clusters for certificate holders. This could be best explained by the factor that the area under investigation, was highly specialised, therefore, respondents would ordinarily have advanced qualifications in the area. Saunders *et al.* (2012) state that qualifications help the researcher to understand the level of skills and knowledge inherent in the sample. The nature of this study required people who understood Cybersecurity terminology and related concepts, therefore, the highest qualifications held by individuals were imperative to address the research questions.

6.3.4 Current Position

This study involved respondents from diverse backgrounds occupying varying positions in society, organisations or political affiliations. Cluster 7 (11%), Cluster 11(20%), Cluster 13 (17.4%) and Cluster 15 (13%) recorded the highest rates of respondents in managerial positions. In Cluster 1 (3%), Cluster 2(17%), Cluster 3 (3%), Cluster 7 (3%), Cluster 8 (3%),

Cluster 9 (3%), Cluster 12 (10%) and Cluster 11 (3%) Honourable Members of Parliament were recorded as respondents. There were a total of 11 Hon MPs in the study. Ministers were recorded as respondents in Cluster 2(5.5%), Cluster 3 (3%), Cluster 5 (5%) and Cluster 10 (3.6%) respectively. A total of 6 Ministers participated in the study. The involvement of senior government officials and Members of Parliament was pertinent because the study gained some credence.

Cluster 2 (0%) did not record any IS engineer respondents, while the other 14 Clusters had at least an IS engineer respondent. Similarly in Cluster 11 (0%) and Cluster 12 (0%) there were Legal expert respondents. The highest legal expert respondents were recorded in Cluster 5 (16%) and Cluster 14 (22.2%) respectively, while other Clusters recorded average responses for legal experts. There wer no responses for Chief Information Security Officer (CISO) respondents in Cluster 11 (0%), Cluster 14(0%) and Cluster 15 (0%). Cluster 3 (6.25%), Cluster 5 (11%) and Cluster 6 (7.3%) recorded the highest number of CISO respondents, while the other Clusters recorded at least one CISO respondent each.

Only Cluster 11 (0%) and Cluster 12 (0%) did not record any respondents with a background in cybersecurity. However, highest responses were recorded in Cluster 1 (11.66%), Cluster 4 (8%), Cluster 5 (25%), Cluster 6 (19.5%), Cluster 7 (8.33%), Cluster 9 (21.4%), Cluster 14 (17%) and Cluster 15 (13%) respectively. Cluster 8 (0%) did not record any responses who were law enforcement, while the other 14 Clusters recorded at least one law enforcement agent. Similary, Cluster 2 (0%) also did not record any fraud specialist responses. The other 14 Clusters recorded at least one fraud specialist respondents. With reference to IT experts, all 15 clusters recorded respondents, with Cluster 3 (9.4%), Cluster 4 (12%), Cluster 6 (7.3%), Cluster 7 (11%), Cluster 8 (7.14%), Cluster 10 (14.3%), Cluster 12 (20%) amd Cluster 14 (11%) recording the highest number of IT expert respondents.

All 15 Clusters comprised respondents from academia. Highest response rates were recorded in Cluster 7 (14%), Cluster 10 (14.3%), Cluster 11(13.3%), Cluster 12 (20%), Cluster 13 (17.4%), Cluster 14 (17%) and Cluster 15 (21.74%) respectively. With reference to respondents occupying the IT Director position, Cluster 2 (0%), Cluster 6 (0%), Cluster 10 (0%), Cluster 11(0%) and Cluster 13 (0%) showed no records. Cluster 1 (6.25%) and Cluster 14 (5.5%) recorded the highest number of respondents occupying the IT Director position. Of the 15

Clusters, 4 of them (2; 4; 12; and 14) did not record any respondents occupying the Chief Information Officer position. However, Cluster 1 (11.66%), Cluster 3(6.25%), Cluster 6 (7.3%), Cluster 10 (7.14%) and Cluster 11 (6.7%) had the highest number of CIO respondents.

Only Cluster 13 (0%), Cluster 14 (0%) and Cluster 15 (0%) did not record respondents occupying the systems analyst position. All other Clusters recorded at least one systems analyst respondent, with the highest responses recorded in Cluster 2 (11%), Cluster 3 (9.4%), Cluster 4 (10%), Cluster 7 (11%), Cluster 9 (10.26%), Cluster 10 (1071%) and Cluster 12 (20%) respectively. Nine clusters recorded at least one strategist respondent, while 6 clusters (2; 7; 12;13;14 and 15) did not record any respondents occupying the strategist position. Respondents occupying the developer position were recorded in Cluster 1 (3%), Cluster 3 (3%), Cluster 4 (8%), Cluster 5 (4.6%), Cluster 6 (7.3%), Cluster 7 (2.8%), Cluster 9 (2.6%) and Cluster 10 (3.6%) respectively, while other clusters (2; 8; 11; 12; 13; 14 and 15) showed no records. Similarly six clusters (4; 9; 11; 12; 13 and 15) did not record any respondents occupying the telecoms engineer position. Cluster 2 (17%) and Cluster 3 (12.5%) recorded the highest number of telecoms engineer respondents, while the other clusters recorded at least one respondent each. Another six clusters (5; 9; 12; 13; 14; and 15) showed 0% records of network engineers. Cluster 2 (11%), Cluster 4 (10%) and Cluster 11 (6.7%) had the highest respondents of network engineers.

By involving people from diverse backgrounds, and occupying different positions in their organisations was pertinent in this study. The researcher acknowledges that inclusivity in research generates a wealth of data to solve a research question. This study was scientific in nature, thus, readers require information about the study participants, as a way of clarifying to whom the study findings apply as well as generalisation of findings (Teddlie & Yu, 2007; Leedy & Omrod, 2019). Respondents' positions were important because that demonstrated that the study sought inputs from knowledgeable people regarding the problem at hand.

6.3.5 Working experience

The study classified the working experience into five categories as shown in Table 6.2 below. 8 clusters (4; 5; 6; 11; 12; 13; 14; 15) did not record any participants will less than one working experience. Cluster 2 (11%) recorded the highest number of respondents with less than 1-year experience. All 15 clusters recorded at least 3 respondents with between 1-5 years working

experience. Cluster 2 (50%), Cluster 3 (53.1%), Cluster 11(60%) and Cluster 13 (52.2%) recorded high responses rates of 50% and above, while the response rates in the other clusters were less than 45%. Cluster 1 (18.75%), Cluster 3 (28.13%), Cluster 4 (29%), Cluster 5 (25%), Cluster 6 (20%), Cluster 8 (21.4%), Cluster 9 (28.2%), Cluster 10 (18%), Cluster 14 (22.2%) and Cluster 15 (30.4%) recorded the highest responses of the 11-20 years working experience. Only Cluster 3 (0%) did not report any respondents with more than 21 years' experience while the other 14 had at least one respondent in the working experience cohort. The highest responses were recorded in Cluster 2 (22.2%), Cluster 9 (20.2%), Cluster 12 (20%) and Cluster 15 (21.74%) respectively. Cluster 1 (6.25%), Cluster 11 (6.7%) and Cluster 13 (4.35%) recorded the least responses respectively. Creswell and Plano Clark (2011); Salkind (2018) state that working experience is key element that helps the researcher to understand if the sample elements have obtained the requisite experience, knowledge and exposure to address the research question. The questions posed in this study sought expertise and knowledge in the subject under investigation. Thus, with experience, the research study described who was involved and to whom research findings generalise and allows for comparisons to be made across replications of studies (Ellis, 2009).

6.3.6 Ethnicity

Six racial demographics adopted in this study were, Black, White, Indian, Coloured, Asian and other. The information in Table 6.2 shows that all 15 Clusters recorded high numbers of respondents in the Black ethnic group. Cluster 2 (50%) and Cluster 8(50%) had the highest responses for Black respondents, while Cluster 4 (34.6%), Cluster 5 (31.8%) and Cluster 12 (30%) had the highest number of respondents from the White ethnic group. All 15 clusters recorded at one respondent from the Indian ethnic group, with Cluster 4 (21.9%), Cluster 6 (22%) and Cluster 10 (21.43%) with the highest number of respondents. Cluster 3 (18.8%), Cluster 9 (30.8%), Cluster 10 (18%), Cluster 11 (20%), Cluster 12 (25%) and Cluster 13(26.1%) had the highest number of Coloured respondents. All other clusters were fairly represented by respondents of this ethnicity. Two clusters (11; 12) did not record any respondents from the Asian ethnic group. Cluster 1 (12.5%), Cluster 7(22.2%), Cluster 8 (21.43%) and Cluster 9(18%) recorded the highest responses. The least responses were reported in Cluster 6 (2.44%). Respondents were requested to indicate which ethnic group they belong to. Seven clusters (2; 4; 8; 9; 10; 11; 12) did not record any respondents, while Cluster

1 (9.4%) and Cluster 14 (16.7%) recorded the highest number of other ethnic groups. However, respondents did not specify even though the surevy instrument made provisions.

All racial groups were included in this study to ensure there was no bias in terms of research findings. As with the other variables discussed above, this study described the ethnicities of respondents in order to determine who was involved and to whom research findings would be generalised, thus, future studies would compare or replicate the findings (Ellis, 2009). Alienating potential sample elements on the basis of ethnicity is perceived as racial discrimination (Sigamoney, 2020). The historical past of South Africa has been mired in discriminatory and marginalisation practices, therefore, this thesis involved everyone to ensure divergent views were gathered. Given the context of the study, all racial groups were working in the area of Cybersecurity, therefore, their participation enhanced inclusivity which is a challenge in some studies (Chin, 1998; Babbie, 2010; Bryman & Bell, 2015).

Hammer (2011) states that social scientists are paying attention on increasing the diversity of research respondents and it is important to describe respondents' demographics when reporting research findings. Thus, information about respondents' ages, gender, race/ethnicity, educational level, languages spoken and current position should be reported on when presenting research findings. Failure to include such information, researchers' risk assuming the stance of "absolutism", that is, there is the assumption that the phenomena under investigation are the same regardless of the diversity in demographics. Whereas, including this information means that the researcher would have moved towards "universalism" a recognition of universal psychological processes (Bein, 2009:359; Hammer, 2011).

Readers and researchers might have a vested interest in the research, therefore, inclusion of demographic information allows them to determine to whom the research findings generalise and make comparisons to be made across replications of studies (Bein, 2009). Demographic information provides information required for secondary data analyses and research syntheses, thus, gaps in existing research can be identified so as variations and universals occurring within and between populations can be ascertained (Bein, 2009). By including demographic information, great value has been added to the IS field's knowledge base and understanding of universals and variations that exist among populations.

Table 6.2 below summarises the frequencies of demographic characteristics profiling of clusters.

Table 6 .2: Demographic characteristics profiling in cluster															
Characteristics	**C:1 (N=32)**	**C:2 (N=18)**	**C:3 (N=32)**	**C:4 (N=52)**	**C:5 (N=44)**	**C:6 (N=41)**	**C:7 (N=36)**	**C:8 (N=28)**	**C:9 (N=39)**	**C:10 (N=28)**	**C:11 (N=15)**	**C:12 (N=20)**	**C:13 (N=23)**	**C:14 (N=18)**	**C:15 (N=23)**
Gender															
Male	12 (37.5%)	9 (50%)	18 (56%)	20 (38%)	19 (43%)	14 (34%)	11 (31%)	10 (36%)	13 (33%)	9 (32%)	5 (33%)	7 (35%)	5 (22%)	7 (39%)	10 (43%)
Female	16 (50%)	6 (33%)	12 (37.5%)	26 (50%)	22 (50%)	23 (56%)	18 (50%)	14 (50%)	24 (62%)	15 (54%)	8 (53%)	10 (50%)	13 (56%)	8 (44%)	7 (30%)
Non-binary	4 (12.5%)	3 (17%)	2 (6.5%)	6 (12%)	3 (7%)	4 (10%)	7 (19%)	4 (14%)	2 (5%)	4 (14%)	2 (14%)	3 (15%)	5 (22%)	3 (17%)	6 (27%)
Total	32 (100%)	18 (100%)	32 (100%)	52 (100%)	44 (100%)	41 (100%)	36 (100%)	28 (100%)	39 (100%)	28 (100%)	15 (100%)	20 (100%)	23 (100%)	18 (100%)	23 (100%)
Age															
18-24	7 (22%)	5 (28%)	3 (9%)	6 (11.5%)	4 (9%)	8 (19.5%)	2 (6%)	3 (10.7%)	6 (15%)	1 (4%)	2 (13%)	0 (0%)	3 (13%)	1 (6%)	2 (9%)
25-44	17 (53%)	7 (39%)	18 (56%)	21 (40%)	19 (20.45%)	15 (36.6%)	22 (61%)	10 (35.7%)	12 (30.8%)	8 (28%)	5 (33%)	9 (45%)	15 (65%)	12 (67%)	12 (52%)
45 and above	8 (25%)	6 (33%)	11 (35%)	25 (48.5%)	21 (70.55%)	18 (43.9%)	12 (33%)	15 (53.6%)	21 (54.2%)	19 (68%)	8 (54%)	11 (55%)	5 (22%)	5 (27%)	9 (39%)
Total	32 (100%)	18 (100%)	32 (100%)	52 (100%)	44 (100%)	41 (100%)	36 (100%)	28 (100%)	39 (100%)	28 (100%)	15 (100%)	20 (100%)	23 (100%)	18 (100%)	23 (100%)
Highest Qualification															
National diploma	6 (19%)	3 (17%)	5 (16%)	13 (25%)	7 (16%)	6 (15%)	6 (17%)	4 (14%)	4 (10%)	0 (0%)	1 (7%)	5 (25%)	5 (22%)	4 (22%)	3 (13%)

Bachelor	**3 (9.4%)**	**2 (11%)**	**7 (22%)**	**18 (35%)**	**6 (14%)**	**9 (22%)**	**5 (14%)**	**5 (18%)**	**2 (5%)**	**5 (18%)**	**3 (20%)**	**6 (30%)**	**5 (22%)**	**2 (11%)**	**2 (9%)**
Honours	**7 (22%)**	**3 (17%)**	**6 (19%)**	**11 (21%)**	**21 (48%)**	**8 (20%)**	**7 (19%)**	**4 (14%)**	**16 (41%)**	**11 (39%)**	**4 (27%)**	**2 (10%)**	**5 (22%)**	**5 (28%)**	**11 (48%)**
Master's	**11 (34%)**	**4 (22%)**	**9 (28%)**	**3 (6%)**	**0 (0%)**	**13 (32%)**	**15 (42%)**	**9 (32%)**	**11 (28%)**	**8 (29%)**	**4 (27%)**	**6 (30%)**	**4 (17%)**	**3 (17%)**	**4 (17%)**
Doctorate	**3 (9.4%)**	**5 (28%)**	**4 (12.5%)**	**6 (12%)**	**9 (20.5%)**	**3 (7%)**	**2 (6%)**	**4 (14%)**	**5 (13%)**	**3 (11%)**	**2 (12%)**	**0 (0%)**	**2 (8.5%)**	**3 (17%)**	**1 (4%)**
Certificate	**2 (6.2%)**	**1 (5%)**	**1 (2.5%)**	**1 (1%)**	**1 (1.5%)**	**2 (4%)**	**1 (2%)**	**2 (8%)**	**1 (3%)**	**1 (3%)**	**1 (7%)**	**1 (5%)**	**2 (8.5%)**	**1 (5%)**	**2 (9%)**
Total	**32 (100%)**	**18 (100%)**	**32 (100%)**	**52 (100%)**	**44 (100%)**	**41 (100%)**	**36 (100%)**	**28 (100%)**	**39 (100%)**	**28 (100%)**	**15 (100%)**	**20 (100%)**	**23 (100%)**	**18 (100%)**	**23 (100%)**
Current position															
Manager	**1 (3%)**	**1 (5.5%)**	**0 (0%)**	**3 (6%)**	**2 (5%)**	**1 (2.4%)**	**4 (11%)**	**1 (3.6%)**	**2 (5.13%)**	**1 (3.6%)**	**3 (20%)**	**0 (0%)**	**4 (17.4%)**	**1 (5.5%)**	**3 (13%)**
Hon MP	**1 (3%)**	**3 (17%)**	**1 (3%)**	**0 (0%)**	**0 (0%)**	**0 (0%)**	**1 (2.8%)**	**1 (3.6%)**	**1 (2.6%)**	**0 (0%)**	**0 (0%)**	**2 (10%)**	**1 (4.35%)**	**0 (0%)**	**0 (0%)**
Minister	**0 (0%)**	**1 (5.5.%)**	**1 (3%)**	**0 (0%)**	**2 (5%)**	**0 (0%)**	**1 (2.8%)**	**0 (0%)**	**0 (0%)**	**1 (3.6%)**	**0 (0%)**	**0 (0%)**	**0 (0%)**	**0 (0%)**	**0 (0%)**
IS engineer	**2 (6.25%)**	**0 (0%)**	**1 (3%)**	**2 (4%)**	**5 (11%)**	**2 (5%)**	**1 (2.8%)**	**2 (7.14%)**	**4 (10.26**	**1 (3.6%)**	**1 (6.7%)**	**2 (10%)**	**2 (8.7%)**	**1 (5.5%)**	**2 (8.7%)**
Legal expert	**2 (6.25%)**	**1 (5.5%)**	**2 (6.25%)**	**4 (8%)**	**7 (16%)**	**2 (5%)**	**3 (8.33%)**	**1 (3.6%)**	**3 (7.7%)**	**2 (7.14%)**	**0 (0%)**	**0 (0%)**	**2 (8.7%)**	**4 (22.2%)**	**1 (4.35%)**

CISO	**1 (3%)**	**1 (5.5%)**	**2 (6.25%)**	**3 (6%)**	**5 (11%)**	**3 (7.3%)**	**1 (2.8%)**	**1 (3.6%)**	**2 (5.13%)**	**1 (3.6%)**	**0 (0%)**	**1 (5%)**	**1 (4.35%)**	**0 (0%)**	**0 (0%)**
Cybersecurity specialist	**3 (11.66%)**	**1 (5.5%)**	**2 (6.25%)**	**4 (8%)**	**11 (25%)**	**8 (19.5%)**	**3 (8.33%)**	**6 (21.4%)**	**3 (7.7%)**	**1 (3.6%)**	**0 (0%)**	**0 (0%)**	**2 (8.7%)**	**3 (17%)**	**3 (13%)**
Law enforcement	**2 (6.25%)**	**1 (5.5%)**	**1 (3%)**	**3 (6%)**	**1 (4.6%)**	**3 (7.3%)**	**1 (2.8%)**	**0 (0%)**	**5 (12.8%)**	**1 (3.6%)**	**3 (20%)**	**2 (10%)**	**4 (17.4%)**	**1 (5.5%)**	**3 (13%)**
Fraud specialist	**2 (6.25%)**	**0 (0%)**	**3 (9.4%)**	**2 (4%)**	**1 (4.6%)**	**2 (5%)**	**1 (2.8%)**	**1 (3.6%)**	**5 (12.8%)**	**3 (10.71**	**1 (6.7%)**	**3 (20%)**	**2 (8.7%)**	**1 (5.5%)**	**3 (13%)**
IT expert	**1 (3%)**	**1 (5.5%)**	**3 (9.4%)**	**6 (12%)**	**1 (4.6%)**	**3 (7.3%)**	**4 (11%)**	**2 (7.14%)**	**1 (2.6%)**	**4 (14.3%)**	**1 (6.7%)**	**3 (20%)**	**1 (4.35%)**	**2 (11%)**	**1 (4.35%)**
Academic	**2 (6.25%)**	**1 (5.5%)**	**2 (6.25%)**	**5 (10%)**	**2 (5%)**	**4 (9.75%)**	**5 (14%)**	**3 (10.71%)**	**3 (7.7%)**	**4 (14.3%)**	**2 (13.3%)**	**3 (20%)**	**4 (17.4%)**	**3 (17%)**	**5 (21.74%)**
IT director	**2 (6.25%)**	**0 (0%)**	**1 (3%)**	**3 (6%)**	**1 (4.6%)**	**0 (0%)**	**1 (2.8%)**	**1 (3.6%)**	**1 (2.6%)**	**0 (0%)**	**0 (0%)**	**1 (5%)**	**0 (0%)**	**1 (5.5%)**	**1 (4.35%)**
CIO	**3 (11.66%)**	**0 (0%)**	**2 (6.25%)**	**0 (0.%)**	**1 (4.6%)**	**3 (7.3%)**	**1 (2.8%)**	**1 (3.6%)**	**1 (2.6%)**	**2 (7.14%)**	**1 (6.7%)**	**0 (0%)**	**1 (4.35%)**	**0 (0%)**	**1 (4.35%)**
Systems analyst	**2 (6.25%)**	**2 (11%)**	**3 (9.4%)**	**5 (10%)**	**2 (5%)**	**3 (7.3%)**	**4 (11%)**	**2 (7.14%)**	**4 (10.26**	**3 (10.71**	**1 (6.7%)**	**3 (20%)**	**0 (0%)**	**0 (0%)**	**0 (0%)**
Strategist	**3 (11.66%**	**0 (0%)**	**1 (3%)**	**3 (6%)**	**1 (4.6%)**	**1 (2.4%)**	**0 (0%)**	**1 (3.6%)**	**3 (7.7%)**	**1 (3.6%)**	**1 (6.7%)**	**0 (0%)**	**0 (0%)**	**0 (0%)**	**0 (0%)**

Developer	**1 (3%)**	**0 (0%)**	**1 (3%)**	**4 (8%)**	**1 (4.6%)**	**3 (7.3%)**	**1 (2.8%)**	**0 (0%)**	**1 (2.6%)**	**1 (3.6%)**	**0 (0%)**	**0 (0%)**	**0 (0%)**	**0 (0%)**	**0 (0%)**
Telecoms engineer	**2 (6.25%)**	**3 (17%)**	**4 (12.5%)**	**0 (0%)**	**1 (4.6%)**	**1 (2.4%)**	**2 (5.56%)**	**4 (14.3%)**	**0 (0%)**	**1 (3.6%)**	**0 (0%)**	**0 (0%)**	**0 (0%)**	**1 (5.5%)**	**0 (0%)**
Network engineer	**2 (6.25%)**	**2 (11%)**	**2 (6.25%)**	**5 (10%)**	**0 (0%)**	**2 (5%)**	**2 (5.56%)**	**1 (3.6%)**	**0 (0%)**	**1 (3.6%)**	**1 (6.7%)**	**0 (0%)**	**0 (0%)**	**0 (0%)**	**0 (0%)**
Total	**32 (100%)**	**18 (100%)**	**32 (100%)**	**52 (100%)**	**44 (100%)**	**41 (100%)**	**36 (100%)**	**28 (100%)**	**39 (100%)**	**28 (100%)**	**15 (100%)**	**20 (100%)**	**23 (100%)**	**18 (100%)**	**23 (100%)**
Working experience															
<1 year	**1 (3%)**	**2 (11%)**	**1 (3%)**	**0 (0%)**	**0 (0%)**	**0 (0%)**	**1 (3%)**	**1 (3.6%)**	**1 (2.6%)**	**1 (3.6%)**	**0 (0%)**	**0 (0%)**	**0 (0%)**	**0 (0%)**	**0 (0%)**
1-5 years	**11 (34.4%)**	**9 (50%)**	**17 (53.1%)**	**8 (15.4%)**	**14 (32%)**	**17 (41.5%)**	**14 (39%)**	**9 (32%)**	**7 (18%)**	**6 (21.4%)**	**9 (60%)**	**5 (25%)**	**12 (52.2%)**	**4 (22.2%)**	**3 (13%)**
6-10 years	**12 (37.5%)**	**1 (5.5%)**	**5 (15.63%)**	**23 (44%)**	**16 (36.4%)**	**13 (32%)**	**11 (31%)**	**8 (29%)**	**12 (31%)**	**11 (39.3%)**	**3 (20%)**	**8 (40%)**	**6 (26.1%)**	**7 (38.9%)**	**8 (34.8%)**
11-20 years	**6 (18.75%)**	**2 (11%)**	**9 (28.13%)**	**15 (29%)**	**11 (25%)**	**8 (20%)**	**6 (17%)**	**6 (21.4%)**	**11 (28.2%)**	**5 (18%)**	**2 (13.3%)**	**3 (15%)**	**4 (17.4%)**	**4 (22.2%)**	**7 (30.4%)**
21 and above years	**2 (6.25%)**	**44 (22.2%)**	**0 (0%)**	**6 (11.5%)**	**3 (6.82%)**	**3 (7.3%)**	**4 (11%)**	**4 (14.3%)**	**8 (20.2%)**	**5 (18%)**	**1 (6.7%)**	**4 (20%)**	**1 (4.35%)**	**3 (16.67%)**	**5 (21.74%)**
Total	**32 (100%)**	**18 (100%)**	**32 (100%)**	**52 (100%)**	**44 (100%)**	**41 (100%)**	**36 (100%)**	**28 (100%)**	**39 (100%)**	**28 (100%)**	**15 (100%)**	**20 (100%)**	**23 (100%)**	**18 (100%)**	**23 (100%)**
Ethnicity															

Black	**11 (34.4%)**	**9 (50%)**	**13 (40.6%)**	**21 (40.4%)**	**16 (36.4%)**	**18 (44%)**	**13 36%)**	**14 (50%)**	**11 (28%)**	**13 (46.43**	**7 (47%)**	**8 (40%)**	**10 (43.5%)**	**7 (39%)**	**11 (48%)**
White	**6 (18.75%)**	**4 22%)**	**6 (18.8%)**	**18 (34.6%)**	**14 (31.8%)**	**9 (22%)**	**4 (11.1%)**	**3 (10.7%)**	**6 (15.4%)**	**2 (7.14%)**	**3 (20%)**	**6 (30%)**	**3 (13%)**	**2 (11.1%)**	**5 (21.8%)**
Indian	**4 (12.5%)**	**3 (16.7%)**	**3 (9.4%)**	**7 (21.9%)**	**6 (13.64%)**	**9 (22%)**	**7 (19.4%)**	**3 (10.7%)**	**3 (7.7%)**	**6 (21.43**	**2 (13.3%)**	**1 (5%)**	**1 (4.35%)**	**2 (11.1%)**	**2 (8.7%)**
Coloured	**5 (15.6%)**	**1 (5.5%)**	**6 (18.8%)**	**3 (11.5%)**	**4 (9.1%)**	**3 (7.3%)**	**3 (8.33%)**	**2 (7.14%)**	**12 (30.8%)**	**5 (18%)**	**3 (20%)**	**5 (25%)**	**6 (26.1%)**	**3 (16.7%)**	**2 (8.7%)**
Asian	**4 (12.5%)**	**1 (5.5%)**	**3 (9.4%)**	**3 (11.5%)**	**2 (4.55%)**	**1 (2.44%)**	**8 (22.2%)**	**6 (21.43%)**	**7 (18%)**	**2 (7.14%)**	**0 (0%)**	**0 (0%)**	**2 (8.7%)**	**1 (5.5%)**	**2 (8.7%)**
Other	**3 (9.4%)**	**0 (0%)**	**1 (3.13%)**	**0 (0%)**	**2 (4.55%)**	**1 (2.44%)**	**1 (2.8%)**	**0 (0%)**	**0 (0%)**	**0 (0%)**	**0 (0%)**	**0 (0%)**	**1 (4.35%**	**3 (16.7%)**	**1 (4.35%)**
Total	**32 (100%)**	**18 (100%)**	**32 (100%)**	**52 (100%)**	**44 (100%)**	**41 (100%)**	**36 (100%)**	**28 (100%)**	**39 (100%)**	**28 (100%)**	**15 (100%)**	**20 (100%)**	**23 (100%)**	**18 (100%)**	**23 (100%)**

***C stands for Cluster**

** The number of respondents are shown in the upper rows while, the corresponding percentages are shown underneath*

6.4 Cluster Profiles of Influencing Factors (patterns)

Table 6.3 below summarises the values for all the nine influencing factors for the cluster solutions. This section presents and discusses the findings for each cluster.

6.4.1 Understanding Cybersecurity (CS)

Respondents Cluster 7 (39%) and Cluster 13 (39.1%) had the highest number of female respondents who agreed that there was an overreliance on ICTs (Q8). Male respondents in Cluster 1 (37.5%), Cluster 2 (39%), Cluster 3 (40.6%), Cluster 5 (41%) and Cluster 15 (52.1%) who were Cybersecurity, Academic and IT experts where they agreed that there was limited understanding of cybersecurity (Q9). Cluster 14 (39%) respondents of the Black ethnic group and with more than 10 years working experience agreed that people failed to understand cybersecurity because of the conflicting terminology that was used (Q10). Cluster 8 (68%) who were mainly female respondents aged 25-44 years agreed that lack of information sharing (Q11) contributed to misunderstanding of cybersecurity. When combined together, respondents in all clusters agreed that people, businesses- private or public, had limited understanding of cybersecurity which ultimately affected their state of preparedness. The number of cyber-attacks and threats and duration of working experience was pertinent for the respondents to concur that there was a general misunderstanding of cybersecurity (Cluster 2; Cluster 9 and Cluster 15 (see Table 6.2)) had more than 21 years working experience in various IT roles within the domain cybersecurity. These findings corroborate Selebalo (2014), van der Merwe et al.'s (2016) and Bote (2019)'s assertions that lack of information sharing or education and awareness programmes contribute significantly to people's understanding of cybercrimes. Malatji et al. (2021) state that silo approaches to addressing cybercrimes created gaps for sharing information which is pertinent to the country if South Africa has to achieve its cybersecurity goals. While it is a good idea to share information, the researcher is cautious to the type, degree of sensitivity and channels of sharing information.

The results are also corroborated by Canhoto (2010) who established that lack of understanding of cybercrimes creates confusion and hinders rapid responses in the event of violation of laws. While Kyobe et al. (2012) assert that lack of understanding of cybercrime is prolonged by conflicting and ambiguous interpretation of the term "cybercrime". Information asymmetries occurs when one party to a transaction has better information than the other party. Given the context of the regulatory environment in the country, one government agency might have better

or withholds information from the other agencies. This could be attributed to bureaucratic and hierarchical political structures and policies that forbids sharing of data security information. Power play politics tend to favour the influential and well-connected individuals. While sharing information, companies or civil society should cognisant that the information might get into threat actors who might leverage on that information leading to the commission of complex cybercrimes.

6.4.2 Law-making process (LMPRE)

The South African law-making process was perceived to be slow and time consuming as demonstrated by high responses in Cluster 1(47%) who were Black and White academics with more than 11 years working, Cluster 5 (47.74%) were mostly male law enforcement and fraud specialists with more than 5 years' experience and Cluster 11 (53.3%) comprising legal and IT experts(Q12). Cluster 10 (39.3%)- cybersecurity and legal experts with more than 11 years working experience and Cluster 14 (44%) mostly female respondents agreed that inconsistencies of approaches in addressing cybercrimes contributed to the misalignment of national laws (Q14). Respondents in Cluster 4(30.8%) Coloured and Asian ethnic groups, Cluster 7 (33.3%) systems analysts and fraud specialists and Cluster 10 (30%) Ministers and Members of Parliament (respondents) confirmed that fragmented and misaligned pieces of legislation (Q16) played a major role in how the country's cyberlaws were developed and enacted into Bills of Parliament. Cluster 3 (34.4%) who were mostly Members of Parliament, Cluster 12 (35%) academics and Cluster 15 (39.1%) legal and IT experts (respondents) agreed that the law-making process was affected by lawmakers' lack of adequate knowledge of the law-making process itself (Q18). The overall consensus from respondents was that the country's law-making process was slow, time-consuming. This is consistent with the findings of Bateman (2013), Selebalo (2014) and Johnson (2017) who indicate that depending with the urgency with which the law-makers want the Bill to enacted into law, the normal process can take between 3 months to more than 12 months to have the Bill passed and enacted into an Act of Parliament. Chigada and Kyobe (2018) posit that there seems to be repetitions in the reading and debating of Bills between the NCOPs and NA, which might degenerate into conflicts, thus, stifling the law-making process. Claassen *et al.* (2012) agree with the respondents that bureaucratic processes in passing Bills is a major hindrance to the misalignment of the NCPF.

6.4.3 Coordination of legislation (MAIS)

Different government departments were mandated to coordinate various pieces of legislation, however, the agencies/departments' mandates overlapped, often creating conflicts resulting in poor coordination of the laws. Cluster 1 (40.6%) mostly legal experts, Cluster 11 (53.3%) academics and Cluster 12 (65%) female respondents with less than 5 years working experience agreed that overlapping mandates create inconsistencies which resulted in poor coordination of legislation (Q19). Predominantly cybersecurity experts, systems and telecommunications engineers in Cluster 7 (41.7%) and Chief Information Officers and Chief Information Security Officers in Cluster 8 (71.4%) respondents indicated that the most challenging aspect of SA legislation was that each law addressed a specific aspect of cybersecurity which leaves room for disharmony (Q20). Exacerbating the misalignment challenge was the lack of sharing of strategies among the coordinators of various legislation. This was indicated by respondents mostly of Indian and Asian ethnic groups in Cluster 3 (28%) and managers with less than 10 years working experience in Cluster 4 (32.7%) for Q21 and Q22 respectively. The overall viewpoint was that the presence of multiple government agencies meant multiple information systems which were fragmented, thus, poor coordination occurred due to overlapping mandates. These results confirm findings by Pistorius (2009), Mahlobo (2015), Schultz (2016), van der Merwe (2016) and Maja *et al.* (2021) who concur with each other that the country's NCPF would yield the desired objectives because of fragmented and incoherent legislation. In addition, these pieces of legislation focus on a specific type of cybercrime, thus, would require the interpretation of another piece of legislation to successfully prosecute cybercriminals. For example, common law can be overridden at any given time by legislation because Parliament is the supreme law-making body (Parliament of South Africa, 2019). Other forms of legislation discussed in chapter 3 demonstrate what type of cybercrimes each of them addresses and the weaknesses thereof.

6.4.4 Monitoring and Control (MC)

Mechanisms for monitoring and controlling information systems security protocols should be devised and implemented in line with the availability of the country's or organisation's resources. Systems and telecoms engineers in Cluster 3 (37.5%), systems analysts in Cluster 4 (40.4%), female respondents (45 years and above) in Cluster 5 (38.64%) and Cluster 12 (40%) mostly developers indicated that most government institutions mandated to coordinate cyberlaws, do not have adequate controls and information systems security protocols, which

leave their own IT assets exposed. Respondents indicated that intrusion detection systems help to curb unauthorised access to data and information technology infrastructure (Q26). IT experts and cybersecurity specialists respondents- Cluster 1 (40.6%), Black telecoms engineers-Cluster 2 (44%) and Cluster 7 (50%) mostly male IT directors indicated that it was difficult to determine which security controls were effective when multiple agencies and information systems were use (Q28). When combined together, respondents perceived that the absence of controls and protocols weaken an NCS, while intrusion detection systems were perceived to reduce unauthorised access to data and information systems. These results are in line with the findings of Kuhlman and Kempf (2015) who recommend the implementation of independent security controls through the organisation's technology system. While Galine *et al.* (2017) suggest a proper cybersecurity risk assessment to identify security weaknesses and likely risks posed by third-party vendors. In Ajala's (2007) findings, it was established that adopting a cybersecurity risk assessment program is a clear indication of the organisation's commitment to containing and addressing cybercrimes.

6.4.5 IT and Legal Skills in Cybersecurity (SIC)

Cluster 8 (46.4%) respondents of the Asian ethnic group and legal experts indicated that the shortage of IT and legal skills/expertise the law-making process because without these skills, government might enlist the services of external consultants, who in most instances do not understand the country's way of doing business (Q30). While Members of Parliament- Cluster 3 (40.6%) and Cybersecurity specialists-Cluster 13 (43.5%) respondents perceive the co-existence of multiple government agencies and replica information systems depletes the few available IT and legal skills in cybersecurity (Q31). Cluster 15 (56.5%) mostly CISOs and CIOs with vast cybersecurity experience indicated that technology is advancing at an accelerated rate, thus, cybercriminals are operating in tandem with the latest trends. IT specialists are therefore, outpaced by sophisticated cybercriminals (Q32). There is a general agreement among all respondents that expanding cyber education would help address the shortage of IT and legal skills prevailing (Q34). This was indicated by Ministers, Managers and Members of Parliament- Cluster 11 (46.7%).

There is a general perception among all respondents that the shortage in IT and legal skills in cybersecurity affects the development of an effective NCS and ability to respond proactively to exponential growth of sophisticated cybercrimes. South Africa, like most developing

economies has a critical shortage of IT skills, thus, cybercriminals outpace cybersecurity experts because they know the skills deficiencies in the country. Respondents agreed that appointing the right people at every level in the organisation, helps to identify, build staff defences and responses (Q34). The results corroborate with Brown (2010) who states the need for management to identify cybersecurity training needs, loss incidents training requirements and risk assessment processes in line with firm's cybersecurity management policies. The absence of cybersecurity training can expose a firm's increased risks of successful cybersecurity attacks and threats (Chang & Coppel, 2020).

6.4.6 Knowledge and Information Sharing (KIS)

Knowledge and information sharing are key ingredients for understanding the law-making process, cyberspace trends and how other organisations or governments respond to threats and attacks. Cluster 3 (40.6%) male respondents, Cluster 4 (36.5%) Ministers, Cluster 5 (36.4%) Members of Parliament, Cluster 9 (38.5%) academics with more than 5 years working experience, Cluster 11 (40%) fraud specialists and Cluster 12 (45%) Coloured ethnicity respondents agreed that there are persistent silo approaches to knowledge and information sharing, which permeate in institutions coordinating cyberlaws (Q35). CIOs and CISOs in Cluster 13 (48%) echoed similar statements when they indicated that these government agencies fear to expose state secrets or information, thus, would not be at liberty to share knowledge and information (Q37). The fear of exposing intellectual property was also highlighted as an impediment to knowledge and information sharing (Q38) by Black- Cluster 10 (53.6%), Cybersecurity specialists- Cluster 13 (52.1%) and White respondents- Cluster 14 (94.4%) respectively. Thus, lack of information sharing was perceived by respondents as a huge impediment to understanding cybercrimes (see Table 6.3). In support of the results, Mahlobo (2015) and Malatji *et al.* (2021) state that some South African legislation is fragmented and inconsistent with regional and international cyberlaws.

For example, cybercriminals commit crime in South Africa while based in Zimbabwe, it would be difficult to detect and prosecute them because South African cyberlaws are not harmonised with Zimbabwean laws let alone SADC cyberlaws. This could partly be caused by the two countries or SADC countries' failure to share information related to cybercrimes. SABRIC (2019) suggests that firms operating in the same industry could establish a body that collates, collects and disseminate cybersecurity information to its stakeholders with the objective of keeping abreast with trends. However, the challenge with multiple agencies' failure to share

information is to protect intellectual property (SSA, 2015). Kyobe *et al*. (2012) aver that sharing of cybersecurity information helps society, business and government to respond rapidly to cyber-attacks.

6.4.7 User Behaviour (PICL)

People behave in certain ways that can stifle the development and implementation of laws (Q40). This viewpoint was argued by legal and IT expert respondents in Cluster 12 (50%) and law enforcement agencies respondents in Cluster 15 (52.1%) respectively. Unacceptable behaviour can lead managers to remove certain people from some tasks, creating a shortage of resources (Q42) as indicated by the Black respondents with master's degrees-Cluster 4 (50%). Network and system engineers with less than 10 years' experience indicated that unacceptable user behaviour manifested through resistance to change, thus, slowing down the process of making laws as well as adaptation pace (Q43). This response was reported by Cluster 5 (45.5%) mostly female respondents and academics whose working experience was less than 5 years working experience-Cluster 6 (44%). The results are supported by Khan *et al*. (2020) who established that unacceptable human behaviour is a manifestation of the absence or presence of a weak cybersecurity culture, hence, the prevalence of cyber-attacks and human errors in the workplace. In addition, when users abandon security policies without punishment, this clearly demonstrates the absence of or a weak cybersecurity culture. Abukari and Bankas (2020) state that organisations lose information assets through unethical and unacceptable employee behaviour because employees understand the weaknesses of their organisation's cybersecurity governance structures. While the WEF (2020) avers that organisations are placing too much emphasis on human intelligence which might result in the firm overlooking the individual person's ethical conduct. Chigada (2020) asserts that individuals study existing cybersecurity practices in the firm, identifies weakest links and commit crime with the full knowledge that their actions might not be detected by the firm. Cluster 10 (53.6%) mostly Asian ethnic group disagreed that resistance to change slowed a number of initiatives especially projects dealing with the protection of the national information technology infrastructure (Q43).

6.4.8 A Cybersecurity Culture (CSC)

Cluster 8 (25%) mostly managers agreed that many organisations overerly on ICTs, therefore, there were enough grounds for organisational leadership to develop a cybersecurity culture (Q44). In support of Cluster 8 respondents, CIOs and academics in Cluster 13 (48%) indicated

that a cybersecurity culture was sustainable because it transforms security from a one-time event into a lifecycle (Q45). Due to the rapid technological innovations, firms needed a cybersecurity culture that adapts qucikly to change and fosters better security (Q46) as indicated by legal experts respondents-Cluster 6 (36.6%) and network engineer respondents in Cluster 15 (39.1%) who agreed that a strong cybersecurity culture defines how security influences the services that a firm provides to its stakeholders (Q47). These results are corroborated by Kerman and Pearlson (2019) who state that unacceptable human behaviour can be reined in if an organisation implements stringent cybersecurity policies and governance structures to guide employee behaviour and increase cyber resilience. By so doing, the organisation will be recognising the role of developing effective cybersecurity controls. However, Gcaza and von Solms (2017) aver that due to lack of a widely accepted understanding of cybersecurity culture, many organisations and people believe that cybersecurity culture is still in its infancy, thus, its effects in terms of improving security cannot be quantified. Cluster 1 (25%) mainly White respondents and Cluster 14 (33.3%) mostly CIOs respondents disagreed that modern security culture enables to work in a way they want, inside or outside the corporate network (Q48). This means that respondents' conduct is guided by ethical behaviour.

Boucher *et al*. (2019) support respondents' perceptions that users can work the way they want, inside or outside the organisation under the guidance of an effective cybersecurity culture. The authors state that if an organisation's top management is committed to a cybersecurity culture and improving cyber attitudes of its employees and promoting accountability, therefore, users can work the way they want, inside and or outside the organisation. From an ethical perspective, whether being monitored or not, information system users should act in such a way that they are accountable (Dlamini, 2020). All computer-mediated activities can be monitored; thus, users are conscientious of the ramifications of unethical conduct.

6.4.9 Coherent Cyberlaws (EGCL)

The existence of many national, regional and global pieces of legislation hinders the pace at which laws are developed and enacted. There is a possibility that multiple global cyberlaws might exarcerbate the incoherence and fragmentation of national laws. This could be through misintepretation, limited understanding or lack of legal skills. This was confirmed by legal experts in Cluster 10 (35.8%) who agreed that the existence of multiple global cyberlaws creates confusion and inconsistencies especially if the policy makers are in the process of making a new law. The interpretation of new laws might override current processes (Q51). IT

experts in Cluster 2 (50%) disagreed that the unprecedented rate of technological developments creates challenges in the formulation of new laws and amendments of existing ones from time to time (Q52). Cluster 1 (40.6%) male respondents and Cluster 12 (45%) mainly Coloured respondents agreed that due to the sophisticatio of cybercrimes, new legislation were developed, thus, putting pressure on developing or resource constrained economies to adapt and develop new laws at a faster pace to keep abreats with cybercrime trends (Q53). This was confirmed by the WHO (2020) and UN (2020) state that cybercrimes are increasingly becoming sophisticated each passing day due to rapid technological advancements. Thus, there is a huge challenge for the global economy and governments to develop new cyberlaws at the same pace as the emergence of new cybercrimes. Cluster 4 (36.5%) mostly fraud specialists and Cluster 11 (46.7%) mostly of the Asian ethnic group agreed that cybercrimes are perpetrated through the use of BYOD, therefore, it is becoming increasingly important to develop BYOD to mitigate cyber-attacks and threats (Q54). However, respondents in Cluster 3 (49.6%) IT directors and Cluster 8 (32.1%) IS engineers and Cluster 15 (26%) respondents of the White ethnicity did not with the view that the increased usage of mobile devices, mobile law emerges was an area of jurisprudence (Q55).

Table 6.3 below summarises the cluster frequencies for each influencing factor

Table 6 .3: Cluster Profiles of Influencing Factors															
Research Question	**C:1 (N=32)**	**C:2 (N=18)**	**C:3 (N=32)**	**C:4 (N=52)**	**C:5 (N=44)**	**C:6 (N=41)**	**C:7 (N=36)**	**C:8 (N=28)**	**C:9 (N=39)**	**C:10 (N=28)**	**C:11 (N=15)**	**C:12 (N=20)**	**C:13 (N=23)**	**C:14 (N=18)**	**C:15 (N=23)**
CS															
Q8	**6 (18.75%**	**4 (22.2%)**	**3 (9.4%)**	**9 (17.3%)**	**1 (2.3%)**	**0 (0%)**	**14 (39%)**	**6 (21.4%)**	**10 (26%)**	**9 (32.1%)**	**5 (33.3%**	**7 (35%)**	**9 (39.1%)**	**4 (22.2%**	**5 (21.74%**
Q9	**12 (37.5%)**	**7 (39%)**	**13 (40.6%)**	**13 (25%)**	**18 (41%)**	**13 (31.7%)**	**6 (16.7%)**	**3 (10.7%)**	**8 (20.5%)**	**6 (21.4%)**	**3 (20%)**	**6 (30%)**	**4 (17.4%)**	**2 (11.1%**	**12 (52.1%)**
Q10	**11 (34.4%)**	**3 (16.7%)**	**9 (28%)**	**16 (30.8%)**	**17 (38.64%)**	**18 (44%)**	**13 (36.1%)**	**0 (0%)**	**11 (28.2%)**	**5 (17.9%)**	**4 (26.7%**	**3 (15%)**	**4 (17.4%)**	**7 (39%)**	**4 (17.4%)**
Q11	**3 (9.4%)**	**4 (22.2%)**	**7 (22%)**	**14 (27%)**	**8 (18.2%)**	**10 (24.5%)**	**3 (7.3%)**	**19 (68%)**	**10 (26%)**	**8 (28.6%)**	**3 (20%)**	**4 (20%)**	**6 (26%)**	**5 (28%)**	**2 (8.7%)**
Total	**32 (100%)**	**18 (100%)**	**32 (100%)**	**52 (100%)**	**44 (100%)**	**41 (100%)**	**36 (100%)**	**28 (100%)**	**39 (100%)**	**28 (100%)**	**15 (100%)**	**20 (100%**	**23 (100%)**	**18 (100%)**	**23 (100%)**
LMPRE															
Q12	**15 (47%)**	**5 (28%)**	**8 (25%)**	**15 (29%)**	**21 (47.73%)**	**14 (34.1%)**	**5 (13.9%)**	**7 (25%)**	**16 (41%)**	**4 (14.4%)**	**8 (53.3%**	**0 (0%)**	**7 (30.4%)**	**3 (16.7%**	**5 (21.74%**
Q14	**2 (6.25%)**	**6 (33.3%)**	**4 (12.5%)**	**7 (13.5%)**	**10 (22.73%)**	**9 (22%)**	**13 (36.1%)**	**6 (21.4%)**	**9 (23.1%)**	**11 (39.3%)**	**3 (20%)**	**7 (35%)**	**6 (26%)**	**8 (44%)**	**3 (13%)**

Q16	**8 (25%)**	**3 (16.7%)**	**9 (28%)**	**16 (30.8%)**	**4 (9.1%)**	**11 (27%)**	**12 (33.3%)**	**7 (25%)**	**10 (26%)**	**9 (32.1%)**	**2 (13.3%**	**6 (30%)**	**5 (21.74%**	**3 (16.7%**	**6 (26%)**
Q18	**7 (22%)**	**4 (22.2%)**	**11 (34.4%)**	**14 (27%)**	**9 (20.5%)**	**7 (17.1%)**	**6 (16.7%)**	**8 (28.6%)**	**4 (10.3%)**	**4 (14.4%)**	**2 (13.3%**	**7 (35%)**	**5 (21.74%**	**4 (22.2%**	**9 (39.1%)**
Total	**32 (100%)**	**18 (100%)**	**32 (100%)**	**52 (100%)**	**44 (100%)**	**41 (100%)**	**36 (100%)**	**28 (100%)**	**39 (100%)**	**28 (100%)**	**15 (100%)**	**20 (100%**	**23 (100%)**	**18 (100%)**	**23 (100%)**
MAIS															
Q19	**13 (40.6%)**	**7 (39%)**	**6 (18.75%)**	**11 (21.2%)**	**15 (34.1%)**	**8 (19.5%)**	**1 (2.8%)**	**0 (0%)**	**11 (28.2%)**	**33 (10.7%)**	**8 (53.3%**	**13 (65%)**	**9 (39.1%)**	**5 (28%)**	**7 (30.4%)**
Q20	**3 (9.4%)**	**5 (28%)**	**4 (12.5%)**	**9 (17.3%)**	**13 (29.55%)**	**12 (29.3%)**	**15 (41.7%)**	**20 (71.4%)**	**14 (36%)**	**11 (39.3%)**	**2 (13.3%**	**2 (10%)**	**6 (26%)**	**33 (16.7%**	**5 (21.74%**
Q21	**7 (22%)**	**2 (11.1%)**	**9 (28%)**	**17 (32.7%)**	**11 (25%)**	**7 (17.1%)**	**7 (19.4%)**	**3 (10.7%)**	**8 (20.5%)**	**5 (17.9%)**	**0 (0%)**	**2 (10%)**	**5 (21.74%**	**3 (16.7%**	**4 (17.4%)**
Q22	**9 (28%)**	**2 (11.1%)**	**5 (15.6%)**	**5 (9.6%)**	**3 (6.8%)**	**9 (22%)**	**5 (13.9%)**	**2 (7.14%)**	**2 (5.1%)**	**7 (25%)**	**3 (20%)**	**2 (10%)**	**1 (4.35%)**	**4 (22.2%**	**5 (21.74%**
Q24	**0 (0%)**	**2 (11.1%)**	**8 (25%)**	**10 (19.2%)**	**2 (4.55%)**	**5 (12.2%)**	**8 (22.2%)**	**3 (10.7%)**	**4 (10.3%)**	**2 (7.14%)**	**2 (13.3%**	**1 (5%)**	**2 (8.7%)**	**3 (16.7%**	**2 (8.7%)**

Total	**32 (100%)**	**18 (100%)**	**32 (100%)**	**52 (100%)**	**44 (100%)**	**41 (100%)**	**36 (100%)**	**28 (100%)**	**39 (100%)**	**28 (100%)**	**15 (100%)**	**20 (100%**	**23 (100%)**	**18 (100%)**	**23 (100%)**
MC															
Q25	**9 (28%)**	**5 (28%)**	**12 (37.5%)**	**21 (40.4%)**	**17 (38.64%)**	**13 (31.7%)**	**4 (11.1%)**	**7 (25%)**	**13 (33.3%)**	**10 (35.8%)**	**4 (26.7%**	**8 (40%)**	**6 (26%)**	**6 (33.3%**	**7 (30.4%)**
Q26	**10 (31.25%**	**5 (28%)**	**11 (34.4%)**	**11 (21.2%)**	**13 (29.55%)**	**16 (39%)**	**14 (38.9%)**	**12 (43.9%)**	**14 (36%)**	**4 (14.4%)**	**6 (40%)**	**5 (25%)**	**11 (48%)**	**6 (33.3%**	**12 (52.1%)**
Q28	**13 (40.6%)**	**8 (44%)**	**9 (28%)**	**20 (38.4%)**	**14 (31.82%)**	**12 (29.3%)**	**18 (50%)**	**9 (32.1%)**	**12 (30.8%)**	**14 (50%)**	**5 (33.3%**	**7 (35%)**	**6 (26%)**	**6 (33.3%**	**4 (17.4%)**
Total	**32 (100%)**	**18 (100%)**	**32 (100%)**	**52 (100%)**	**44 (100%)**	**41 (100%)**	**36 (100%)**	**28 (100%)**	**39 (100%)**	**28 (100%)**	**15 (100%)**	**20 (100%**	**23 (100%)**	**18 (100%)**	**23 (100%)**
SIC															
Q30	**5 (15.6%)**	**4 (22.2%)**	**9 (28%)**	**12 (23.1%)**	**16 (36.4%)**	**8 (19.5%)**	**11 (15.3%)**	**13 (46.4%)**	**15 (38.5%)**	**9 (32.1%)**	**6 (40%)**	**5 (25%)**	**6 (26%)**	**7 (39%)**	**2 (8,7%)**
Q31	**12 (37.5%)**	**5 (28%)**	**13 (40.6%)**	**2 (3.8%)**	**5 (11.4%)**	**7 (17.1%)**	**4 (11.1%)**	**6 (21.4%)**	**11 (28.2%)**	**0 (0%)**	**0 (0%)**	**5 (25%)**	**10 (43.5%)**	**4 (22.2%**	**0 (0%)**
Q32	**6 (18.75%**	**3 (16.7%)**	**7 (22%)**	**8 (15.4%)**	**12 (27.3%)**	**9 (22%)**	**13 (36.1%)**	**8 (28.6%)**	**5 (12.8%)**	**5 (17.9%)**	**1 (6.7%)**	**5 (25%)**	**4 (17.4%)**	**3 (16.7%**	**13 (56.5%)**

Q33	**7 (22%)**	**3 (16.7%)**	**1 (3.1%)**	**19 (36.5%)**	**4 (9.1%)**	**13 (31.7%)**	**3 (7.3%)**	**0 (0%)**	**2 (5.1%)**	**4 (14.4%)**	**1 (6.7%)**	**4 (20%)**	**1 (4.35%_**	**2 (11.1%**	**3 (13%)**
Q34	**2 (6.25%)**	**3 (16.7%)**	**2 (6.25%)**	**11 (21.2%)**	**7 (16%)**	**4 (9.8%)**	**5 (13.9%)**	**1 (3.6%)**	**6 (15.4%)**	**10 (35.8%)**	**7 (46.7%**	**1 (5%)**	**2 (8.7%)**	**2 (11.1%**	**5 (21.74%**
Total	**32 (100%)**	**18 (100%)**	**32 (100%)**	**52 (100%)**	**44 (100%)**	**41 (100%)**	**36 (100%)**	**28 (100%)**	**39 (100%)**	**28 (100%)**	**15 (100%)**	**20 (100%**	**23 (100%)**	**18 (100%)**	**23 (100%)**
KIS															
Q35	**9 (28%)**	**6 (33.3%)**	**13 (40.6%)**	**19 (36.5%)**	**16 (36.4%)**	**9 (22%)**	**11 (15.3%)**	**10 (35.8%)**	**15 (38.5%)**	**3 (10.7%)**	**6 (40%)**	**9 (45%)**	**0 (0%)**	**1 (5.5%)**	**8 (35%)**
Q37	**12 (37.5%)**	**5 (28%)**	**9 (28%)**	**18 (34.6%)**	**15 (34.1%)**	**14 (34.1%)**	**13 (36.1%)**	**9 (32.1%)**	**13 (33.3%)**	**10 (35.8%)**	**4 (26.7%**	**5 (25%)**	**11 (48%)**	**0 (0%)**	**7 (30.4%)**
Q38	**11 (34.4%)**	**7 (39%)**	**10 (31.25%)**	**15 (28.8%)**	**13 (29.55%)**	**18 (44%)**	**12 (33.3%)**	**9 (32.1%)**	**11 (28.2%)**	**15 (53.6%)**	**5 (33.3%**	**6 (30%)**	**12 (52.1%**	**17 (94.4%**	**8 (35%)**
Total	**32 (100%)**	**18 (100%)**	**32 (100%)**	**52 (100%)**	**44 (100%)**	**41 (100%)**	**36 (100%)**	**28 (100%)**	**39 (100%)**	**28 (100%)**	**15 (100%)**	**20 (100%**	**23 (100%)**	**18 (100%)**	**23 (100%)**
PICL															
Q40	**7 (22%)**	**5 (28%)**	**12 (37.5%)**	**10 (19.2%)**	**13 (29.55%)**	**9 (22%)**	**12 (33.3%)**	**5 (17.9%)**	**13 (33.3%)**	**6 (21.4%)**	**4 (26.7%**	**10 (50%)**	**9 (39.1%)**	**6 (33.3%**	**12 (52.1%**

Q42	**10 (31.25%**	**7 (39%)**	**10 (31.25%)**	**26 (50%)**	**11 (25%)**	**14 (34.1%)**	**12 (33.3%)**	**13 (46.4%)**	**14 (36%)**	**7 (25%)**	**5 (33.3%**	**8 (40%)**	**7 (30.4%)**	**7 (39%)**	**9 (39.1%)**
Q43	**11 (34.4%)**	**6 (33.3%)**	**10 (31.25%)**	**16 (30.8%)**	**20 (45.5%)**	**18 (44%)**	**12 (33.3%)**	**10 (35.8%)**	**12 (30.8%)**	**15 (53.6%)**	**6 (40%)**	**2 (10%)**	**7 (30.4%)**	**5 (28%)**	**2 (8.7%)**
Total	**32 (100%)**	**18 (100%)**	**32 (100%)**	**52 (100%)**	**44 (100%)**	**41 (100%)**	**36 (100%)**	**28 (100%)**	**39 (100%)**	**28 (100%)**	**15 (100%)**	**20 (100%**	**23 (100%)**	**18 (100%)**	**23 (100%)**
CSC															
Q44	**5 (15.6%)**	**3 (16.7%)**	**7 (22%)**	**12 (23.1%)**	**9 (20.5%)**	**0 (0%)**	**6 (16.7%)**	**7 (25%)**	**5 (12.8%)**	**3 (10.7%)**	**3 (20%)**	**6 (30%)**	**2 (8.7%**	**4 (22.2%**	**4 (17.4%)**
Q45	**6 (18.75%**	**6 (33.3%)**	**6 (18.75%)**	**17 (32.7%)**	**8 (18.2%)**	**14 (34.1%)**	**5 (13.9%)**	**11 (39.3%)**	**9 (23.1%)**	**10 (35.8%)**	**3 (20%)**	**3 (15%)**	**11 (48%)**	**2 (11.1%**	**4 (17.4%)**
Q46	**4 (12.5%)**	**3 (16.7%)**	**9 (28%)**	**11 (21.2%)**	**12 (27.3%)**	**15 (36.6%)**	**7 (19.4%)**	**5 (17.9%)**	**13 (33.3%)**	**5 (17.9%)**	**3 (20%)**	**5 (25%)**	**3 (13%)**	**5 (28%)**	**3 (13%)**
Q47	**9 (28%)**	**3 (16.7%)**	**7 (22%)**	**5 (9.6%)**	**7 (16%)**	**11 (26.8%)**	**10 (28%)**	**2 (7.14%)**	**3 (7.7%)**	**5 (17.9%)**	**3 (20%)**	**4 (20%)**	**2 (8.7%**	**1 (5.5%)**	**9 (39.1%)**
Q48	**8 (25%)**	**3 (16.7%)**	**3 (9.4%)**	**7 (13.5%)**	**8 (18.2%)**	**1 (2.44%)**	**8 (22.2%)**	**3 (10.7%)**	**9 (23.1%)**	**5 (17.9%)**	**3 (20%)**	**2 (10%)**	**5 (21.74%**	**6 (33.3%**	**3 (13%)**
Total	**32 (100%)**	**18 (100%)**	**32 (100%)**	**52 (100%)**	**44 (100%)**	**41 (100%)**	**36 (100%)**	**28 (100%)**	**39 (100%)**	**28 (100%)**	**15 (100%)**	**20 (100%**	**23 (100%)**	**18 (100%)**	**23 (100%)**

EGCL															
Q51	**3 (9.4%)**	**4 (22.2%)**	**5 (15.6%)**	**15 (28.8%)**	**9 (20.5%)**	**12 (29.3%)**	**5 (13.9%)**	**1 (3.6%)**	**3 (7.7%)**	**10 (35.8%)**	**4 (26.7%**	**4 (20%)**	**3 (13%)**	**4 (22.2%**	**5 (21.74%**
Q52	**11 (34.4%)**	**9 (50%)**	**1 (3.1%)**	**16 (30.8%)**	**14 (31.82%)**	**10 (24.4%)**	**12 (33.3%)**	**3 (10.7%)**	**13 (33.3%)**	**7 (25%)**	**1 (6.7%)**	**5 (25%)**	**4 (17.4%)**	**2 (11.1%**	**3 (13%)**
Q53	**13 (40.6%)**	**2 (11.1%)**	**3 (9.4%)**	**1 (1.9%)**	**3 (6.82%)**	**5 (12.2%)**	**11 (15.3%)**	**8 (28.6%)**	**15 (38.5%)**	**6 (21.4%)**	**1 (6.7%)**	**9 (45%)**	**7 (30.4%)**	**5 (28%)**	**7 (30.4%)**
Q54	**2 (6.25%)**	**1 (5.5%)**	**10 (31.25%)**	**19 (36.5%)**	**11 (25%)**	**6 (14.6%)**	**1 (2.8%)**	**7 (25%)**	**5 (12.8%)**	**2 (7.14%)**	**7 (46.7%**	**1 (5%)**	**5 (21.74%**	**3 (16.7%**	**2 (8.7%)**
Q55	**3 (9.4%)**	**2 (11.1%)**	**13 (40.6%)**	**1 (1.9%)**	**7 (16%)**	**8 (19.5%)**	**7 (19.4%)**	**9 (32.1%)**	**3 (7.7%)**	**3 (10.7%)**	**2 (13.3%**	**1 (5%)**	**4 (17.4%)**	**4 (22.2%**	**6 (26%)**
Total	**32 (100%)**	**18 (100%)**	**32 (100%)**	**52 (100%)**	**44 (100%)**	**41 (100%)**	**36 (100%)**	**28 (100%)**	**39 (100%)**	**28 (100%)**	**15 (100%)**	**20 (100%**	**23 (100%)**	**18 (100%)**	**23 (100%)**

**The number of respondents is shown in the upper rows while, the corresponding percentages are shown underneath*

***C stands for Cluster**

6.5 Analysis of Coherence in Clusters

A strong coherence was attained in 15 clusters for the four items (Q8; Q9; Q10; Q11) measured to establish if there was and how limited understanding of cybersecurity contributed to misalignment of national laws. When combined together, respondents in all clusters agreed that people, businesses- private or public, had limited understanding of cybersecurity which ultimately affected their state of preparedness. Respondents in Cluster 7 (39%) and Cluster 13 (39.1%) had the highest number of female respondents perceived that people failed to understand cybersecurity because of the conflicting terminology that was used (Q10). Cluster 8 (68%) who were mainly female respondents aged 25-44 years agreed that lack of information sharing (Q11) contributed to misunderstanding of cybersecurity. Respondents in Cluster 1(47%) who were Black and White academics with more than 11 years working, Cluster 5 (47.74%), Cluster 11 (53.3%) comprising legal and IT experts all agreed that the law-making process was slow and time consuming. Given the responses for all 4 items measured (Q12; Q14; Q16; Q18), it can be concluded that coherence in all clusters has been attained and it is strong. With reference to the responses, there is a correlation between the limited understanding of cybersecurity and slow law-making process. Limited understanding of cybersecurity impedes the pace at which laws are developed and enacted**.**

Different government departments were mandated to coordinate various pieces of legislation, however, the agencies/departments' mandates overlapped, often creating conflicts resulting in poor coordination of the laws. Respondents in Cluster 1 (40.6%) mostly legal experts, Cluster 11 (53.3%) academics and Cluster 12 (65%) female respondents agreed that overlapping mandates create inconsistencies which resulted in poor coordination of legislation (Q19; Q20; Q21; Q22; A24). The overall viewpoint was that the presence of multiple government agencies meant multiple information systems were fragmented, thus, poor coordination occurred due to overlapping mandates. There was a strong coherence between lack of IT and Legal skills in cybersecurity with the law-making process and limited understanding of cybersecurity factors. The coherence arises when people are appointed to key positions without the necessary skills and knowledge to make laws for the country. Respondents agreed that appointing the right people at every level in the organisation, helps to identify, build staff defences and responses (Q34). This has ramifications on the pace of implementing new laws as stated by respondents in Cluster 8 (46.4%), respondents in Cluster 13 (43.5%) who indicated that with vast

cybersecurity experience indicated that technology is advancing at an accelerated rate, thus, cybercriminals are operating in tandem with the latest trends. IT specialists are therefore, outpaced by sophisticated cybercriminals for all the five items measured (Q30; Q31; Q32; Q33; Q34).

Knowledge and information sharing are key ingredients for understanding the law-making process, cyberspace trends and how other organisations or governments respond to threats and attacks. Respondents in Cluster 3 (40.6%) male respondents, Cluster 4 (36.5%), Cluster 5 (36.4%), Cluster 9 (38.5%), Cluster 11 (40%) fraud specialists and Cluster 12 (45%) all agreed that limited understanding of cybersecuirty was atributed to lack of knowledge and information sharing among government agencies, business and civil society, thus, had implications on the law-making process. Given the perceptions of respondents in Cluster 3, Cluster 4, Cluster 5, Cluster 9, Cluster 11 and Cluster 12, it can be concluded all clusters attained an adequate level of coherence among multiple agencies, limited understanding of cybersecurity and law-making process (Venkatraman, 1989).

An adequate level of coherence was attained among 3/3 items measured (Q40; Q42; Q43) regarding unacceptable user behaviour. People behave in certain ways that can stifle the development and implementation of laws. Respondents in Cluster 12 (50%), Cluster 4 (50%) and Cluster 15 (52.1%) respectively agreed that unacceptable behaviour can lead managers to remove certain people from some tasks, creating a shortage of resources. Unacceptable user behaviour manifested through resistance to change, thus, slowing down the process of making laws as well as adaptation pace. This response was reported by respondents in Cluster 6 (44%). who established that unacceptable human behaviour is a manifestation of the absence or presence of a weak cybersecurity culture, hence, the prevalence of cyber-attacks and human errors in the workplace. In addition, when users abandon security policies without punishment, this clearly demonstrates the absence of or a weak cybersecurity culture. When collectively viewed, these elements attained a strong coherence.

While respondents in Cluster 8 (25%) mostly managers agreed that firms are compelled to establish cybersecurity cultures due to the overreliance on ICTs, respondents in Cluster 13 (48%) also buttressed the concept of establishing a cybersecurity culture because the respondents perceived culture to transform security from a one-time event into a lifecycle. However, respondents in Cluster 1 (25%) and respondents in Cluster 14 (33.3%) disagreed that

modern security culture enables to work in a way they want, inside or outside the corporate network (Q47; Q48). It can be concluded that there was some weak coherence between 3/5 items measured (Q44; Q45; Q46).

The existence of many national, regional and global pieces of legislation hinders the pace at which laws are developed and enacted. There is a possibility that multiple global cyberlaws might exarcerbate the incoherence and fragmentation of national laws through limited understanding of global cyberlaws.This could be through misintepretation, limited understanding or lack of legal skills. This was confirmed by respondents in Cluster 1 (40.6%), Cluster 2 (50%), respondents in Cluster 10 (35.8%) and Cluster 12 (45%) on the 5/5 items measured (Q51; Q52; Q53; Q54; Q55). The results suggest that an adequate level of coherence among the factors was attained (see Table 6.3) and other factors (Venkatraman, 1989). With reference to the cluster analyses presented in this section, the research concludes that coherence was attacined in all 15 clusters and for all the 37 items measured (see Table 6.3).

Given the analysis of coherence of all 15 clusters, my proposition **P1** is therefore supported: that is, the stronger the coherence among the elements the more aligned the South African National Cybersecurity Policy Framework for CS, LMPRE, MAIS, MC, SIC, KIS, PICL, CSC and EGCL. This is consistent with the Gestalts theory which states that the stronger the coherence among organisational elements over a sustained period of time, the greater would the alignment or effectiveness of the SA-NCPF. This study established that the more coherent the SA-NCPF is perceived, the greater would be the degree of effectiveness and alignment to national, regional and global cyberlaws. Therefore, proposition **P2** is also supported. When the NCPF is perceived to be weak, so will be the NCS in addressing cybersecurity in order to protect national IT infrastructure and socio-economic growth objectives (Schultz, 2016; Johnson, 2017, Bote, 2019).

Public perceptions on issues relating to the effectiveness of the SA-NCPF differed in a few clusters. Similar or differing viewpoints about certain aspects of the above elements belonged to both clusters. For example, respondents in Clusters 1, 2, 3, 5, 6, 7, 9, 10, 11, 14 and 15 perceived strong coherence among all seven elements, while Cluster 4, Cluster 8, Cluster 12 and Cluster 13 respondents did not perceive a strong coherence among cybersecurity culture and unacceptable user behaviour. It can be concluded that respondents in all clusters perceived that a strong coherence among the elements also perceived an effective SA-NCPF. Therefore,

proposition **P3** is supported (that is, groups of respondents that perceive strong coherence among the elements will also perceive effectiveness of the SA-NCPF).

The findings from this study show that coherence among the elements is strong across all 15 clusters. By attaining an adequate level of coherence in all clusters, therefore, it can be concluded that all the elements have a combined influence on the degree of alignment of the SA-NCPF. The results are consistent with previous studies by von Solms and von Solms (2018) who established that the South African regulatory environment comprised different pieces of poorly coordinated and fragmented legislation which affected the NCPF and the NCS. Given the complexity and prevalence of cybercrimes, South African laws are fragmented and inconsistent, resulting in misalignment of the NCPF (von Solms & von Solms, 2018).

The present study also confirms that there are a few previous studies in South Africa relating to the degree of mis/alignment of the NCPF to national, regional and international cyberlaws, thus, presenting an unwelcome situation permeating the country's NCS. Lack of IT and legal skills in cybersecurity have been raised in this study as a major impediment to the development and implementation of a cogent NCS. This is confirmed in a news bulletin on News24 (2018), StatsSA (2019) and Bote (2019), that due to lack of cybersecurity skills, South African firms (private and public) were using old and irrelevant solutions, technologies and approaches to respond to a new wave of cybercrimes used by cybercriminals which were more advanced than contemporary information security strategies. A huge gap exists between an NCS and egregious modus operandi of cybercriminals, therefore, with reference to the skills shortage, South Africa has to introspect and strategize its cybersecurity preparedness and response pattern (Maja *et al.,* 2020; Letham, 2021; Malatji *et al*, 2021).

6.6 Chapter Summary

This chapter presented, interpreted and discussed research findings. First, the demographic characteristics of respondents (age, gender, ethnicity, highest qualification, current position, working experience) were analysed and presented. It was established that more female respondents participated in the study compared to their male counterparts. When reporting findings, it is important to describe respondents' demographics to ensure diversity is achieved in research. Inclusion of demographics allowed the researcher to describe the sample elements in order to determine if the findings could be generalisable. These demographic characteristics

were presented as cluster profiles. In the second section of the chapter, the research findings on cluster profiling of influencing factors were presented in the form of frequencies. Data was analysed through cluster analysis (cluster algorithms) to arrive at two clusters with usable data sets. Research findings were discussed through the lens of the fifteen Clusters whose data-sets were found usable. This study focused on alignment of the NCPF, therefore, towards the end of this chapter, the researcher analysed the coherences of clusters to tease out strong patterns (Gestalts) among the elements. The last chapter of the study, presents conclusions, research contributions, limitations and future research.

PART IV

CHAPTER SEVEN: CONCLUSIONS, RESEARCH CONTRIBUTIONS, LIMITATIONS AND FUTURE RESEARCH

7.1 Introduction

In the preceding chapter, research findings were analysed, interpreted and discussed. Chapter seven (7) presents the conclusion by restating the research problem and objectives that guided this study. It is paramount importance to discuss key research findings and draw conclusions for informed decisions. After presenting the research findings, the research contributions are presented to different beneficiaries, followed by the limitations to this thesis. Suggestions for future research are presented followed by the final research conclusion.

7. 2 Conclusion

Cybercrime and Cybersecurity are topical issues in the global economy and have been increasing at an exponential and worrisome rate (WHO, 2020) especially after the emergence of the global COVID-19 pandemic. Cybersecurity experts predict that by 2025, more than USD6 trillion would be lost through cybercrimes, therefore, governments have another "pandemic" to deal with if they aspire to protect their country's IT and information assets (Johnson, 2017). The exponential growth rate and level of sophistication of cybercrime, governments, throughout the whole world, are developing national cybersecurity strategies which include policy frameworks, legislation and other interventions to address cyber-attacks and threats (Claassen et al., 2012; Orji, 2012; Freedman, 2016; Chigada & Kyobe, 2018). Evidence from the study demonstrates that achieving an effective national cybersecurity strategy was a shared responsibility (Selebalo, 2014; Keman & Pearlson, 2019). In order to develop a national cybersecurity culture and drive towards one common goal, the South African government has developed the National Cybersecurity Policy Framework to guide cyberlaws (regulatory environment), society, government and businesses (Mahlobo, 2015; SSA, 2015; van der Merwe, 2016). However, it has been established that past studies have failed to measure the degree of alignment of the NCPF using linear approaches (Johnson, 2017; Bote, 2019). This study identified nine influencing factors that contributed to the alignment of

the NCPF. These influencing factors interact with each other continuously producing complex relationships, therefore, it is difficult to measure the degree of influence of each factor, hence the need to look at and measure the relationships as Gestalts. Gestalts view individual interactions between pairs of constructs only as a part of the overall pattern (Venkatraman, 1989; Miller, 1991). Therefore, the integrative theoretical framework and Gestalts approach were used to develop a conceptual framework to measure the degree of alignment of influencing factors.

This study proposed that the stronger the coherence among the influencing factors, the more aligned the South African National Security Policy Framework. The more coherent the SA-NCPF is perceived, the greater would be the degree of alignment of the country's cybersecurity framework to national, regional and global cyberlaws. Respondents that perceived a strong coherence among the elements also perceived an effective SA-NCPF. Empirically, this proposition was tested using nine constructs. Quantitative data was gathered from respondents using a survey. A major contribution of this study was that it was the first attempt in South Africa to measure the alignment of the SA-NCPF using the Gestalts approach as an effective approach for measuring complex relationships. The study also developed an integrative theoretical framework which integrates various theories that helped to understand and better explain the law-making process in South Africa.

The study also identified that shortage of IT and legal skills in cybersecurity, technological advancements and emerging sophisticated cybercrime hinder the alignment of the NCPF and NCS. These elements need to be aligned continuously because threat actors were devising complex attacks and threats in tandem with technological developments. If the country does not have the requisite skills, capabilities and ability to proactively respond to a global challenge, the desired goals of curbing cybercrime will not be achieved (GCSCC, 2021). New technologies are disrupting the status quo, forcing organisations to reconfigure cybersecurity cultures, employees' behaviour, and attitudes. With the adoption of new technologies, management and employees have to rebuild a new set of cybersecurity norms and value systems (Da Veiga & Eloff, 2010; GCSCC, 2021). The author acknowledges that cybersecurity presents particular problems where the shortage of skilled individuals impedes the development of an effective NCS, defence and security sectors, banking and finance, in critical national infrastructure and other sectors (ITU, 2019; World Bank, 2017; NIST, 2014).

Findings from the study also show that the human being was the greatest threat to information systems and cybersecurity in the organisation. Respondents perceived that unacceptable human behaviour was attributed to a lack of a cybersecurity culture, weak governance policies and the lure for money. In support of the findings, Chang and Coppel (2020) state that unacceptable human behaviour is a manifestation of the absence or presence of a weak cybersecurity culture, hence, the prevalence of cyber-attacks and human errors in the workplace. In addition, when users abandon security policies without punishment, this clearly demonstrates the absence of or a weak cybersecurity culture. While the WEF (2020) avers that organisations are placing too much emphasis on human intelligence which might result in the firm overlooking the individual person's ethical conduct, thus, creating opportunities for unethical behaviour.

Respondents in all clusters perceived that multiple government agencies, with overlapping mandates contributed to poor coordination, fragmentation and misalignment of the NCPF. In addition, multiple government agencies/departments operated in silos-did not share information and knowledge about cybercrime trends. Mahlobo (2015), Schultz (2016), van der Merwe (2016), Bote (2019), Maja *et al.* (2020) and Malatji *et al.* (2021) corroborated the findings by restating the level of inconsistencies, incoherencies and poor coordination of legislation. Compounding the weaknesses of the NCPF was the fact that different pieces of legislation focused on different types of cybercrime. There were few instances of commonality among the laws. From the 4/5 items measured, respondents' perceptions demonstrated a strong coherence between multiple government agencies, and coordination of coherent legislation (Venkatraman, 1989).

Findings from the study established that the public had limited access to media to contribute to Parliamentary debates, thus, there was a perception of exclusion from the law-making process which concerned their well-being. This was corroborated by de Villiers (2001) whose findings are in line with the respondents' perception. Legislatures should facilitate and enable the active involvement of civil society in the law-making process which include promotion of access of the public to the legislature buildings, Constituency Offices, Committee meetings and Public Hearings (Constitution 108 of 1996, s (118)). The importance of public participation in the law-making process should not be overlooked because these laws affect the well-being of civil society, private and public sector entities. The public's assertions that they are alienated from contributing to Parliamentary debates is affirmed by respondents who stated that after Bills have been passed into law or Act of Parliament, there appears to be no or little feedback to the

public (Selebalo, 2014). Given the context of public participation debates, the study established that there was correlation between public participation and information and knowledge sharing and understanding of cybercrime (Knowles, 2016; Wout, 2019).

Lastly, the study established that the combined influence of all nine elements over a sustained period of time achieved an adequate level of coherence (Miller, 1991), resulting in improved performance or alignment of the NCPF. Combined influence or coherence shows that the elements complement each other (Venkatraman, 1989).

The conclusion presented above, has been drawn from different aspects of the research study. The conclusion relating the primary research question is summarised in the next subsection.

7.2.1 Research Question

The alignment of influencing factors to achieve an aligned NCPF has been the degree of coherence among the elements (see Table 6.3, CS, LMPRE, MAIS, MC, SIC, KIS, PICL, CSC and EGCL). This was guided by the research question, ***"How can influencing factors be measured and aligned to achieve an effective South African National Cybersecurity Policy Framework?*** Respondents in Clusters 1, 2, 3, 5, 6, 7, 9, 10, 11, 14 and 15 perceived strong coherence among all seven elements, while Cluster 4, Cluster 8, Cluster 12 and Cluster 13 respondents did not perceive a strong coherence among cybersecurity culture and unacceptable user behaviour. Consistent with the Configuration/Gestalts fit perspective of alignment, all clusters have attained adequate levels of coherence. This, therefore means that the combined influence of all elements (see Figure 4.2) have attained an adequate level of coherence as espoused by Venkatraman (1989). Having established that the proposed conceptual model has guided the measurement of the extent of alignment of influencing factors, the primary research question posed for this study has been adequately addressed.

7.3 Contributions of the Study

This section presents the major research contributions discussed as follows:

7.3.1. Originality/Value

For long, people and businesses have been ceased with the concept of cybersecurity and its impact on the global economy. Guetzkow and Lamont (2004) posit that research should present

new discovery that adds new knowledge. This results in originality of knowledge or value of the study. In this study, the researcher has been exposed to the concept of Gestalts for the first time and has dutifully applied the theory to understand and explain alignment of cyber laws. After reviewing a number of studies, the researcher was convinced that this study is the first attempt to measure the alignment of the South African National Cybersecurity Policy Framework. Originality of the study was achieved by adopting and using the Gestalts approach. Chigada and Kyobe (2018) agree that measuring alignment of the SA-NCPF has been a major challenge for many scholars and researchers in South Africa because of the complexity of multiple factors interacting with each other.

7.3.2 Theoretical Contribution

The development of the integrative theoretical framework brought together various theories that helped to explain and understand the South African law-making process and why it is a very slow process. The researcher identified nine influencing factors which continuously interacted with each other producing complex relationships. When elements at the organisational level interact, the relationships become so complex to understand by linear relationships. Hence the need to look at and measure the relationships as Gestalts. Therefore, the first major contribution of the study was the Gestalts model for measuring alignment of the influencing factors. The extent to which these factors influence each other is not known, therefore, the conceptual model was developed to measure extent of alignment that would achieve an effective NCPF. Miller (1991) states that Gestalts view individual interactions between pairs of elements only as part of the overall pattern/configuration.

This study adopted the Cluster-based configuration perspective to distinguish, describe and predict the degree of alignment of the SA-NCPF. The cluster-based configuration provided a valid measurement of alignment of the SA-NCPF which is a major methodological contribution of the thesis. The researcher was convinced that the integrative, conceptual model and adoption of the Gestalts approach were the first attempt in South African studies to address the challenge of alignment of the NCPF. This is in line with the assertions of Malatji *et al*. (2021) who admit that past studies have concluded that the NCPF is misaligned and ineffective due to a number of reasons, some of which are the influencing factors described in this study. However, there is a dearth of studies that have addressed the challenge of alignment. The Configurations theory was adopted to test this interplay and understand an organisation and examine the constructs as a whole and not in parts. Venkatraman (1989) posits that organisational elements interacting

with each other, produce relationships and can influence each other over a certain period of time which result in the elements achieving an adequate level of coherence to produce an aligned NCPF. Knowledge has been advanced through the following:

i) Past studies have examined the constructs in isolation and not as a whole, thus, have failed to address the challenge of alignment of the NCPF. This thesis has examined these elements as a whole to measure the degree of alignment of the NCPF, thus, addressing the challenge of alignment.

ii) Extant literature on the NCPF suggests that there are different pieces of fragmented and incoherent legislation which are poorly coordinated. The findings in this study also corroborate the discussions in literature. Various scholars, legal experts and political leaders who have been directly involved in the development of the national cybersecurity strategy confirmed what has been reviewed in literature. The multiplicity of fragmented and incoherent legislation contributed significantly to the misalignment of the NCPF.

iii) The findings also demonstrated that cybersecurity is a topical issue that requires well-coordinated initiatives and efforts from everyone in the country. Given the context of the global Covid-19 pandemic, an exponential increase in cybercrimes demands a paradigm shift in how individuals, business or government reacts to combating cybercrime.

7.3.3 Practical Contribution

The misalignment of the SA-NCPF is caused by the lack of IT and cybersecurity legal skills, fragmented pieces of legislation, poor coordination of legislation by multiple government departments, slow pace in the law-making process and the fast-paced rate of sophisticated cybercrime space. In addition, the global village is grappling with Corona Virus Disease-2019 on hand and cybercriminals taking advantage of the overreliance on Information Communication Technologies (ICTs) during this pandemic. The complexity of cybercrimes during the global Covid-19 pandemic exerts pressure on governments and economies that do not have IT and legal skills in cybersecurity, effectively, exposing many countries and companies to cyber-attacks and threats (WHO, 2020; WEF, 2020). An adequate level of coherence is attained when influencing factors support and reinforce each over a sustained

period of time. The study identified many areas that require interventions and revision of the NCPF. Education, awareness and involvement of everyone in society helps to develop a cybersecurity culture in South Africa.

Given the context of the global Covid-19 pandemic, it is high time that a strong partnership should be formed to fight both pandemics simultaneously. This study is important because it raises fundamental issues that the country should invest in the development of IT and legal skills in cybersecurity as well as the need for technology preparedness. The transition to online business transactions caught many people and industries off-guard, and in the midst of trying to assimilate to working remotely, windows of opportunities for cybercrimes have been rising (WHO, 2020). Whilst the global economy is focusing on the Covid-19 pandemic, cybercriminals are busy with their nefarious acts, thus, the current thesis is fundamental to what is presently happening globally, that both legal, technological, non-technological, tools, practices and interventions should be developed and implemented at a faster pace if the country is to develop and implement an effective national cybersecurity strategy. Events occurring at the time of compiling this research study, require a paradigm shift and complete overhaul of the law-making process and coordination of cyber-legislation.

7.4 Recommendations for Practice

Both literature review and primary research findings concluded that the law-making process in South Africa is slow and time-consuming. Unless the Bill is extremely urgent, it can take between 3 months and 12 months to have the Bill passed and enacted into law. Reviewing the law-making process in the country should be considered to ensure the country keeps pace of development and implementation of cyberlaws in line with global trends. By reviewing the process, there is a high likely opportunity that the roles and responsibilities of the NCOPs and NA might be reviewed to minimise bureaucratic processes. For example, Bills are referred to Portfolio Committees for debates then back to the House for further debates and then referred to Portfolio Committees for final debates before they are approved by Parliament for the President's signature. Bureaucratic procedures in the law-making process not only derail the development of laws, but force the country to lag behind regional and international trends.

A legislative committee should be established involving IT/IS, Courts and cybersecurity experts from industry and academia to review the country's regulatory landscape. Current

legislation does not adequately address most cybercrimes, thus, leaving a huge challenge for courts to successfully prosecute cybercriminals. Reviewing the current legislation might help to align them to national, regional and global cyberlaws with the objective of developing an effective NCS and NCPF. IS scholars and researchers have indicated that cybercriminals are conversant of the country's weaknesses, especially with reference to legislation. Criminal elements can perpetrate crime in South Africa but residing in another country in the region, fully aware that their nefarious acts would take time to be detected and with slim chances of being prosecuted. It is because the country (SA) where the crime is committed, its laws cannot be successfully applied in the other country from which the perpetrator resides or commits the crime from due to misalignment of legislation.

The study revealed that lack of IT and legal skills in cybersecurity contribute significantly to the country's failure to interpret cybercrimes, proactively respond to and address sophisticated cybercrimes. Thus, this study recommends a review of the skills development policy of scarce skills. Practitioners and policy makers should look at capacitating schools (primary and high schools) with libraries, computer laboratories, books and optic fibre and IT or computer teachers. These resources should be mobilised to provide the incubation for IT and legal skills development at grassroots level. Apart from capacitating schools, policy-makers should also look at supporting small-medium enterprises because these entrepreneurial ventures have been known to be innovative and engine room for economic growth. Deficiencies in financial and technology resources have hindered the survival and success for some of the SMEs, yet, novel and innovative ideas have been resident in these business minds. Therefore, SMEs and schools would be incubators for addressing the shortage of skills facing the country. On the other hand, universities and other institutions of higher learning have a responsibility to develop a new crop of cybersecurity skills through revaluation of their degrees, diplomas or certificates. A new university graduate should be equipped with competences to address cybercrimes.

Findings from the study established that the country's legislation is poorly coordinated, fragmented and incoherent leading to misalignment of the NCPF. Political expediency at the expense of efficiency is consequential to the national cybersecurity strategy, therefore, policy makers should review the appointment of management or custodians of legislation. Government should establish structures that involve courts and legal minds to take full responsibility of each piece of legislation. These individuals, by virtue of their legal backgrounds, might be able to interpret and apply law. The review of management structures

of legislation can be done simultaneously when the overall review of the country's legislation framework is done to ensure overlapping mandates are mitigated.

Given the complexity of cybercrimes, society, business and government should be in the propensity of sharing knowledge and information about latest trends to enhance awareness and state of preparedness. The findings show that different government agencies operated silo approaches, that is, they did not share information for fear of exposing intellectual property as well as having sworn to secret service. However, the objective is to develop an effective national cybersecurity strategy, it becomes imperative for these institutions to share information and knowledge among themselves in order to become aware of and proactively prepare for cyber-attacks and threats. Sharing information and knowledge among agencies improves trust and confidence from the public.

With the increased usage of mobile devices, the acceleration of cybercrimes is perpetrated when employees bring and connect their personal devices to the corporate network, including in Parliament which has been hacked or exposed to a Zoom cyber-attack. Respondents indicated the need for a BYOD policy to mitigate cyber-attacks and threats. Therefore, when reviewing the country's legislation, policy makers should suggest the development of law for mobile devices- mobile law as an area of jurisprudence. The emergence of BYODs creates a need for government to develop or evaluate current legislation to ascertain which jurisprudence will address crimes committed through BYODs.

Given that cybersecurity is a growing centrality, policy- developers in South Africa should focus on capacity building to withstand cyber threats to the public and the country's digital resources. This recommendation is suggested by Creese, Dutton, Esteve-Gonzalez and Shilliar, 2021) who have observed the attention and drive towards capacity building by nations across the globe. Creese et al (2021) posit that capacity building is a relatively new era, however, South Africa, like any other developing economies can leverage on a number of international organisations for assistance cooperation. Building a nation's cybersecurity strategy would require the guidelines of the NIST CSF five core functions; ITU NCS; GCSCC CMM five dimensions; World Bank Cybercrime toolkit (GCSCC, 2021).

There are number of international organisations such as the World Bank, International Telecommunications Union, National Institute of Standards and Technology and the GCSCC

that have and continue to assist emerging countries develop national cybersecurity strategies. In section 2.6, the author discussed the GCSCC CMM model, ITU NCS; NIST CSF and the World Bank Cybercrime toolkit. South Africa, being a signatory to global conventions on cybersecurity, can engage some of these institutions for guidance. Of particular interest is the issue of capacity building to enhance a country's cybersecurity strategy. This thesis established that the SA-NCPF has alignment challenges, therefore, it would be important to enlist the services and guidelines of cybersecurity experts in the development, deployment and monitoring of the country's cybersecurity strategy.

7.5 Limitations of the Research

The researcher highlights some limitations that confronted the study confronted. It is possible to encounter limitations when conducting a study of this magnitude. These limitations or shortcomings could be methodological or researcher-related (Saunders *et al.,* 2019). In many instances, the researcher is confronted with influences beyond one's control. When faced with limitations, the research methodology and conclusions can be affected (Creswell, 2014). In this thesis, the researcher acknowledges the limitations, so that appropriate suggestions are recommended for future research to avoid encountering the same conditions. Creswell (2012) and Chigada (2014) state that limitations can be used to demonstrate the researcher's critical thought, focus on the research problem, reviewed appropriate and relevant literature and the methods for studying the problem. The following were the limitations of this thesis:

7.5.1 Methodological Limitations

The first methodological limitation of this study was the absence or lack of prior research on the alignment of the NCPF. Without the theoretical underpinnings of literature of the SA-NCPF, it was a challenge to draw lessons from empirical studies from a South African or SADC region perspective. Prior studies provide the basis on which to explain and understand the problem under investigation.

The second limitation was attributed to the Gestalts approach adopted in this study was tested in a very dynamic environment. Cybercrimes are growing at an exponential rate; thus, the cyberspace is uncertain, limiting the ability of managers to make decisions (Soin & Paul, 2013). Alignment is not a one-time activity but constantly change act of the contemporary business environment, therefore, the researcher was exposed to and used the Gestalts fit perspective to

understand the concept of alignment in a dynamic environment. Due interactions between organisations and the emergence of the global Corona Virus Disease-2019 (COVID-19) pandemic, measures of alignment should be cognisant that the global economy is dynamic and probably, a longitudinal study might help to understand the phenomenon.

The target population for the study were information systems professionals, legal experts, lawmakers and information systems and legal academics. This is in line with the GCSCC which involved academia, cybersecurity experts, private & public sectors, policy-developers etc in the development of the CMM. The goal of this thesis was to obtain relevant insights from professionals working with the domain of cybersecurity. Members of civil society were excluded from study, whose responses could have changed the findings of this study. In addition, a mono-quantitative research method was used, thus, the voice of the respondent was not heard. Ngulube (2019); Saunders et al (2019) state that the use of a mono-method has pros and cons, as has been admitted by the author of this thesis. This would have been ameliorated if a mixed method research had been adopted, where both qualitative and quantitative data are collected (Herman & Edwards, 2014). The use of one research method created a deficiency in enhancing the reliability of research findings. Data collected from multiple sources using different techniques tends to improve the validity and reliability of the findings. Future researchers would need to combine/mix qualitative and quantitative in a single study to get rich datasets (Creswell, 2012).

The author of this thesis identified that some of the questions probing the degree to which respondents believe the various issues identified through the survey work are relevant, use negative language, therefore, one might conclude that the results could be biased towards the preconceptions of the author. This is not true in every aspect of the survey, for example the section on cybersecurity culture has examples of positive language and reverse framing of questions where high scores indicate evidence of alignment.

7.5.2 Researcher Limitation

The only limitation experienced in this study was accessing politicians, Ministers and some law-makers. These individuals' work schedules were tight, thus, sending them emails or universal resource locator (URL) to complete the survey would not have yielded the desired results. Therefore, appointments were made to meet the individuals ate their earliest convenient schedules. Thus, the researcher had to fly or drive to other Provinces where the respondent was

readily available to participate in the survey. Survey meetings could have easily been converted into face-to-face interviews for probity, but due to prior discussions, this would not take place without jeopardising the merits of the study.

7.6 Suggestions for Future Research

Suggestions for future research are derived from the findings and limitations of this study. For future studies, the following recommendations are made:

i) This study adopted a mono-quantitative method; thus, the voice of the participant was missing from the study. Personal opinions and perspectives would have enhanced the understanding of the problem at hand. When participants are probed for clarity, certain issues become clearer, thus, informing the research findings. As opposed to the use of mono methods, future studies can adopt mixed methods so that both quantitative and qualitative data can be collected from multiple sources leading to triangulation. In addition, mixing methods in a single study enhances the reliability and validity of research findings.

ii) Past studies have examined influencing factors in isolation to address the challenge of alignment. Most studies used linear approaches in their quest to understand the complex relationships arising from the interplay between influencing factors. Future studies can use the Gestalts approach to address the challenge of alignment. Future research is needed to test the conceptual model developed (See Figure 4.2) with more elements of the configurational approach while retaining the same logic binding the core elements in the model. For example, political appointments, involvements and periodic reviews of legislation are critical factors that should be considered when testing the extent of alignment of the conceptual model.

iii) The conceptual model developed in this study could be validated by using multiple cases and more research participants and respondents. This can increase the validity and reliability of research findings to a larger population. Research on the alignment and effectiveness of the NCPF should be conducted to provide insights to government and other stakeholders with a vested interest in cybersecurity. This

study is the first attempt to use the Gestalts approach to address the challenge of alignment of the NCPF.

iv) The study established that user behaviour played a significant role in the commission of cybercrimes, therefore, an area for future study would be required to understand the role of user behaviour and ethical conduct in the cyberspace. From the discussions presented in this thesis, the human being has been central to every activity. However, the study did not provide their specific level of influences. Future studies might shed some light on how acceptable human behaviour can address cybercrimes.

v) Given the context of advanced technological developments and an exponential increase of cybercrimes during the global Covid-19 pandemic, the environment is very dynamic, businesses are constantly reconfiguring their models to accommodate new technologies, society's demands and responding to the challenges posed the Covid-19 pandemic. Therefore, a longitudinal study could be conducted to changes that may occur overtime with the NCPF.

vi) Given the growing importance of developing an effective national cybersecurity strategy, regulatory and legal frameworks, future comparative studies could be undertaken to determine how other countries have integrated the GCSCC CMM, ITU NCS, World Bank toolkit or the NIST CSF in the development of national cybersecurity legal and regulatory frameworks. The involvement of international cybersecurity experts and bodies will also be ascertained in order to understand their contributions, challenges and successes.

7.7 Final Conclusion

This research journey started in 2017 with the development and defence of a research proposal. The aim of this thesis was to develop a conceptual model to measure and align influencing factors to achieve an effective NCPF in South Africa. Measuring the extent of alignment of cybersecurity policy frameworks has been problematic for many researchers because of the complexities arising from interplays between different elements involved in the coordination of cybersecurity legislation. A new approach to measure such a complex interplay was required

by the SA government, private and public sector organisations and society to demonstrate the benefits of an effective Cybersecurity Policy Framework.

Appropriate interventions are required because addressing cybersecurity issues is a shared responsibility. A number of factors identified in this study were fundamental to the alignment of the SA-NCPF, as evidenced by the use of the Gestalts fit perspective of alignment and Cluster analysis. Respondents in both clusters perceived all elements to be significantly influencing and complementing each other towards an effective NCPF. Respondents in all fifteen clusters, agreed that civil society, private & public sectors had limited understanding of ***understanding cybersecurity (CS) issue***. Sharing of cybersecurity knowledge and information enhanced the levels of understanding and state of awareness of cybercrimes. Respondents indicated that with an enabling environment, private & public sectors and civil society would remove silo barriers to sharing cybersecurity information and knowledge.

Clusters 1; 5; 10 and 15 respondents indicated that the ***law-making process*** was pivotal at how the country enacted its statutes, responds to and successfully prosecute cybercrimes. Respondents indicated that the country's law-making process was slow, time-consuming and bureaucratic, thus, lagged behind the pace of global cyberlaws. To pass and enact a Bill ordinarily takes between 3-12 months in South Africa, which is regarded as very slow compared to international standards. Respondents in clusters 1; 3; 4; 5; 7 and 8 strongly agreed that ***coordination of e-legislation*** was pertinent in the process of developing an effective national cybersecurity strategy. Respondents indicated that currently, South Africa e-legislation was coordinated by different government agencies or departments, creating windows of opportunities of fragmentation and poor coordination. The consensus from all respondents was that coordination of e-legislation should be effective towards the country's national cybersecurity critical infrastructure strategy.

Respondents in clusters 1-4 and 7 indicated that mechanisms for ***monitoring and controlling information*** systems security protocols should be devised and implemented in line with the availability of the country's or organisation's resources. When combined together, all respondents perceived that the absence of controls and protocols weaken an NCS, while intrusion detection systems were perceived to reduce unauthorised access to data and information systems. Respondents in Clusters 3; 11; 13 and 15 who comprised cybersecurity experts, policy makers, CISOs and CIOs agreed that ***IT and legal skills*** were important

resources required in the development of an effective NCPF. Similar responses were provide in relation to ***knowledge and information sharing***. Respondents noted with concerns that silo approaches of addressing cybercrimes would not yield the desired cybersecurity goals, therefore, a paradigm shift was required to ensure information and knowledge were shared since there were multiple government agencies/departments coordinating different pieces of legislation.

The huge security threat lurking in companies today, ***is human behaviour***. This was confirmed by respondents in all clusters who indicated that unacceptable or unethical conduct contributed significantly to data breaches reported in many industries. In addition, companies were placing too much emphasis on human intelligence, whilst overlooking an individual person's ethical conduct. With the right and acceptable behaviour, countries were likely to enhance their IT and legal skills, capacity building and evaluation of the cybersecurity maturity position. Interestingly, respondents did not think that a ***cybersecurity culture*** influenced the country's NCPF. With a wide range of global cyberlaws, coupled with the law-making process, IT and legal skills challenges, respondents strongly agreed that ***multiple global laws*** were enacted at a very fast pace compared to South African laws.

Given the responses provided, the author of this thesis concludes that the identified influencing factors indicated the strongest correlation of views and relationships between the issues. The learnings for policy-makers are that the current cybersecurity approaches requires inputs from different stakeholders including global experts and organisations such as the NIST, ITU, World Bank and GCSCC have and continue to make a global contribution towards combating cybersecurity. These institutions have developed and deployed guidelines through models, toolkits etc for emerging countries. It would not be too late for policy-makers to revisit the advice and guidelines from these institutions in order to develop and enact cyberlaws, legal and regulatory frameworks aligned to regional and international standards. Therefore, the author can conclude that the primary and secondary research questions were adequately addressed. The key contribution of this thesis was to present a reasoned argument upon which capacity building investment could be based.

REFERENCES

Abukari, A.M. & Bankas, E.K.(2020). Some Cybersecurity hygienic Protocols for teleworkers in Covid-19 Pandemic Period and beyond, *International Journal of Scientifie and Engineering Research*, 11 (4):1401-1407.

Africa News Agency [ANA], 2018). How African states can improve their cybersecurity. https://www.brookings.edu/techstream/how-african-states-can-improve-their-cybersecurity/

Agarwal, R., & Lucas Jr, H. C. (2005). The information systems identity crisis: Focusing on high-visibility and high-impact research, MIS Quarterly, 29(3):381-398.

Agrafiotis, I., Nurse, J.R.C., Goldsmith, M., Creese, S., Upton, D. (2018), 'A Taxonomy of Cyber-harms: Defining the Impacts of Cyber-attacks and Understanding How They Propagate', Journal of Cybersecurity, v 4 n 1, p.1-15. nd https://academic.oup.com/cybersecurity/article/4/1/tyy006/5133288?searchresult=1 [Accessed 4 March 2022]

Ahmed,M., Sharif,L., Kabir, M. & Al-Maimani, M. (2012). Human errors in Information Security, *International journal of Advanced Trends in Computer science and Engineering*, 1(3). Available Online at http://warse.org/pdfs/ijatcse01132012.pdf

Alzubaidi L & Abdulaziz J. (2021). "Measuring the level of cyber-security awareness for cybercrime in Saudi Arabia." *Helion* 7, no. 1 (January). 10.1016/j.heliyon.2021.e06016.

Ajumobi, D. & Kyobe, M. (2017). Alignment of Human Competencies with Mobile Phone Technology and Business Strategies by Women-LED SMEs in South Africa, *The Electronic Journal of Information Systems in Developing Countries*, 80(1):1-25.

Amazon (2017).Biggest AWS Security Breaches of 2017. https://www.sumologic.com/blog/aws-security-breaches-2017/

Anastasiou, A., Androutsou, T., Costarides, V., Pitoglou,S., and Giannouli, D. (2020). *Cybercrime and Private Health Data: Review, Current Developments, and Future Trends.* Athens: IGI Publishers.Argaw

Apple Inc (2021). Apple targeted in US$50 Million Ransomware Hack of Supplier Quanta. https://www.bloomberg.com/news/articles/2021-04-21/apple-targeted-in-50-million-ransomware-hack-of-supplier-quanta

Arewa, A. (2018). Borderless crimes and digital forensics: Nigerian perspectives, *Journal of Financial Crime*, 25(2):619-631. https://doi.org/10.1108/JFC-12-2016-0079

Armstrong, C. L. (2009). Providing a clearer view: An examination of transparency on local government websites. *Government Information Quarterly*, 28(1):11-16.

Atoum, I., Otoom, A. & Ali, A.A. (2014). A holistic cybersecurity implementation framework, *Journal of Information Management & Computer Security*, 22 (3):251-264.

Australian Parliament (2018). Australia's Parliament House in 2018: a Chronology of Events. https://www.aph.gov.au/About_Parliament/Parliamentary_Departments/Parliamentary_Library/pubs/rp/rp1920/Chronologies/APH2018

Babbie, E.R. (1998). The Practice of Social Research, 13th Edition, Wadsworth Publishing Company, Belmont: CA

Babbie, E. (2010). The Practice of Social Research. In: *The Practice of Social Research.* 12th ed. s.l.: Wadsworth, Cengage Learning:125-130.

Baker, W.H. (2010). Thoughts on Mapping and Measuring Cybercrime. Oxford Internet Institute Forum Mapping and Measuring Cybercrime [Online] Available http://www.sfu.ca/~icrc/content/oxford.forum.cybercrime.pdf[10June 2017].

Bandura, A. (1971). *Social Learning Theory*, General Learning Press, New York.

BankServAfrica, (2016). Africa reports big jump in digital and card fraud, Blue Label Data Solutions, Annual Report, Sandton, Johannesburg.

Barney, J. (1991). Firm resources and sustained competitive advantage, Journal of Management, 17(1):99–120.

Banking Association of South Africa [BASA] (2018). Annual Report. https://www.banking.org.za/wp-content/uploads/2019/08/BASA-Annual-Report-2018.pdf

Banking Association South Africa [BASA] (2019). Annual Report. https://www.banking.org.za

Bateman,C. (2013). *Discovery Health's take on regulation 8, South African Medical Journal*,103(12):887. DOI:10.7196/SAMJ.7692.

Bates, S.C. & Cozby, P.C. (2012). Methods in behavioural research, 11th Ed, McGraw Hill Higher Education, California.

BBC News. "How China Is Ruled." Accessed August 12, 2000. http://news.bbc.co.uk/2/shared/spl/hi/in_depth/china_politics/government/html/2.stm.

Benbasat, I., & Zmud, R.W. (2003). The identity crisis within the IS discipline: defining and communicating the discipline's core properties, *MIS Quarterly*, 27(2):183-194.

Bertalanffy, L.V., Rapoport, A. & Gerard, R. (1956). General Systems Theory: Essays on its foundation and development, revised edn. New York: George Braziller.

Bhagattjee, P. & Govuza, A. (2021). The Cybercrimes Bill is one-step away from benoming law, Cliff Decker Hofmeyer. Available at: https://www.cliffedekkerhofmeyr.com/en/news/publications/2020/technology/tmt-alert-7-july-The-Cybercrimes-Bill-is-one-step-away-from-becoming-law.html/ (Accessed 13 July 2021).

Bogdanoskaia, J. (2013). Yahoo says all three billion accounts hacked in 2013 data theft. https://www.reuters.com/article/us-yahoo-cyber-idUSKCN1C82O1

Boucher,D., Gundu, T. & Maronga, M. (2019). Industry 4.0 Business Environments: fostering a Cybersecurity Culture in a Culturally Diverse workplace, Proceedings of the 4th International Conference on the Internet, *Cybersecurity and Information Systems,12:85-94.*

Bote, D. (2019). The South African National Cybersecurity Policy Framework: a Critical Analysis. Published Dissertation. North West University.

Bowen, S.M. & Seth, G. (2020). What was it that got me into Cyber? https://www.linkedin.com/in/smbowen.

Budnik, K & Kirkwood, K. (2021). Building a united front on financial crimes in the financial services sector. https://www.pwc.co.za/en/press-room/cyber-security.html/ (Accessed 10 July 2021).

Burns, R, P., & Burns, R. (2008). Business research methods and statistics using SPSS, Sage: London, UK.

Brown, D.R. (2010). *An experiential approach to organisational development*, 8th edn. New Jersey: Pearson International.

Bryman, A. & Bell, E. (2010). Business Research Methods. 3rd Edition. Oxford: Oxford University Press.

Bryman, A. & Bell, E. (2015). Business Research Methods. 4th Edition. Oxford: Oxford University Press.

Bryman, A. & Bell, E. (2017). Business Research Methods. 5th Edition. Oxford: Oxford University Press.

Calland, R. (2016). Make or Break: How the next three years will shape South Africa's next three decades. Penguin Random House.

Camponovo, G. and Pigneur, Y. (2004). Information systems alignment in uncertain environments, IFIP International conference on decision support system DSS'2004: Decision Support in an uncertain and complex world, Prato, Tuscany:134-146.

Candel, J.J.L. & Biesbroek, R. (2016). Toward a processual understanding of policy integration, *Journal of Public Administration and Policy*, WASS, 49:211-231.

Canhoto, A. (2010). 'What' before 'How', Oxford Internet Institute Forum, [Online], Available: http://www.sfu.ca/~icrc/content/oxford.forum.cybercrime.pdf [24,May 2018].

Capitec Bank South Africa, 2019, Biometrics authentication, viewed 17 June 2019, from https://www.capitecbank.co.za/biometricsproject/html (Accessed 17 June 2019)

Chalmers,D. (2002). Does conceivability entail possibility, Journal of Conceivability and possibility: 145-200. New York: Oxford University Press.

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

Chatterjee S, Kar AK, Dwivedi YK et al (2019) Prevention of cybercrimes in smart cities of India: from a citizen's perspective. Information Technology & People. 32(5):1153-1183.

Chernyshev, M., Zeadally, S., Baig, Z., & Woodward, A. (2018). Internet of things forensics: The need, process models, and open issues. *IT Professional*, 20(3):40-49. doi:10.1109/MITP.2018.032501747

Chen, W.S. & Hirschheim, R. (2004). A paradigmatic and methodological examination of information systems research from 1991-2001, *Information Systems Journal*, 14(3):197-235.

Chenthara,S., Ahmed, A. & Whittaker, F. (2019). Security and Privacy-Preserving Challenges of e-Health Solutions in Cloud Computing, IEEE Access, 7(1):74361-74382.

Chernyshev M, Zeadally S, Baig Z. Healthcare Data Breaches: Implications for Digital Forensic Readiness. J Med Syst. 2018 Nov 28;43(1):7. doi: 10.1007/s10916-018-1123-2. PMID: 30488291.

Chigada, J.M. (2014). The role of knowledge management in enhancing organisational performance in selected banks of South Africa. Published PhD Thesis. University of South Africa. Available at: http://uir.unisa.ac.za/handle/10500/14332/hmtl/ (Accessed 19 March 2018).

Chigada, J. & Kyobe, M.E. (2018). Evaluating Factors Contributing to Misalignment of the South African National Cybersecurity Policy Framework, *Con-FIRM 2018 Proceedings*, 4(1). Available at: https://core.ac.uk/download/pdf/301375684.pdf/html/ (Accessed 10 March 2019).

Chigada, J. (2020). A qualitative analysis of the feasibility of deploying biometric authentication systems to augment security protocols of bank card transactions, *South African Journal of Information Management*, 22,1(a1194).

Chigada, J. & Madzinga, R. (2021). Cyberattacks and threats during COVID-19: A systematic literature review, *South African Journal of Information Management*, 23, 1(a1277).

Chigada, J. & Ngulube, P. (2015). Knowledge management practices at selected banks in South Africa, South African Journal of Information Management, 17 (1)#634: Available at: https://dx.doi.org/104102/sajim.v17iL.634.

Childlinesa (2016). Childline SA Annual General Report 2015/2016. https://www.childlinesa.org.za/about/agm-reports/ (Accessed 18 May 2018).

Chin, W. W. (1998). The partial least squares approach for structural equation modelling. In G. A. Marcoulides (Ed.), Modern methods for business research (pp. 295–336). Lawrence Erlbaum Associates Publishers.

Chuma, K G., & Ngoepe. M. (2021). "Security of electronic personal health information in a public hospital in South Africa." *Information Security Journal: A Global Perspective*, no. 1 (March). 10.1080/19393555.2021.1893410.

Chun-Tie, Y., Birks, M. & Francis, K. (2019). Grounded theory research: A design framework for novice researchers. SAGE open medicine. 7. DOI: 10.1177/2050312118822927.

Classen, L., Cupido, C., Etsebeth, V., Klopper, H., Van der Walt, L.M., Ncube, C., Nel, S., Papadopoulos, S., Snail, S., Taylor, D. & Watney, M. (2012). Cyberlaw @ SAIII: The Law of the Internet in South Africa, 3rd Edition, Van Schaik Publishers, Pretoria.

Coghlan, D. & Brydon-Miller, M. (2014).The big picture: Implication and imperatives for action research community from the SAGE Encyclopaedia of Action research, 12(2):224-233.

Colangelo, A.J. (2016). A Systems Theory of Fragmentation and Harmonisation, New York University, *Journal of International Law and Politics (JILP)*, Forthcoming; SMU Dedman School of Law Legal Studies Research Paper No. 261. Available at SSRN: http://ssrn.com/abstract=2754402 [Accessed 22 June, 2018].

Comizio, G.V., Dayanin, D. & Bain, L. (2016). Cybersecurity as a Global Concern in Need of Global Solutions: An Overview of Financial Regulatory Developments in 2015, *Journal of Investment Compliance*, 17 (1). Available on http://dx.doi.org/10.1108/JOIC-01-2016-0003 [6 May 2017].

Constitution of the Republic of South Africa (108 of 1996) Available at: https://www.gov.za/sites/default/files/images/a108- 96.pdf/ (Accessed 2 March 2019).

Córdoba, J. R., Pilkington, A., & Bernroider, E. W. (2012). Information systems as a discipline in the making: Comparing EJIS and MISQ between 1995 and 2008. *European Journal of Information Systems*, 21(5):479-495.

Cotae, P., Kang, M. & Velazquez, A. (2020). A Cybersecurity Model for Decision-Making Problems Under Uncertainty using Game Theory. *In Proceedings of the 13th International Conference on Communications (COMM)*, Bucharest, Romania, 18–20 June 2020; IEEE: Piscataway, NJ, USA; 15–22.

Creese, S., Dutton, W.H., Esteve-Gonzalez, P. & Shilliar, R. (2021). Cybersecurity capacity-building: cross-national benefits and international divides, Journal of Cyber Policy, 6(2):214-235.

Creswell, J. W. (1994), Research design: Qualitative, quantitative, and mixed methods approaches, Thousand Oaks, CA: Sage.

Creswell, J.W. (2013). Qualitative Inquiry & Research Design: Choosing among Five Approaches, 3rd ed., Thousand Oaks, CA: SAGE.

Creswell, J.W. (2012). Research design: Qualitative, quantitative and mixed methods. 2nd ed.In V. Knight, Ed. Lincoln: Sage.

Creswell, J.D. (2015). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches.* 4th ed. s.l.: SAGE Publishing Inc.

Creswell, J. W. & Plano Clark, V. L. (2011). *Designing and Conducting Mixed Methods Research.* 2nd ed. s.l.: SAGE Publications.

Creswell, J.W. & Creswell,J.D. (2017). Research design: qualitative, quantitative and mixed methods approaches, 5th edn, Los Angeles: SAGE.

Creswell, J.W. (2018). Research Design: Qualitative, Quantitative and Mixed Methods. Sixth Edition. Thousand Oaks Publications, CA: SAGE.

Crook, G. (2017). BDO promotes the need for proactive Cyber defence, BDO South Africa.

Cronbach, L. J. (1951). Coefficient alpha and the internal structure of tests. Psychometrika, 16(3):297-334.

Cronbach, L.J. (1971). Test validation. In educational measurement, 2nd Edition, R.L. Thorndike (Ed.), *American Council on Education*, Washington, D.C.: 443-507.

Curtiss, M.R. (2011). Technologies that matter. https://s1.q4cdn.com/395056968/files/doc_financials/2011/Annual/letter.html

Daily Maverick (25 July 2019). Cyber crooks try hold Johannesburg's City Power to ransom, https://www.dailymaverick.co.za/article/2019-07-25-cyber-crooks-try-to-hold-johannesburgs-city-power-to-ransom/

Daniels, P.W. (2004). Reflections on the "Old" economy, "New" ECONOMY AND SERVICES, *Journal of Urban and Regional Policy*, 35 (2):115-138.

Davis, F.D. (1989). Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology *MIS Quarterly*,13(3):319-339.

Da Veiga, A., & Martins, N. (2015). Improving the information security culture through monitoring and implementation actions illustrated through a case study. *Computers & Security*, 49:162- 176. doi:https://doi.org/10.1016/j.cose.2014.12.006

Da Veiga, A. and Eloff, J.H.P. (2010) A framework and assessment instrument for information security culture, *Computers and Security*, (29):196–207.

De, R. (2016). Cybersecurity Conference, Delaware University, State of Delaware, Washington DC, USA.

de Carvalho, R.S. & D. Saleem, D. (2019) "Recommended Functionalities for Improving Cybersecurity of Distributed Energy Resources," 2019 Resilience Week (RWS):pp. 226-231, doi: 10.1109/RWS47064.2019.8972000.

Deng, J. Tang, Y., Zhang, Y., Yang, X. & Chen, J.L. (2012). Cybersecurity and Privacy Issues in Smart Grids, *IEEE Communications Surveys and Tutorials*, 14(4):981-997.

Deloitte. (2020). Outsourcing is good for job creation in South Africa. Johannesburg: Deloitte & Touché.

Denzin, N.K., and Lincoln, Y.S. (1994). *Handbook of qualitative research*. London: Sage.

Department of Homeland Security (DHS). (2016). Cybersecurity Insurance. Washington DC, USA.

Department of Justice (2019). https://www.justice.gov.za/reportfiles/report_list.html

Department of Justice and Constitutional Development, 2021. Cybercrimes bill[B 6-2017]. s.l.: Government Gazette No. 40487 of 9 May 2021.

De Villiers, S. 2001. A People's Government: The People's Voice – A Review of Public Participation in the Law and Policy-making Process in South Africa. Cape Town: Parliamentary Support Programme.

Dingwayo, M. & Kabanda, S. (2017). Bring Your Own Device (BYOD) and Information Privacy Compliance in South Africa, *Proceedings Of The Second International Conference On Information And Communication Technology for Africa Development*, (May):1–17. Cape Town.

District Court of Northern Transvaal, Pretoria, *Case no*.111/150/2003.

Dlamini, S. (2020). Data breach at Experian, 24 million South Africans' personal information exposed. Available at: https://www.iol.co.za/business-report/companies/data-breach-costs-sa-companies-r402-million-average-in-2020-6649ae0a-b803-482c-978f-b395517c7fa7/ (Accessed 19 June 2021).

Dlamini, S. (2021). Data breach costs SA companies R40.2 million average in 2020. https://www.iol.co.za/business-report/companies/data-breach-costs-sa-companies-r402-million-average-in-2020-6649ae0a-b803-482c-978f-b395517c7fa7

Donahue, J.L. (2017).A comparative analysis of international encryption policies en route to a domestic solution, Published Master's Thesis, Naval Postgraduate School, CA.

Dowding, K. (1995). *Model or Metaphor? A Critical Review of the Policy of Network Approach, Political Studies*, 45(1):136-158.

Drazin, R., & Van de Ven, A. H. (1985). Alternative forms of fit in contingency theory. Administrative science quarterly, 30 (4):514-539.

Drucker, P.F. (1997). The future that has already happened, *Harvard Business Review*, 75(5): 20-26.

Drucker, P.F. (1987). Social Innovation-Management's new dimension, *Long Range Planning*, 20(6):29-34.

Dulock, H.L.(1993). Research Design: Descriptive Research, *Journal of Paediatric Oncology Nursing*, 10 (4):154-157.

Dusane, P. S., & Pavithra, Y. (2020). Logic bomb: An insider attack. *International Journal of Advanced Trends in Computer Science and Engineering*, 9(3), 3662–3665. Available at https://doi.org/10.30534/ijatcse/2020/176932020/ (Accessed 19 May 2021).

Dutton, W.H., Creese, S., Shilliar, R. & Bada, M. (2019). Cybersecurity Capacity: Does it Matter?, Journal of Information Policy, 9(1):280-306.

Eagan, M. (2007). A Strategic Framework Aligned to the INCOSE Long Range Plan, INCOSE Infrastructure, 10(1):46-47.

eNCA (21 July, 2021).Cellphone hacking by an Israeli-based software company-NSO Group. Live Broadcast.

Equifax (2017). Data Breach Settlement. https://www.ftc.gov/enforcement/cases-proceedings/refunds/equifax-data-breach-settlement.

Etschmaier, M.M. (2019). Critical Issues of Cybersecurity: Solutions Beyond the Technical, IJCA, 26 (4):1-15.

Fache, T. (2018). *Taking Action Against the Growing Threat of Cyberattacks Healthcar e*Chigaco: Frontiers of health service management.

Fin24 (2016). Fin24 infringed Moneyweb's copyright in one article. https://www.moneyweb.co.za/news/south-africa/fin24-infringed-moneywebs-copyright-one-article/

Fin24 (2017). Massive data leak could be from a credit bureau. https://www.news24.com/fin24/tech/massive-data-leak-could-be-from-a-credit-bureau-20171018.

Financial Intelligence Centre (2020). Annual Report. https://www.fic.gov.za/aboutus/Pages/Annual-Reports.aspx

Fin24tech (2019). SA public ICT spending to hit $707m in 2019. https://www.news24.com/fin24/tech/companies/sa-public-ict-spending-to-hit-707m-in-2019-20150709

Fintech (2018).The Fintech Revolution: How Data Breaches can result in Regulatory Enforcement Actions.

Fitch Co. (2020). Exploring Bank Cybersecurity Risk, Gulf International Bank, Saudi Arabia.

Fleckenstein, M. & Fellows, L. (2020).Modern Data Strategy. https://www.researchgate.net/publication/323122990_Modern_Data_Strategy/html/

Formann, A. K. (1984). Latent Class Analysis, Encyclopaedia of Statistical Sciences, DOI:10.1002/0471667196.ess1083.pub2

FortiGuard Labs (2014). Fortinet's FortiGuard Labs Reveals Top 10 Threat Predictions for 2014.https://investor.fortinet.com/news-releases/news-release-details/fortinets-fortiguard-labs-reveals-top-10-threat-predictions-2014

Freedman, M. (2016).South Africa: ICT white paper under fire. *Extensia.* Retrieved from http://extensia-ltd.com/south-africa-ict-white-paper-fire/

Frey, B. B. (2018). In: *The SAGE encyclopaedia of educational research, measurement, and evaluation.* Thousand Oaks(CA): SAGE Publications, Inc.

Frost & Sullivan (2016). Artificial Intelligence Systems Poised for Dramatic Market Expansion in Healthcare.[Online]. Available: ww2.frost.com. (Accessed 11 April, 2020).

Furstenau, L.B.; Sott, M.K.; Homrich, A.J.O.; Kipper, L.M.; Al Abri, A.A.; Cardoso, T.F.; López-Robles, J.R.; Cobo, M.J. (20202).20 years of scientific evolution of cyber security: A science mapping. In Proceedings of the International Conference on Industrial Engineering and Operations Management, Dubai, United Arab Emirates, 10–12 March 2020; 314–325.

Galinec, D., Možnik, D. & Guberina, B. (2017). Cybersecurity and cyber defence: national level strategic approach, Automatika, 58:3, 273-286, DOI: 10.1080/00051144.2017.1407022.

Gelo, O. C. G. (2012). On research methods and their philosophical assumptions: "raising the consciousness of researchers" again. Psychotherapie und Sozialwissenschaft,14(2): 111-130.

Giddens, A. (1984). *The constitution of society: outline of the theory of structuration*. Berkeley: University of California Press.

Given, L. M. (2008). In: *The SAGE encyclopaedia of qualitative research methods.* Thousand Oaks (CA): SAGE Publications, Inc.

Gould, J.L. & Kolb, W.L. (1964). A dictionary of the social science, The Free Press, New York.

Government Gazette. (2021). South African Government. National Departments. Available at: https://www.gov.za/about-government/government-system/national-departments/ (Accessed 16 July 2021).

Grinyer, P.H., Yasai-Ardekani, M. & Al-Bazzaz, S. (1980). Strategy, Structure, the Environment, and Financial Performance in 48 United Kingdom Companies, *Academy of Management*, 23(2). https://doi.org/10.5465/255427

Palmer, D. (2017). Misconfigured firewall blamed for hospital ransomware infection. ZDnet. Retrieved from http://www.zdnet.com/article/misconfigured-firewall-blamed-for-hospital-ransomware-infection/(Accessed 1 February 2017)

Pawlick, J., & Zhu, Q. (2021). Current Challenges in Cyber Deception. In Static and Dynamic Game Theory: Foundations and Applications (pp. 175-177). (Static and Dynamic Game Theory: Foundations and Applications). Birkhauser. https://doi.org/10.1007/978-3-030-66065-9_11

Penrose, E.T. (1959). *The theory of the growth of the firm*. Oxford: Oxford University Press.

Peters, M. (2018). Encyclopaedia of Educational Philosophy and Theory, 1st Edition, Springer: Singapore.

Perrin, A.J. & McFarland, K. (2011). Social Theory and Public Opinion. https://dx.doi.org/10.1146/annurev.soc.012809.102659

Pillay,Y. (2020). Human fallibility-the weakest link in cybersecurity. https://itweb.africa/content/xA9POvNZjzAvo4J8

Pinnock, B. (2020). What recent data breaches tell us about cybersecurity in South Africa. https://businesstech.co.za/news/industry-news/433797/what-recent-data-breaches-tell-813us-about-cybersecurity-in-south-africa/ (Accessed 4 May 2021).

Pinsonneault, A. & Kraemer, K. (1993). Research Methodology in Management Information Systems. Journal of Management Information Systems - Special Section: *Strategic and Competitive Information Systems Archive*, 10, 75-105.

Pistorius, T. & Mwim, O.S. (2019). "The impact of digital copyright law and policy on access to knowledge and learning." *Reading & Writing*, 10*(1)*, Gale Literature Resource Center,link.gale.com/apps/doc/A592955971/LitRC?u=anon~6af06ae0&sid=googleScholar&xid=3990e56a./(Accessed 2 July 2021).

Pokwana, U. & Kyobe, M.E. (2016). Investigating the Misalignment in the Existing e-Legislation of South Africa, Masters' Thesis, University of Cape Town, Cape Town.

Popper, K.R. (1983). *Realism and the Aim of Science*, pp 1-13. Routledge, London.

Porter, M.E. & Siggelkow, N. (2008). Contextuality within Activity Systems and Sustainability of Competitive Advantage, *Academy of Management Perspective*, 22(2):1-41.

Preller, W.J. (2021). Data breaches in terms of POPIA: what you need to know. https://www.vdt.co.za/NewsResources/NewsArticle.aspx?ArticleID=3984

Pribanic, E. (2018). The role of artificial intelligence in digital recruitment. https://www.techfunnel.com/hr-tech/the-role-of-artificial-intelligence-in-digital-recruitment/

Prior, B. (2020). The most common banking scams of 2020. https://mybroadband.co.za/news/banking/379566-the-most-common-banking-scams-of-2020.html/ (Accessed 1 March 2021).

Progress in International Reading Literacy Study [PIRLS] (2017). National Centre for Education Statistics. https://nces.ed.gov/surveys/pirls/

Punj, G. & Stewart, D.W. (1983). Cluster analysis in marketing research: Review and suggestions for applications, *Journal of Marketing Research*, 20:134-148.

PwC. (2018). Disrupting Africa: Riding the wave of the digital revolution. Paper presented at PricewaterhouseCoopers.

Quade, P. (2020). A deep dive into the universe of cybersecurity: The Digital Big Bang. World Economic Forum COVID Action Platform. [Online]. Available: www.weforum.org. (Accessed 8 February 2020).

Raimundo, R.J. & Rosario, A.T. (2022). Cybersecurity in the Internet of Things in Industrial Management, Applied Sciences, 12, 1598. https://doi.org/103390/app12031998 (Accessed 4 May 2022).

Romm, N. & Ngulube, P. (2014). Mixed methods research. In Mathipa, E.R. and Gumbo, M.T. (eds). Addressing research challenges: making headway for emerging researchers (in press).

Rowley, J. (2012). Conducting research interviews. Management Research Review, 35(3/4), 260- 271.

Ruel, E., Wagner, W.E. & Gillespie, B.J. (2016). The Practice of Survey research: theory and Applications, 1st edn, Amazon: SAGE.

SABRIC. (2017). Escalating Cybercrime: Banking clients' personal details accessed. (Online]http://www.sabric.co.za [Accessed 2 June 2018].

SABRIC.(2019), Crime Statistics 2019, viewed 10 December 2019, from http://www.sabric.co.za.

SABRIC. (2020), *Identity theft*, viewed n.d., from https://www.sabric.co.za/stay-safe/identity-theft/.

SADC Secretariat (2020). Towards a Common Future. https://www.sadc.int/sadc-secretariat/directorates/

SA Fraud Prevention Services (2019).Avoid becoming a victim of fraud/identity theft. https://www.safps.org.za

Safaricom (13 July 2016).Safaricom sued over alleged breach of privacy; company comments, https://www.business-humanrights.org/en/latest-news/kenya-safaricom-sued-over-alleged-breach-of-privacy-company-comments/

Salkind, N.J. (2018). *Exploring research.* 4th ed. Harlow: Pearson Education.

Saunders, M., Lewis, P. & Thornhill, A. (2012). *Research methods for business students*, 4th Edition. Harlow: Prentice Hall.

Saunders, M., Lewis, P. & Thornhill, A. (2016). *Research methods for business students*, 10th Edition. Harlow: Prentice Hall.

Saunders, M., Lewis, P., Thornhill, A. & Bristow, A. (2019). *Research methods for business students*, 8th ed., Harlow: Pearson Education.

Schmitt, N. (1996). Uses and abuses of coefficient alpha. *Psychological Assessment*, 8(4), 350- 353.

Schultz, C.B. (2016). Cybercrime: An analysis of current legislation in South Africa, Published Master's Dissertation, University of Pretoria. Pretoria.

Schofield, A. (2016). *2016JCSE ICT skills survey.* Johannesburg: Joburg Centre for Software Engineering (JCSE).

Schwab, A. (2016). *Recommendation for a second reading.A8-0211/2016.* Brussels: European Parliament. Retrieved from http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A8-2016-0211+0+DOC+PDF+V0//EN

Schwab, K. (2016). The Fourth Industrial Revolution: what it means, how to respond.[Online] Available at: https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond (Accessed 06 August 2020).

Schwab, K. (2019). *The Fourth Industrial Revolution*. World Economic Forum.

Shaw, M. (2017). *Hitmen for hire: Exposing South Africa's underworld.* Johannesburg: Jonathan Ball.

Shaw, M., & Thomas, K. (2016). The commercialization of assassination: "Hits" and contract killing in South Africa, 2000-2015. *African Affairs*, 1-24. https://doi.org/10.1093/afraf/adw050

Scotland, J. (2012). Exploring the Philosophical Underpinnings of Research: Relating Ontology and Epistemology to the Methodology and Methods of the Scientific, Interpretive and Critical Research Paradigms, *English Language Teaching*, 5(9):9-16.

Simonović, L. (2020). Are utilities doing enough to protect themselves from cyber-attacks? World Economic Forum. COVID Action Platform. [Online]. Available: www.weforum.org. (Accessed 9 May 2020).

Siponen, M. Vance, A.O. (2010). Neutralisation: New Insights into the problem of employee systems security policy violations, *MIS Quarterly*, 34(3);487-502

Smillie, S. (2019). Hackers give City of Joburg, banks until Monday to pay 'ransom'. https://www.iol.co.za/saturday-star/news/hackers-give-city-of-joburg-banks-until-monday-to-pay-ransom-35957235/ (Accessed 2 February 2020).

Smith, R.E., Richardson, V.J. & Watson, M.W. (2018). Much ado about Nothing: The (Lack of) Economic Impact of Data Privacy Breaches, *Journal of Information Systems*, 33(3):227-265.

Smits, J.M. (2010). The Complexity of Transnational Law: Coherence and Fragmentation of Private Law, *Electronic Journal of Comparative Law*, 14 (3):1-14.

Smits, J.M. (2010). 'Plurality of Sources in European Private Law, or: How to Live With Legal Diversity?', in: Brownsword, R., Micklitz, H., Niglia, L. & Weatherill, S. (eds.), *The Foundations of European Private Law*, Oxford: Hart Publishing.

Snail, S. (2009). Cybercrime in South Africa-Hacking, cracking and other unlawful online activities, *Journal of Information, Law and Technology*, http://go.warwick.ac.uk/jilt/2009_1/snail [22 June 2019].

Soin, K.& Paul, C. (2013). Editorial: Risk and Risk Management in Management Accounting and Control, Available at:https://core.ac.uk/download/pdf/43094694.pdf/ (Accessed 10 March 2020).

South Africa Government Gazette, 4. (2015). The National Cybersecurity Policy Framework, 39475 of 2002. Pretoria.

South African Post Office (2020). Postbank security breach highlights SASSA's failures. https://www.groundup.org.za/article/postbank-security-breach-highlights-sassas-failures/

Standard Bank South Africa (2019). External credit bureau data breach. https://www.standardbank.co.za/southafrica/news-and-media/newsroom/external-credit-bureau-data-breach.

State Security Agency, 2015). Report of the High-Level Review Panel on the SSA. https://www.gov.za/sites/default/files/gcis_document/201903/high-level-review-panel-state-security-agency.pdf

Statistics South Africa (StatsSA). (2019). Poverty trends in South Africa: An examination of absolute poverty between 2006 and 2011, 2015. Pretoria.

StatsSA, (2020). Report. Available at www.statssa.gov.za-annual report(Accessed 2 January 2021).

Stein, S. & Jacobs, J. (2020). 'Cyber-attack hits U.S. Health Agency amid COVID-19 outbreak', *Bloomberg*, viewed 20 March 2020, from https://www.bloomberg.com/news/articles/2020-03-16/u-s-health-agency-suffers-cyber-attack-during-covid-19-response.

Ster-Kinekor (2017). Cinema Chain Ster-Kinekor Hacked in South Africa' Biggest Data Breach. https://www.forbes.com/sites/tobyshapshak/2017/03/17/cinema-chain-ster-kinekor-hacked-in-south-africas-biggest-data-breach/?sh=2aca4c5fa109/

Stewart, J.M., Chapple, M. & Gibson, D. (2018). CISSP(ISC)2 Certified Information Systems Security Professional Official Study Guide, 7th edn, Amazon.CA

Straub, D. W., Gefen, D., & Boudreau, M.C. (2005). Quantitative Research. In D. Avison & J. Pries-Heje (Eds.), Research in Information Systems: A Handbook for Research Supervisors and Their Students (pp. 221-238), Amsterdam: Elsevier.

Straub, D.W. (1989). Validating instruments in MIS research, *MIS Quarterly*, 13(2)147-169.

Strous, L., von Solms, S. & Zúquete, A. (2020) Security and Privacy of the Internet of Things, Computers and Security, 102. 1-3. Available at: https://doi.org/10.1016/j.cose.2020.102148. (https://www.sciencedirect.com/science/article/pii/S0167404820304211).

Sullivan,J.V. (2010). How our laws are made. House Document:110-149, House of Representatives, United States of America. https://www.congress.gov/help/learn-about-the-legislative-process/how-our-laws-are-made

Sutherland, E. (2017). Governance of cybersecurity-The case of South Africa, The African *Journal of Information and Communication*, 20, Online version https://dx.doi.org/10.23962/10539/23574/html

Takeuchi, H. and Nonaka, I. (1986) The New New Product Development Game. *Harvard Business Review*, 64:137-146.

Tashakkori, A. & Creswell, J.W. (2007). The new era of mixed methods, *Journal of Mixed Methods Research*, 1(1):3–7. DOI: 10.1177/2345678906293042.

Tashakkori, A., & Teddlie, C. (2003). The past and future of mixed methods research: From data triangulation to mixed model designs. In A. Tashakkori & C.Teddlie (Eds.), Handbook of mixed methods in social & behavioural research (pp. 671-702). Thousand Oaks, CA: Sage.

Teddlie, C. & Tashakkori , A. (2008). *Foundations of Mixed Methods Research Integrating Quantitative and Qualitative Approaches in the Social and Behavioural Sciences.* s.l.: SAGE Publications, Inc.

Teddlie, C., & Yu, F. (2007). Mixed methods sampling: A typology with examples. *Journal of Mixed Methods Research*, 1(1):77-100.

Tejada, J. J., & Punzalan, J. R. B. (2012). On the Misuse of Slovin ' s Formula. The Philippine Statistician, 61(1):129-136.

Telegraph, 2014). https://www.telegraph.co.uk/house-of-commons/

The Business News (4 June, 2016). List of data breaches and cyber-attacks in June 2016 (289,150,000 + records leaked). https://www.itgovernance.co.uk/blog/list-of-data-breaches-and-cyber-attacks-in-june-2016-135000000-records-leaked.

The Human Rights Watch (2012). International Human Rights Clinic. https://www.hrw.org/sites/default/files/reports/arms1112_ForUpload.pdf/

Trim, P. & Lee, Y.I. (2016). Cybersecurity Management, 1ts edn, London: Routledge

Trochim, W. M. (2020). *Research Methods Knowledge Base,* Sydney: Conjoint.ly.

United Nations Conference on Trade and Development [UNCTAD], (2009). Harmonising Cyberlaws and Regulations: The Experience of the East African Community. United Nations.

United Nations (2019). United Nations Confirms "Serious"Cyber-attack With 42 core servers compromised.https://www.forbes.com/sites/daveywinder/2020/01/30/united-nations-confirms-serious-cyberattack-with-42-core-servers-compromised/?sh=b6571f3633da

United Nations [UN] (2021). United Nations suffers data breach. https://www.securitymagazine.com/articles/94325-united-nations-suffers-data-breach

Van der Merwe, D. (2008). Criminal Law– Your partner in preventing information loss, Presented at the Lex Informatica, 23 May 2008 at the Innovation Hub.

van der Merwe, D. (2016). A comparative overview of the (sometimes uneasy) relationship between digital information and certain legal fields in South Africa and Uganda, Available at: http://www.scielo.org.za/pdf/pelj/v17n1/08.pdf/ (Accessed 19June 2019).

van der Merwe, D.P., Roos, A., Pistorius, T., Elselen, G.T.S. & Nel, S. S.(2016).Information and Communication Technology Law, 2nd edn, https://www.loot.co.za/product/d-p-van-der-merwe-information-and-communications-techn/nmtp-3098-g330.

Van de Ven, A. & Robert, R. (1985). Alternative forms of Fit in Contingency Theory, *Administrative Science Quarterly*, 30(4):514-539.

Van Niekerk, J. F., & Von Solms, R. (2010). Information security culture: A management perspective. *Computers & Security*, 29(4), 476-486. doi:https://doi.org/10.1016/j.cose.2009.10.005

Van Wyk, MM. (2012). Measuring Student's Attitudes to Economics Education: A Factorial analysis approach, *Journal Social Science*, 31 (1):1-42.

Venkatraman, N. (1989). The Concept of Fit in Strategy Research: Toward Verbal and Statistical Correspondence, *The Academy of Management Review*, 14(3):423-444.

Venkatraman, N., & Prescott, J.E. (1990). Environment-strategy co-alignment: an empirical test of its performance implications, Strategic Management Journal, 11(1), 1–23.

Venkatesh, V., Brown, S. A., & Bala, H. (2013). Bridging the qualitative-quantitative divide: Guidelines for conducting mixed methods research in information systems, *MIS Quarterly*, 37(1):21-54.

Verizon, 2016). Verizon's 2016 Data Breach Investigations Report Finds cybercriminals are exploiting human nature. https://www.verizon.com/about/news/verizons-2016-data-breach-investigations-report-finds-cybercriminals-are-exploiting-human

Vlachos, V. (2011). The landscape of cybercrime in Greece, *Information Management and Computer Security*, 19(2):113-123.

Von Solms, R. & Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, 38: 97-102.

von Solms, R., & von Solms, B. (2015). National Cyber Security in South Africa: A Letter to the Minister of Cyber Security. In The Proceedings of the 10th International Conference on Cyber Warfare and Security: ICCWS2015 (p. 369). Kruger National Park: Academic Conferences Limited.

Von Solms, B. & von Solms, R. (2018). Cybersecurity and Information security-what goes where?, *Information and Computer Security*, 26(1). Available at: https://www.researchgate.net/publication/322792154_Cyber_security_and_information_security_-_what_goes_where: DOI:10.1108/ICS-04-2017-0025

Von Solms, S. & Marnewick, A. (2019). Identifying Security Requirements Body of Knowledge for the Security Systems Engineer, IFIP World Conference on Information Security Education, 59-71, Springer, Charm. https://scholar.google.co.za/citations?view_op=view_citation&hl=en&user=ljlPC68AAAAJ&citation_for_view=ljlPC68AAAAJ:kNdYIx-mwKoC

Walsham, G. (2012). Are we making a better world with ICTs & quest: Reflections on a future agenda for the IS field, *Journal of Information Technology*, 27(2):87-93.

Wangwe, C. K., Eloff, M. M. and Venter L. M., (2012), A Sustainable Information Security Framework for e-Government - Case of Tanzania, *Technological and Economic Development of Economy Journal*, 18(1):117–131.

Warren, B.C. (2012). Challenges to Criminal Law Making in the New Global Information Society: A Critical Comparative Study of the Adequacies of Computer-Related Criminal Legislation in the United States, the United Kingdom and Singapore; 2-4.

Weekend Argus (2018). British Airways settles with victims of 2018 data breach. https://www.iol.co.za/technology/software-and-internet/british-airways-settles-with-victims-of-2018-data-breach-93b01a3b-7c1c-43d5-a90b-f770bc25f9cb

Wells, L., Camelio, J., Williams, C. and White, J., 2014. Cyber-physical security challenges in manufacturing systems. *Manufacturing Letters*, 2(2):74-77.

Wilson, T.D. (1999). Models in Information Behaviour Research, *Journal of Documentation*, 55(3):249-270.

WhatsApp Inc (2019). WhatsApp security breach may have targeted human rights groups. https://www.reuters.com/article/us-facebook-cyber-whatsapp-idUSKCN1SK0SM

White, K. (2020). *Life healthcare reports hacking attack*, viewed 14 June 2020, from https://www.businessday.co.za.

Wolff, P. & Holmes, K.J. (201). Linguistic Relativity. Cognitive Science, 2(3):253-265.

World Bank (2017). Combating Cybercrime: Tools and Capacity building for Emerging Economies:https://documents1.worldbank.org/curated/en/355401535144740611/pdf/129637-WP-PUBLIC-worldbank-combating-cybercrime-toolkit.pdf/html (Accessed 16 April 2022

World Bank (2019). World Bank Annual Report: Available: https://documents.worldbank.org/ (Accessed 12 September 2020).

World Bank (2020). World Bank's Network Breached. https://www.bankinfosecurity.com/world-banks-network-breached-a-1008

World Economic Forum. (2020). The Global Competitiveness Report. Available from: www3.weforum.org-docs. (Accessed: 2 June 2021).

World Economic Forum (2019). Global Risks Report: Global Risks Perception Survey 2018-2019. [Online]. Available: https://www3.weforum.org. (Accessed 9 March 2020).

World Health Organisation (WHO), (2020). *Beware of criminals pretending to be WHO*, viewed 24 May 2020, from https://www.who.int/about/communications/cyber-security.

Wolf, L. (2015). The National Prosecuting Authority (NPA) in a nimbus between the executive and the judicature. *Administratio Publica*, 23(4), 30-53.

Zuma v DA (771/2016 & 1170/2016) [2017] ZASCA 146 (13 October 2019). Retrieved from http://www.saflii.org/za/cases/ZASCA/2017/146.html

Yahoo (2014). Yahoo says hackers stole data from 500 million accounts. https://www.reuters.com/article/us-yahoo-cyber-idUSKCN11S16P

Yin, R. K. (2014). Case study research: Design and methods. Thousand Oaks, CA: Sage Publications.

Yoon, K.M. (2021). The World Bank's efforts in combating Cybercrime and the importance of international Cooperation, in "Combatting Cybercrime: Tools and Capacity Building for Emerging Economies" 2017, World Bank; available at: www.combattingcybercrime.org/html.Counsel, Legal Vice Presidency, The World Bank. (Accessed 18 April, 2022)

Yusif, S. & Hafeez-Baig, A. (2021). A conceptual Model for Cybersecurity Governance, *Journal of Applied Security Research*, 16(4):1-24

Zhang-Kennedy, l & Chiasson, S. (2020). A Systematic Review of Multimedia tools for Cybersecurity Awareness and Education, ACM Computing Surveys, 54(12):1-39.

APPENDIX A: QUESTIONNAIRE

Towards an aligned South African National Cybersecurity Policy Framework

Department of Information Systems

Researcher:

Joel Chigada

Email: chigadajm@gmail.com

Cell: +27 74 535 6824

Tel: +27 21 959 2578

Dear Participant

My name is Joel Chigada, a PhD candidate in the Department of Information Systems, Faculty of Commerce at University of Cape Town. Currently, I am conducting research on "***Towards an aligned South African National Cybersecurity Policy Framework",*** therefore, I invite you to participate in this study. The University of Cape Town, Faculty of Commerce Ethics in Research Committee has approved and granted permission to proceed with the study. Your participation in this study is voluntary and you are free to withdraw from the study anytime. Your responses will be treated in the strictest confidence, remain confidential and will be invaluable to completing this study. You will not be requested to supply any identifiable or sensitive information in this research. The questionnaire will take approximately 15 minutes to complete. By completing this questionnaire, you implicitly give consent to take part in the research study. Should you have any questions regarding the research please feel free to contact the researcher.

SECTION A: DEMOGRAPHIC INFORMATION

In this section, you are requested to mark your answer with an X.

What is your gender?

Gender	
Male	
Female	
Non-binary	

What is your age?

18-24 years	
25-44 years	
45 years +	

What is your highest qualification?

National Diploma	
Bachelor's Degree	
Honours	
Masters Degree	
Doctorate	
Other (specify)	

What is your current position/title

Manager (Specify)	
Hon Member of Parliament	
Honourable Minister	
Information Systems Engineer	
Legal Expert	
Chief Information Security Officer	
Cybersecurity Specialist	
Law Enforcement Agent	
Fraud Specialist	
IT Professional	
Academic	
IT Director	
Chief Information Officer	
Systems Analyst	
Cybersecurity Strategist	
Developer	
Telecoms Engineer	
Network Engineer	

What is your experience

<1 year	
1-5 years	
6-10 years	
11-20 years	
21 years +	

Indicate your race

Black	
White	
Indian	
Coloured	
Asian	
Other (specify)	

SECTION B: CYBERSECURITY

In this section, you are requested to select only one choice that represents your viewpoint. Regarding cybersecurity. Please indicate your level of agreement with the following statements:

Variable

LIMITED UNDERSTADING OF CYBERSECURITY (CS)	**Strongly Disagree**	**Disagree**	**Somewhat disagree**	**neither agree or disagree**	**Somewhat Agree**	**Agree**	**Strongly agree**
Q8. Overreliance on ICTs is creating opportunities for cybercrimes, attacks and threats leading to conflicting understanding of cybersecurity	**1**	**2**	**3**	**4**	**5**	**6**	**7**
Q9. Conflicting terminology	**1**	**2**	**3**	**4**	**5**	**6**	**7**
Q10. Lack of sharing of cybersecurity information and knowledge hinders people from understanding cybercrime.	**1**	**2**	**3**	**4**	**5**	**6**	**7**
Q11. No education and awareness programmes	**1**	**2**	**3**	**4**	**5**	**6**	**7**

SECTION C: FACTORS CONTRIBUTING TO MISALIGNMENT OF E-LEGISLATION

Kindly select the option that represents your opinion.

SLOW LAW-MAKING PROCESS AND REGULATORY ENVIRONMENT (LMPRE)							
The South African Cyber Regulatory Landscape comprises: Common Law; Electronic Communications and Transactions Act; Interception and Monitoring Prohibition Act; Financial Intelligence Centre Act; King Code IV and National Cybersecurity Policy Framework and Revised Bill on Cybercrimes							
	Strongly agree	**Disagree**	**Somewhat disagree**	**Neither agree or disagree**	**Somewhat agree**	**Agree**	**Strongly agree**
Q12. The law- making is slow and time consuming	**1**	**2**	**3**	**4**	**5**	**6**	**7**
Q14. Inconsistencies of approaches in addressing cybercrimes due to multiple pieces of legislation and agencies.	**1**	**2**	**3**	**4**	**5**	**6**	**7**
Q16. Fragmented and misaligned pieces of e-legislation	**1**	**2**	**3**	**4**	**5**	**6**	**7**
Q18. Lawmakers lack adequate knowledge of the law-making process.	**1**	**2**	**3**	**4**	**5**	**6**	**7**
MULTIPLE AGENCIES AND INFORMATION SYSTEMS (MAIS)							
The existence of two legislative bodies- National Council of Provinces and National Assembly and different pieces of e-legislation creates multiple parties involved in the development, implementation and coordination of legislation resulting in incoherencies of the laws.							
Q19. Overlapping mandates that create conflicts resulting in inconsistencies.	**1**	**2**	**3**	**4**	**5**	**6**	**7**

Q20. Each piece of legislation addresses only one aspect of cybersecurity	**1**	**2**	**3**	**4**	**5**	**6**	**7**
Q21. Multiple agencies do not share their strategies on how to mitigate/reduce cybercrimes	**1**	**2**	**3**	**4**	**5**	**6**	**7**
Q22. Multiple incoherent information systems impede alignment of e-legislation.	**1**	**2**	**3**	**4**	**5**	**6**	**7**
Q24. The presence of multiple information systems requires more IT and legal expertise.	**1**	**2**	**3**	**4**	**5**	**6**	**7**
MONITORING AND CONTROL (SECURITY CONTROLS) (MC)							
Monitoring and control mechanisms are designed to safeguard information systems against cyber-attacks , crimes and threats. The most important security controls include: maintaining an inventory of authorised and unauthorised hardware and software; securing configurations for hardware and software; securing configurations for network devices such as firewalls and routers; boundary defence; maintenance and analysis of complete security audit logs; application software security; controlled use of administrative privileges; controlled access based on need to know; continuous vulnerability testing and remediation; dormant account monitoring and control; anti-malware defences; limitation and control of ports, protocols and services; wireless device control,; data leakage control; secure network engineering; red team exercise; incident response capabilities; disaster recovery capability and security skills assessment and training.							
Q25. Absence of controls and protocols in an information security strategy.	**1**	**2**	**3**	**4**	**5**	**6**	**7**
Q26. Intrusion detection systems help to curb unauthorized access to data and information systems.	**1**	**2**	**3**	**4**	**5**	**6**	**7**
Q28. It is difficult to determine which security controls are effective when multiple agencies and information systems are in use.	**1**	**2**	**3**	**4**	**5**	**6**	**7**
LACK OF SKILLS IN CYBERSECURITY (SIC)							
Q30. The shortage of cybersecurity (IT) and legal skills and expertise hinders the law-making process.	**1**	**2**	**3**	**4**	**5**	**6**	**7**
Q31. The existence of multiple information systems depletes the few IT and legal skills available.	**1**	**2**	**3**	**4**	**5**	**6**	**7**
Q32. IT specialists are outpaced by sophisticated cybercriminals.	**1**	**2**	**3**	**4**	**5**	**6**	**7**
Q33. Expanding cyber education will help address shortage of cybersecurity (IT) and legal skills.	**1**	**2**	**3**	**4**	**5**	**6**	**7**
Q34. Appoint the right people at every level to identify, build and staff defences and responses.	**1**	**2**	**3**	**4**	**5**	**6**	**7**
KNOWLEDGE AND INFORMATION SHARING (KIS)							
Cyber security incidents are constantly increasing in frequency and magnitude, becoming more complex and unconstrained by borders. Firms can share information relating to their role and responsibilities to strengthen cybersecurity both nationally and globally; network information security; security controls dealing with specific cyber-attacks and threats; regulation; law							

enforcement; developing cyber defence policy and capabilities; cross-sector information on industry standards and trends; sector regulation challenges and successes							
Q35. Persistent silo approach hinders information and knowledge sharing	**1**	**2**	**3**	**4**	**5**	**6**	**7**
Q37. Fear of exposing state secrets or information hinders information sharing	**1**	**2**	**3**	**4**	**5**	**6**	**7**
Q38. Fear of exposing intellectual property impedes information sharing	**1**	**2**	**3**	**4**	**5**	**6**	**7**
UNACCEPTABLE USER BEHAVIOUR (PICL)							
Q40. People's behaviour can stifle the pace of implementation of cyberlaws	**1**	**2**	**3**	**4**	**5**	**6**	**7**
Q42. Inadequate resources affect the pace of implementation of cyberlaws.	**1**	**2**	**3**	**4**	**5**	**6**	**7**
Q43. Resistance to change slows the pace of implementation of cyberlaws	**1**	**2**	**3**	**4**	**5**	**6**	**7**
ABSENCE OF A CYBERSECURITY CULTURE (CSC)							
Information Security Culture entails the attitudes, assumptions, beliefs, values and knowledge that stakeholders use to interact with the firm's systems and procedures at any point in time. The interactions result in acceptable or unacceptable behaviour or incidents that become part of the way things are done in the organisation to protect its information assets. Literature acknowledges that information security culture changes over time.							
Q44. Overreliance on ICTs forces firms to develop a cybersecurity culture	**1**	**2**	**3**	**4**	**5**	**6**	**7**
Q45. Cybersecurity culture is sustainable and it transforms security from a one-time event into a lifecycle	**1**	**2**	**3**	**4**	**5**	**6**	**7**
Q46. Cybersecurity culture fosters change and better security.	**1**	**2**	**3**	**4**	**5**	**6**	**7**
Q47. A strong security culture defines how security influences the services that a firm provides to its stakeholders.	**1**	**2**	**3**	**4**	**5**	**6**	**7**
Q48. Modern security culture enables users to work in the way they want, inside or outside the corporate work.	**1**	**2**	**3**	**4**	**5**	**6**	**7**
INCOHERENT AND FRAGMENTED LEGISLATION (MANY GLOBAL CYBERLAWS (EGCL)							
Various global cyber laws have been developed and implemented. These include: Model Law on Computer and Computer-related crime; SADC Model Law on Computer Crime and Cybercrime; Harmonization of ICT Policies, Legislation and Regulatory Procedures in the Caribbean; International Telecommunications Union Cybercrime Resources; Cybercrimes and Security Bill (South Africa); Cybersecurity Information Sharing Act (CISA) (USA), European Union Network and Information Security Directive, Criminal Code Act 1995 of Australia, Cybercrime Act 2001 of Australia, Criminal Code of Canada, Cybersecurity Law of China, Criminal Code-France, Cybercrimes Prevention Act of Malaysia, Cybercrimes Act 2015 of Tanzania and the UK Misuse Act, 2013.							
Q51. The existence of multiple global cyberlaws creates confusion	**1**	**2**	**3**	**4**	**5**	**6**	**7**
Q52. The unprecedented rate of technological developments creates challenges for formulating new laws and amendments of existing ones from time to time.	**1**	**2**	**3**	**4**	**5**	**6**	**7**

Q53. The existence of different cyberlaws creates pressure on countries to develop coherent legislation	**1**	**2**	**3**	**4**	**5**	**6**	**7**
Q54. There is need for BYOD policies to mitigate cyber-attacks	**1**	**2**	**3**	**4**	**5**	**6**	**7**
Q55. With the increased usage of mobile devices, mobile law emerges as an area of jurisprudence.	**1**	**2**	**3**	**4**	**5**	**6**	**7**

Strictly confidential

Thank you for your participation.

APPENDIX B: ETHICAL CLEARNACE

Faculty of Commerce
Private Bag X3, Rondebosch, 7701
2.26 Leslie Commerce Building, Upper Campus
Tel: +27 (0) 21 650 4375/ 5748 Fax: +27 (0) 21 650 4369
E-mail: com-faculty@uct.ac.za
Internet: www.uct.ac.za
@Commerce_UCT **UCT Commerce Faculty Office**

05/01/2018

Mr Joel Chigada
Department of Information Systems
University of Cape Town

REF: REC2018/001/005

Dear Joel Chigada

Project : **Evaluating Factors Contributing to misalignment oft he South African National Cyber-security Policy Framework.**

It is a pleasure to inform you that the EiRC has **formally approved** the above-mentioned study.

Approval is granted for the period of 12 months. Should you require an extension or make any substantial changes to the research methodology which could affect the experiences of participants, you must submit a revised protocol to the Committee for approval.

Please note that the ongoing ethical conduct of the study remains the responsibility of the principal investigator.

Your sincerely

Litha Tyulu
Administrative Assistant
University of Cape Town
Commerce Faculty Office
Room 2.26 | Leslie Commerce Building

Office Telephone: +27 (0)21 650 2695
Office Fax: +27 (0)21 650 4369
E-mail: litha.tyulu@uct.ac.za
Website: www.commerce.uct.ac.za<http://www.commerce.uct.ac.za/