3-27-2024

Cybersecurity Fiscal Statecraft Conundrums in South Africa

Sabelo Lyndon Mbokazi
Walden University

Walden University

College of Health Sciences and Public Policy

This is to certify that the doctoral dissertation by

Sabelo Mbokazi

has been found to be complete and satisfactory in all respects,
and that any and all revisions required by
the review committee have been made.

Review Committee
Dr. Ernesto Escobedo, Committee Chairperson,
Public Policy and Administration Faculty

Dr. Karel Kurst-Swanger, Committee Member,
Public Policy and Administration Faculty

Chief Academic Officer and Provost
Sue Subocz, Ph.D.

Walden University
2024

Abstract

Cybersecurity Fiscal Statecraft Conundrums in South Africa

by

Sabelo Mbokazi

MCom, University of KwaZulu Natal, 2011

BA, University of Zululand, 1992

Dissertation Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Philosophy

Public Policy and Administration

Walden University

May 2024

Abstract

Cybersecurity is a major global concern that is gaining traction in domains of governance and policy debates geared toward protection of digital infrastructure and information systems in public and private sectors. Cyberspace disruptions and uncertainties manifest in events of hacking and cyberattacks mounted by adversaries which are ubiquitous and form a major part of the organizational risk matrix. The purpose of this qualitative case study was to explore and describe cyber-threat conditions caused by the Denial-of-Service (DoS) cyberattack, the negative effects of DoS on cyber resilience and vulnerability of digital data and information assets, and the resultant conundrum of government fiscal planning and budgeting for cybersecurity in South Africa. The semistructured interviews were conducted with 10 participants who were senior officials of the Government Communication Information System and National Cybersecurity Hub, South Africa. Findings from coding and thematic analysis by NVivo qualitative data analysis included South Africa data which was collected during interviews and archival research in respect to country cybersecurity strategies to circumvent, prevent, and recover from instances of cyber-threat events. The findings revealed that international markets drive high price factor of cybersecurity equipment and devices, thus impeding South African government to achieve optimal budgeting for the cybersecurity. Findings also highlighted importance of affiliation to the global Forum for Incident Security Response Team (FISRT) which tracks the cyberattack events. Findings provided information and strategies that organizations can apply for positive social change to mitigate the impact of cyber-threat events such as DoS cyberattacks to strengthen cybersecurity.

Cybersecurity Fiscal Statecraft Conundrums in South Africa

by

Sabelo Mbokazi

MCom, University of KwaZulu Natal, 2011

BA, University of Zululand, 1992

Dissertation Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Philosophy

Public Policy and Administration

Walden University

May 2024

Dedication

I dedicate this dissertation to my parents. Dr. Simon Zwelibanzi Mbokazi and Mrs. Greta Senzangani Mbokazi who laid the foundation for the zeal to embark on PhD study journey and the resilience to soldier on till the end. Your enduring countenance, love and encouragement sustained my aspiration to reach the pinnacle of the academic hierarchy. It is for this reason that I will forever be grateful to you my dear parents.

Acknowledgements

Completing this research study is a culmination of efforts that were both demanding, rewarding and reflected the contribution of many individuals who were instrumental in sustaining my motivation to reach the finish line.

I cannot thank enough the dissertation committee members: the Chair Dr. Ernesto Escobedo and the methodology expert Dr. Karel Kurst-Swanger for the tremendous, guidance and inspirational support during the entire process.

Special recognition goes to the participants who did not only share insights, experiences and expertise but also their valuable time.

My siblings are a pillar of strength and Mbokazi family at large are oozing with a pioneering positive energy which invigorated me to pursue my research with requisite passion and enthusiasm. Thank you, my sons Langa, Sithabiso and Mfundo and my wife Mrs. Hlanze Mbokazi for your amazing support and landing me an ear to tell the stories on milestones of my study journey.

Table of Contents

List of Tables

List of Figures

Chapter 1: Introduction to the Study

More than ever before the global community is experiencing extensive proliferation and super penetration of Internet of Things (IoT), information, communication and technology (ICTs), artificial intelligence (AI), computer-mediated communication (CMC), mobile computing, cloud computing, quantum mechanics, software and hardware applications, big data analytics, and technological advancement in the most ubiquitous way to the extent of existential dependency (Jonas & Burrell, 2019; Srinivas et al., 2018; Wang et al., 2018; Wilner, 2018). The connectivity, split of a second service consumption, speed, and agility have transformed the operations and ways of doing work in government, business, civil society sectors, and at the individual level (Chatfield & Reddick, 2018). Significant efficiency gains at various levels of operations in the workplace demonstrates the catalytic utility and value yielded upon deployment and employment of integrated ICT and IoT to drive business operations in all the sectors; business operations that could take a week's worth of traveling to conferences can now be executed via numerous meeting virtual platforms including Zoom, Microsoft Teams, and Webex. Governments, the private sector, and all other sectors are engaged in deploying not only the cyber systems policy frameworks only but also substantial financial investments to procure advanced fourth industrial revolution technology products (Vance et al., 2012).

Although the demand for use of the digital space has increased across the world in every sector, cyber space is confronted by challenges that are increasing at an exponential rate (Taewoo, 2019). This is due to the interaction between digital space (that is

extensively interfaced and networked with cyberspace communication tools, ICT, IoT, software and hardware, and devices) with the cyber-threat landscape characterized by unprecedented cyber risks, vulnerabilities, and enormous uncertainties (UNIDIR Report, 2017). The economies of the world are become highly digital; therefore, the governments are becoming dependent on cyberspace (Celik & Gurkaynak, 2019). The literature has established that governments bear the responsibility to build strong cybersecurity technical depth to protect citizens through deploying an integrated cyber-defense systems against the intensifying surge of cyberattacks, cyberterrorism, cyber espionage, and cyberwars waged within the digital space. Furthermore, research reports provided two cybersecurity subdimensions: the technical dimension, which is anchored on computer-mediated information technologies and applications, and the social dimension, which pronounces political and legal practices concerning national security concerns (Celik & Gurkaynak, 2019). An overview perspective on French cybersecurity chronicled by Vitel & Bliddal (2015) equated cyberspace with the jugular vein upon which modern society owes its existential dependence.

Research on cybersecurity acknowledged an unprecedented increase in the proliferation of offline criminal activities. Criminal activities and threats have penetrated the online domain in alarming proportions (Vitel & Bliddal, 2015). Consequently, investing and establishing in a cybersecurity framework that is confidence building, stable, resilient, cyberattack tolerant, and predictable is neither a choice nor an option but a strategic imperative for organizations and governments (Andreasson, 2018). Governments are compelled to deal with this conundrum by providing optimum

budgeting to deploy cyber-defense architecture and infrastructure that is responsive, agile, and resilient to protect and preserve the digital assets of the states. Although cybersecurity proponents highlight optimal budgeting for cybersecurity as policy imperative for governments, the literature stated a caveat that the extensive proliferation of Industry 4.0 and IoT induces an affinity to expand the cyberattack surface area and cyber-threat landscape, and the cost to address potential subversion of the cyberspace systems is exorbitant (Lees et al., 2018).

Juxtaposing and probing the conundrums emanating from DoS cyberattacks and its causal effects to optimal budgeting and financing for cybersecurity is a necessary research focus. The focus of this research is the constituent dimensions and dynamics including the unlimited nature of cyberspace, the ubiquitous IoT, and the rapid emergence and spiraling intrusion of DoS cyberattacks causing damage to the information system or rendering inaccessible the computer data (Wang et al., 2018). Although the literature identified a vast array of cyberattacks and cyber threats, this research study was confined to investigating conundrums associated with DoS cyber threat and optimal budgeting as a government function (see Quigley et al., 2015). The devastating impact of DoS cyber threats to crash the service or cause flooding of the network, thereby rendering the service unavailable, is dire and costly (Fielder et al., 2018).

The advent of cyberattacks has created antagonism toward the optimism associated with revolutionary efficient utility of digital infrastructure and CMC, which is driven by IoT (Fielder et al., 2018). Although cyberspace networks offer an

unprecedented agility for workflow and service delivery for organizations and societies, the literature indicated that an exponential increase of cyberattacks constitutes an existential societal challenge (Zoto et al., 2019). Consideration of the interplay between the cybersecurity exigencies and inevitable need for business continuity generates a sociotechnical dilemma for organizations (Zoto et al., 2019). Andreasson (2011) pointed out that the consequence of heavy dependence on ICT and IoT networks, which have become basic tools for trade for organizations and individuals, is a vulnerability in cyberspace. Staying ahead of the rapid emergence and uncertainties induced by cyber risks, governments are required to address a challenge to instill preventive psychology among employees through awareness training, national cybersecurity policies, budgets, and standard operating procedures to mitigate the adverse impact of cyber threats such as DoS (Quigley et al., 2015).

Chapter 1 of the current study consists of the background of the study, which provides details on the nexus between the cyberspace instruments and communication tools, the associated conditions of cyberattacks, vulnerabilities, and the optimal budgetary difficulties for governments. The first chapter also presents the problem statement, which frames the problem that this study addressed and the research gap in the literature concerning the phenomenon of concern. Furthermore, Chapter 1 presents the purpose of this study and how it is connected with the problem statement. This chapter also covers the research questions, the theoretical framework, and the nature of the study. The last aspects covered in Chapter 1 include definitions, assumptions, delimitations, limitations, significance, and a summary.

Background of the Study

Situating Cybersecurity in Global Governance Architecture

The international security environment is experiencing constant changes (Swiatkowska, 2017). This trajectory is evident in cyberspace, and due to the increase of cybercrime and the growing sophistication of cyberattacks, the international cyberspace stability and resilience have been compromised (Margulies, 2017). Governments are compelled to contend with cyberspace disruptive operational havoc and spiraling costs, budgetary allocations, and investments. Governments and organizations are considering cybersecurity as a strategic security risk requiring attention (Ogut et al., 2011). Cybersecurity is gaining traction in global governance and policy debates because it forms an integral part of the globalized world and security concern (Craig, 2018). The vulnerabilities of the digital space due to the agile, sophisticated, persistent, and hard to predict cyberattacks is a reality (Craig, 2018). The digital infrastructure of several organizations and governments have experienced physical and electronic damage leading to devastating loss of data and intellectual property due to malicious cyberattacks (Pătrașcu, 2018). The discourse on cybercrime is attracting attention, with global concerted efforts undertaken to create more sensitization and awareness building among organizations and governments to take a proactive pro-cybersecurity policy posture as considerable efforts to protect digital infrastructure and information systems in public and private sectors (Dor & Elovici, 2016).

An idiosyncratic trait about cyberspace exemplified by the internet is that it is a shared global network and a public good (Mikesell, 2014). Cybersecurity is a challenge

that requires the collective effort of public and private sectors at the domestic and global levels (Ogut et al., 2011). Although stewardship of cyberspace and cybersecurity transcends global and transnational ramifications, adverse and substantial losses are more keenly felt at individual, government, and private firm levels (Margulies, 2017). In this regard, the cyber risk complexities characterized by detrimental threats to prevention, mitigation, and recovery interventions give rise to challenges to attaining optimal budgetary allocations and investments.

The 21st century is experiencing exponential increase and proliferation of ICT gadgets and digital technologies and expanded utilization of CMC systems such as the internet, which is a driver of everyday workflow in almost all industries in private and public sectors (Chaudhuri & Ghosh, 2012). Ubiquitous connectivity powered by the IoT was estimated to facilitate connectivity of approximately 20 billion gadgets by 2020 (Chaudhuri & Ghosh, 2012).This is exemplified by evolving internet-based systems such as e-learning, e-governance, e-commerce, e-health, and e-videoconferencing (Craig, 2018). Adversely, the research literature on cybersecurity demonstrated that along with the proliferation of electronic technology, cybercrime incidents are on the rise and can be detrimental to computerized digital systems. This could lead to catastrophic harm to information systems in the workplace (Cavelty, 2018).

Cyberspace is characterized by a sophisticated global scale of interconnected ICT networks (Craig, 2018). One cyberspace failure can escalate to a national or global crisis with far-reaching consequences in the cyber techno-infrastructure (Schneider, 2018). Governments are adopting policies to prevent cyberattacks on critical infrastructure to

reduce national vulnerabilities. The expansive interconnected ecological digital infrastructural networks and dependency of governments, organizations, and individuals on cyberspace to perform basic daily operation such as communication through internet is not without challenges (Lees et al., 2018). Deploying diversified digital defense infrastructure often inadvertently creates large a cyberattack surface area, thereby increasing the vulnerability of the digital infrastructure, information systems, and data assets to attacks (Njilla et al., 2017).

The response of governments and organizations involving multifaceted cyber threats requires substantial investments to bolster cybersecurity and to safeguard cyberspace infrastructure (Srinidhi et al., 2015). Out of the shrinking fiscal space due to slow economic growth and a number of other global factors, governments are confronted with the requirement to divert more resources to cybersecurity (Srinidhi et al., 2015). If not addressed, the risks associated with cyber threats could grow into a transnational concern with catastrophic impact on government and private sectors' digital assets and CMC infrastructure security (Schneider, 2018).

In 2010, Iran's critical infrastructure experienced a malicious cyberattack by a STUXNET computer virus that affected the nuclear power (Patrascu, 2018). Experts in cyber technology confirmed that STUXNET was a sophisticated computer virus developed by cyber criminals with deep knowledge of supervisory control and data acquisition through which they infiltrated and sabotaged the Iranian nuclear power system (Patrascu, 2018). The Iran cyberattack incident shocked the world, catapulted cybersecurity to a global priority, and raised awareness of the disruptive nature of

cyberattacks and how they can be used to attack national CMC infrastructure, digital assets, and systems. The research output on cybersecurity increased in 2012 as the world developed strong interest to understand cybersecurity (Cavelty, 2018). Policy development and debates on government strategies and public budgets on cybersecurity also began to experience traction among the practitioners in domains of public and private spheres of workplace and governance (Schneider, 2018).

Cybersecurity and Electronic Technology

Cybersecurity is a phenomenon that is embedded in digital technology. Cybersecurity is traced from the proliferation of the digital technologies and activities residing in cyberspace (Cavelty, 2018). Cybersecurity is gaining momentum and is featured in national state craft in various countries, particularly as a policy issue that requires budget allocation. In 2018, research pointed out that in a period of 15 years countries that adopted cybersecurity strategic plans and policies were well over 70 in total (Patrascu, 2018). Cybersecurity is a significant emerging phenomenon located in the cyberspace and interwoven with ICT, particularly the internet network (Njilla et al., 2017).

Furthermore, technologies embedded in cyberspace are dynamic and change frequently in terms of their configuration, thereby prompting governments and organizations to adapt to new technologies frequently (Fielder et al., 2016). Compounded by the dynamism exemplified by new innovations in ICT platforms, cybersecurity is a growing challenge for organizations due to increasing cybercrime and the infiltration of information systems by malware in digital environments (Lees et al., 2018). Predictions

indicated that in 20 years cybercrime will reach high levels and organizations will be required to allocate more financial resources and expertise to circumvent cyberattacks expected to escalate to a disproportionate number (Dor & Elovici, 2016).

Although the importance of allocating financial resource to bolster cyber resilience has been documented in numerous research papers, the literature did not focus on challenges and difficulties associated with unpredictability and significant measure of uncertainty within the digital space, which serve as an inevitable constraint to budgetary process for cybersecurity in public and private institutions (Srinidhi et al., 2015). Leveraging qualitative methodology's ability to provide an explanatory and descriptive account of a phenomenon (Ravitch & Carl, 2016), I explored the cybersecurity challenges as they manifest in budgetary processes in government units responsible for cybersecurity function. I studied the digital space's wide- ranging emergence of threats and uncertainties that gave rise to challenges amounting to constraints for the cybersecurity optimal budgetary process.

Problem Statement

The cyberspace engendered by the IoT is under security threats due to rising cybercrime (Ogut et al., 2011). Margulies (2017) observed that among many negative impacts induced by cyberattacks is the wholesale interruption of financial transactions, thereby plunging the banking processes into disarray. The literature on cybersecurity is replete with devastating stories of how governments and companies succumbed to cyberattacks.

Exacerbating cyberthreat risks and compromising cybersecurity is the fact that cyberattacks occur within the ubiquitous internet medium that has become a global public good with an international scope and scale with people's daily lives (Pour et al., 2019). Furthermore, Lees et al. (2018) predicted that based on a 2015 baseline cost of $3 trillion, cybercrime cost might reach $6 trillion annually by 2021. The increase in intrusion, disruptions of information systems due to malicious malware, hacking, and attacks mounted by adversaries are creating cybersecurity operational havoc and spiraling costs for organizations and governments (Njilla et al., 2018). A recent survey of information security professionals revealed 68% probability of data breaches in the public sector cyberspace (Ogut et al., 2011). A British cybersecurity insurance firm reported a 56% worldwide increase of claims in the recent past (Srinidhi et al., 2015). This is evident in untenable situations characterized by wide-ranging cyber risks that place the information systems, infrastructure, and data assets of organizations and governments in precarious conditions. Along with cyber uncertainties is the requirement for budgetary planning and allocation for effective and efficient cyberattack prevention establishing cyber resilience measures, mitigation, and recovery (Dor & Elovici, 2016). Furthermore, McKinsey's recent report (2015 as cited in Srinidhi et al., 2015) estimated that the economic losses resulting from cyberattacks may reach $20 trillion by 2020.

Although the literature recognized the skyrocketing financial demands required to circumvent cybercrime and to manage cyber risks as a daunting constraint to organizations, the challenges created by the expansive nature of the cyber-threat landscape and multilayered digital domain of budgeting and investment for cybersecurity

have not received adequate research attention (Fielder et al., 2016). Recognizing budgetary difficulties for cybersecurity, Njilla et al. (2018) pointed out that, owing to a cyber-threat landscape coupled with a cyberattack surface area exacerbated by the multifold nature of the digital domain, governments are confronted with budgetary difficulties that compromise their ability to achieve optimal financial investment. Governments are experiencing budgetary constraints due to the rising budgetary demand for cybersecurity and its wide-ranging cyber vulnerabilities (Dor & Elovici, 2016). Optimal budgeting for cybersecurity is difficult to achieve (Fielder et al., 2016). This is hinged on the dynamic nature of the digital space; for instance, at any given time, the cyber-threat landscape presents numerous conditions often with detrimental variations leading to uncertainties and vulnerabilities, thereby creating direct and indirect budgetary difficulties (Lees et al., 2018). The Deloitte Report (2014) revealed that 75.5% of managers responsible for the cybersecurity portfolio cited the insufficient budget as a major constraint.

In this regard, the government of South Africa through its cybersecurity policy architecture recognizes that cybersecurity is an integral part of the risk profile; therefore, building a resilient defense against potential cyberattacks has become not only a strategic priority but also a cyberspace policy imperative (Fielder et al., 2016). However, building a resilient cybersecurity infrastructure with strong cyber defense mechanisms requires optimal level funding and investment solutions that take into consideration the budgetary complexities underpinned by dynamism and multilayered nature of cyberspace systems (Pătrașcu, 2018). The cybersecurity literature highlighted an exponential increase of

budgetary allocations required to build a defense against cyber threats in digital spaces of organizations (Srinidhi et al., 2015).

However, cybersecurity challenges associated with the inherent uncertainties and changing digital environment, disruption of computerized systems' normal functioning, and many repercussions result in compromised integrity of security of intellectual capital in cyberspace (Raban & Hauptman, 2018). Cyber threats of various types have become a major concern lurking in the ubiquitous internet (Ben-Asher & Gonzalez, 2015). The literature provided a taxonomy of types of cyber threats. Pour et al. (2019) argued that a notable malicious cyberattack agent among many is the DoS that it is used by intruders to launch attacks to the network components such as webservers, memory processor, bandwidth, and physical network infrastructure. Accentuating this point, it is worth mentioning that severe impact of DoS could include restricted access to the network and, in worse case scenarios, the cyberattack could cause a network to grind to halt as well as exfiltration of intellectual capital (Ben-Asher & Gonzalez, 2015).

Although cybersecurity literature highlighted several operational risks induced by cyber threats to government ICT systems, cyber-threat conditions caused by categories of cyber threats and their negative impact on optimal government funding for cybersecurity have not been adequately researched. Several studies exploring the detrimental effects of cyber threats have found that DoS is among the most common attack vectors that feature prominently in the cybersecurity threat landscape (Dor & Elovici, 2016). Although studies have examined the issue of allocation of budget for cybersecurity policy implementation, studies focusing on the limitations caused by conditions induced by DoS

cyber threats to optimal budgeting have not received adequate scholarly focus in the growing body of cybersecurity literature (Ben-Asher & Gonzalez, 2015). Attesting to the increasing importance of public and private sectors investing to counter cyberattacks, Paul and Wang (2019) postulated that the review of cybersecurity budgets across organizations and governments confirms a growing anxiety.

The complex nature of cyberspace conditions induced by DoS cyber threats warrants the need to conduct additional research on this phenomenon. A qualitative case study would enable an in-depth exploration and description of the DoS cyber-threat conditions in contexts of the internet network system governance, in line with government policy framework on ICT as well as national intelligence architecture (see Yin, 2003). The unit of analysis for the current study was the Chief Directorate: Cyber Security Operations and National Cybersecurity Hub located within the Department of Communications and Digital Technologies (DCDT), including the Government Communication and Information System of South Africa (GCIS). The research design was a case study to explore, describe, and understand how DoS cyber threats, which are classified as active attacks, create cyberspace uncertainties, vulnerabilities, and instability to digital data, information assets, and ICT critical infrastructure, thereby creating difficulties for the government to provide optimal allocation of the budget.

Purpose

The purpose of this qualitative case study was to explore and describe cyber-threat conditions caused by the DoS cyberattack, which compromises cyber resilience of computerized systems by creating network instability, interruption, and vulnerability to

the digital data and information assets (see Lutscher et al., 2019). Drawing from the case of the South African, Government Communication and Information System and Cyber Security Operations and National Cybersecurity Hub, a subunit charged with the responsibility for national cybersecurity coordination, I explored the phenomenon of DoS cyber threat and budgetary implications. Through the enacted South African National Cybersecurity Policy Framework (NCPF), 2012, the National Cybersecurity Hub draws its mandate to be a key point of contact for cybersecurity matters, including coordination of cybersecurity response activities, and facilitates information and technology sharing. The Cybersecurity Hub is South Africa's National Computer Security Incident Response Team (CSIRT), and part of its responsibility is to make cyberspace an environment where all residents of South Africa can safely communicate, socialize, and transact in confidence .

I investigated the dynamic and rapid emergence of DoS cyberattacks, which create cyberspace vulnerabilities, acute interruption, and instability that results in difficulties for optimal budgeting and financing of cybersecurity. Investigation of DoS cyberthreats and associated threat landscape conditions was done in response to the difficulties caused by frequently changing cyber threats and the complex impact on government fiscal planning and budgeting for cybersecurity. The exploration was conducted using qualitative methodology to contribute to the understanding of cyber risks and conditions associated with DoS that constrain the ability of organizations to determine optimal budgetary allocations and investment for cybersecurity to protect digital data and information assets. Qualitative methodology allows research on

phenomena of concern to be conducted in participants' natural settings (Patton, 2015). The geographical location of the study was the South African government, Government Communication and Information System including the Chief Directorate unit charged with the national mandate for cybersecurity operations and the National Cybersecurity Hub within the Department of Communications and Digital Technologies.

Research Questions

RQ1: What are the various Denial-of-service cyber-threat events and responses coordinated by the National Cybersecurity Hub unit in South African national government?

RQ2: How does the rapid emergence of Denial-of-service cyber-threat conditions cause challenges for optimal budgeting and financing for cybersecurity operations managed by the Department of Communication and Digital Technology in South Africa?

Theoretical Framework

Ludwig von Bertalanffy (1972) is credited for originating general systems theory in 1937, refining it in 1949, and revitalizing it in 1972. General systems theory has been applied in social and natural sciences (Quinn, 2011). The theoretical constructs pivotal to the understanding and application of systems theory include function, process, and structure. Systems thinking theory is the lens through which a researcher's worldview considers existing things (e.g. government cybersecurity unit) as systems that are characterized by interconnected parts that combine to form cause-effect feedback loops (Arnold & Wade, 2015). I leveraged the central notions of holistic thinking, interconnectedness, and interdependence to explore and describe cyberspace, frequent

changes and uncertainties, and their subsequent influence on the budgetary difficulties for cybersecurity policy (see Patton, 2015). the cyber-threat conditions associated with DoS and dynamics concerning the uncertainties within the digital space (system) were explored with the intent to understand its systemic effects on financing of government cybersecurity units (see Drack & Schwarz, 2010). The suitability of employing the general systems theory for the current study was derived from the theoretical thrust on complex systems, a construct that resonated with cyberspace, which is a complex system and a central focus for the study (Mulej et al., 2004).

Nature of the Study

Consistent with the research purpose and research questions, qualitative methodology was appropriate for the current study. The qualitative approach aligned with the purpose of the study, which was the exploration and description of cyberspace high uncertainty conditions and events that create challenges and difficulties for budgeting and financing cybersecurity policy implementation for the South African government unit responsible for cybersecurity operations. Rudestam and Newton (2007) asserted that qualitative research does not provide instruments for testing hypotheses or theoretical propositions; rather, theories emerge from the collection and interpretation of textual data. I employed the qualitative paradigm to describe the phenomenon of uncertainties in cyberspace and their effects on budgetary processes in the domain of cybersecurity as it unfolds in natural settings of cybersecurity the public sector (see Ravitch & Carl, 2016).

The methodology selected for this study was the qualitative approach, which aligned with the purpose of describing a phenomenon of concern (see Ravitch & Carl,

2016). I used a qualitative case study design to explore the complex phenomenon of cyberspace conditions that negatively affect budgetary function in the Chief Directorate unit responsible for cybersecurity operations at the national government of South Africa. Case studies possess idiosyncratic traits that draw the attention of a researcher to conduct a scholarly investigation (Kumar, 2014). Furthermore, the literature within the domain of research design and methodology underscored the utility of the qualitative case study design (Dooley, 2002). The utility of the case study design is manifested in researchers' quest to understand complex phenomena by posing questions such as "what", "how," and "why" in research projects (Yin, 2003). Leveraging the distinctive advantages inherent in the case study design, researchers are able to meet investigative needs arising from the desire to gain holistic understanding of complex organizational and managerial processes in real-life contexts (Yin, 2003).

The government unit responsible for cybersecurity in South Africa, selected for this case study unit, was a complex and specific unit of analysis to explore the DoS phenomenon with associated cyber-threat conditions and how this is an impediment to optimal budgeting for cybersecurity.

The nature of the study involved selection of the South African government unit responsible for cybersecurity operations with a specific focus on the budgeting domain. I used a purposeful sampling strategy and targeted a minimum of 10–14 interview with participants from the unit of analysis and relevant ministry persons responsible for cybersecurity within the government of South Africa in line with attendant fiduciary responsibility to execute the allocated budget (see Cooper, 2012). Consistent with the

guidelines for using the case study design in research, other sources of data were equally reviewed and considered for data collection. Amongst these were, annual reports, reports on the subject matter, policy framework, legislative tools, ministerial speeches focusing on the phenomenon of concern, and social media platforms (Dooley, 2002).

Definitions of Terms

Definitions of key terms related to the phenomenon under investigation provide a cogent understanding of the application of terms to the reader throughout the study. This need was relevant for this study focusing on cybersecurity, an emerging phenomenon with an evolving knowledge base including shaping of the research agenda definition (see Wilner, 2018). The definitions of terms such as cybersecurity provide consistent meaning, the standardization of the utility and application of terms in the research, and the shaping of policies and practice in governments, industries, organizations, and countries (Craigen et al., 2014). The following definitions related to the study provide uniform, concise, and reliable definitions of terms:

Adversary/attacker/hacker: An intruder or unauthorized user attempting to gain access to an information system (Kissel, 2013).

Critical infrastructure: Vital physical and virtual assets that, if they were to be incapacitated or destroyed, the national security, national economic security, national public health, and safety of telecommunications would experience a debilitating impact (Kissel, 2013).

Cyber resilience: Cyber-system strength to withstand potential malicious cyber threats and the ability to quickly adapt and recover from the attack or off-setting changes

within the cyber environment through the holistic contingency and the implementation of risk management (Kissel, 2013).

Cyber threat: Any incidence or cyber event carrying the potential to cause an adverse impact compromising the safety, performance, and integrity of organizational network systems and operations (Kissel, 2013).

Cyberattack: A malicious, deliberate action of adversaries aiming to alter, disrupt, deceive, degrade, or destroy computer systems or networks to gain entry and access to information and programs resident in these systems or networks (Caplan, 2013).

Cyberattack surface area: The expansive cyber system networks, infrastructure, instruments, and communication tools and associated conditions of vulnerability to cyberattacks. The extensive proliferation of Industry 4.0 and IoT induces organizations to expand the cyber components, which increases the cyberattack surface area (Vance et al., 2012).

Cybercrime: An umbrella term for two categories of e-crime: cyber-dependent and cyber-enabled crimes. Although both occur within cyberspace, the difference is that the former refers to criminal acts targeting the ICT hardware or software, such as infecting computers with malicious malware. In the latter, cybercrime is facilitated and enabled by ICT. The examples are stalking, fraud, or online child exploitation of various forms (Lagazio et al., 2014).

Cybersecurity: A constellation of risk management measures, equipment, policies, technologies, security safeguard applications, and practices to bolster the ability of the

organization to protect, build resilience, and defend its CMC operations and safe functioning of cyber environment against cyber threats (Rudasill & Moyer, 2004).

Cyberspace: A global domain of intersecting multimodal technology in information and communication media (Williams, 2014). Furthermore, cyberspace refers to the virtual system consisting of the interdependent network of information systems infrastructures including the internet, telecommunications networks, computer systems, and embedded processors and controllers (Kissel, 2013).

Cyber-threat landscape: The level of proneness of cyberspace to cyber risks, vulnerabilities, and uncertainties (UNIDIR Report, 2017).

Denial-of-service (DoS): The intentional malicious cyberattack by intruders launching a vector leading to the blocking of access to a computer, webserver, memory processor, bandwidth, physical network infrastructure, or network resource of another user (Pandey & Singh, 2019).

Digital asset: A system-based application output file, database, documented information, webpage, or digital service provided to access data from an application (Kissel, 2013).

Vulnerability: System weaknesses leading to susceptibility to information system breaches, weakened system security procedures, compromised internal network controls, or a situation that may lead to exploitation by cyber intruders or systemic failure triggered by a threat (Kissel, 2013).

Assumptions

Several aspects of the current study were dependent on a set of assumptions. The first assumption was the philosophical framework upon which this qualitative study was predicated, which was a constructivist tradition that considers the meanings of reality as varied and multiple according to how an individual constructs the reality. In the constructivist domain, researchers investigate the complexity of opinions instead of reducing them to a few categories. In this regard, I assumed that diverse perspectives derived from the interview participants would enrich the findings and create in-depth understanding of the nexus of cybersecurity and budgeting difficulties for organizations and governments (see Burkholder et al., 2016).

Given that cybersecurity is a specialized field within the domain of modern technological advancements in varied forms such as IoT, AI, and ICTs, I assumed that the sample population had adequate knowledge of the cyberspace environment as a government imperative. Although I made initial contact with the leading authorities at the unit of analysis, the extent of support for participation was a function of this assumption. Another assumption was based on the hope that the participants would be willing to accept in-person interview sessions or agree to the online Zoom interviews. Part of the assumptions was that the respondents would be accessible online and would provide honest information during the interview. South Africa categorizes cybersecurity as a security apparatus, and the National Policy Framework on Cybersecurity was developed by the State Security Agency. I assumed that the South African policy posture would not constrain the respondents to provide comprehensive information. Furthermore, privacy

regulations restricting public information to be disclosed was part of the assumption that had the potential to hamper free flow of information during interviews (see Yin, 2014).

The epistemological nature of the study also influenced the assumptions. Knowledge that individuals (interviewees) provided emanated from their unique experience and understanding of the world. Knowledge and the knower are interwoven (Gelo at al., 2008). Based on the knowledge and quality of data that were collected from the interview participants, I assumed that the analysis method adopted in this study would yield findings consistent with the purpose of this study.

Furthermore, I assumed that the responses of the interview participants would give rise to the construction of meaning and understanding in line with the research goal. I also assumed that the qualitative exploration of the perspectives of the participants in relation to the topic on phenomenon would yield credible conclusions (see Baxter & Jack, 2008). An interpretive analysis was predicated on the assumption that the interviewees would offer accurate information about their experiences in the context of constructivism (see Burkholder et al., 2016).

Scope and Delimitations

The geographical area of the study represented a delineation in the sense that, as the primary data collector, I chose South Africa, which is my country of origin. South Africa was chosen based on easy accessibility, convenience purposes, and familiarity. Furthermore, according to Patton (2015), the sampling criteria take into consideration cases meeting a "predetermined criterion of importance" (p. 45). Part of the criteria was to enroll participants considered to have adequate insight and experience on

cybersecurity. This was a crucial delimitation because it ensured collection of relevant data for the study.

Limitations

Following an intensive search for literature on the study area of concern identified in the problem statement, very limited research was found. In this regard, one limitation of the study was that the body of knowledge on the specific area of concern was narrow. Furthermore, among factors representing external threat, there was a lack of literature focusing on cybersecurity in juxtaposition to budgeting in government domain, which represented another limitation.

Another limitation associated with the study was that cybersecurity is an emerging policy issue; therefore, the likelihood for interview participants to have limited expertise was high. Furthermore, across the world, cybersecurity is considered a domain with strong connections to national intelligence and state security, and South Africa is not an exception. In this regard, I expected that because participants were drawn from government, there might be reluctance to share all information as a result of a common understanding of the categorization of cybersecurity information as sensitive and classified information.

Transferability of data determines the quality and the significance of the study (Creswell, 2013). The primary source of data was the officials working within the unit of analysis: the National Cybersecurity Hub including Government Communication Information System. The depth of knowledge of the participants was difficult to measure,

and this could have adversely affected the quality of data and the transferability of findings.

Although the findings of this study may enhance the body of knowledge within public policy and administration in general and contribute to the domain of governance and operations of cybersecurity domain, findings might not be applicable to other government agencies due to the geographical context and country-specific dynamics of the location of the study. However, this geographical limitation did not disregard the basic tenets adopted to enhance the cybersecurity operations in any jurisdiction.

Significance

Cybersecurity is an emerging field that has caught the attention of the public and business sectors due to its potential adverse impact on the economy, social justice, and peace. If not addressed, the risks associated with cyber threats could grow into a global concern with a catastrophic impact on government and private sectors' digital assets and CMC infrastructure security (Cavelty, 2018). The literature postulated that cybersecurity is one of the emerging topical policy focus areas debated in global governance, and cybersecurity is an integral part of globalization and security concern. Globally, governments are experiencing rising security threats, which has placed the subject of cybersecurity at center stage (Swiatkowska, 2017). Governments are required to define and formulate cybersecurity policy frameworks and put in place necessary infrastructure to minimize cyberattack risks (Ogut et al., 2011). Furthermore, Lees et al. (2018) found that the cost of avoiding investment on cybersecurity defense is too high. Among many points of contention, cybersecurity brings forth compelling evidence for government's

obligation to support policy implementation through budget allocation (Schneider, 2018). Central to the purpose of the current study was the need to explore the South African national government Chief Directorate and GCIS responsible for cybersecurity operations budgetary and financing approaches and the wide-ranging, multilayered, and changing conditions of the digital domain.

In the recent past, South African media reported several cybersecurity attacks experienced by some organizations. Furthermore, South Africa is considered one of the countries that has developed plausible cybersecurity frameworks and has invested considerable financial resources on cybersecurity infrastructure. However, there was a need for scientific evidence to establish budget efficiency in the context of unpredictable and dynamic cyberspace vulnerabilities and uncertainties. The cybersecurity unit within the South African national government sphere provided a unique case study for me to explore the cybersecurity budgetary landscape and associated digital environment conditions.

Summary

Cybersecurity is an emerging public discourse that government policies are yet to be accustomed to and integrate as cross-cutting policy. Countries are at different levels of articulating cybersecurity in their national policy architecture. Policy frameworks are instrumental in defining the policy posture of a government. Consistent with the government's responsibility to offer cybersecurity policy frameworks is the need to allocate budget resource with the purpose of safeguarding sensitive data and critical infrastructure (Kissoon, 2020). Cybersecurity is not only an emerging policy area but also

a complex phenomenon embedded in expansive and complex ICT and internet networks' governance (Mueller, 2017).

Adding to the complexity of cybersecurity are multifaceted dimensions encompassing cyberspace, which include critical infrastructure hardware, software components, IoT networks, ICT, AI, digital information management systems, and the daunting challenges of keeping the system secure and safeguarded against cyber threats. In the past 2 decades, cyberattacks have emerged as a matter of global safety for organizations that are compelled to deploy defense mechanisms via technological and social means (Zoto et al., 2019). The detrimental adverse effects resulting from cyberattacks on public safety are immerse (Margulies, 2017). It for this reason, as well documented in the literature, that cybersecurity has been acknowledged as a public good within the purview of public safety and security (White & Ettkin, 2013).

The current study focused on the exploration and description of how DoS cyber threats' insurgence and their attendant conditions create instability and vulnerability in the cyber system and CMC, thereby causing a systemic compromise of information networks and digital assets and negatively impacting the daily functioning of organizations. In line with knowledge gap on the relationship between the insurgence of cyberattacks and the need for an optimal budget for cybersecurity, I explored policy propositions in financing and budget allocation for cybersecurity by organizations and governments.

Findings of the study will offer a leeway for professional insight, understanding, and knowledge to empower the current and future public administrators in charge of the

policies, standard operating procedures, and budgeting function within the milieu of cybersecurity. The broad view was that this study would contribute to the reduction of the knowledge gap regarding the phenomenon of concern, thereby stimulating social change by empowering public policy administrators to improve cybersecurity governance within the South African government. Chapter 2 focuses on the review of relevant literature on cybersecurity, cyberattacks, and cyber threats, including those associated with DoS and optimal budgeting as a government function (Quigley et al., 2015).

Chapter 2: Literature Review

Cybersecurity challenges have become a major global concern and are induced by cyber threats of various types, lurking in the ubiquitous internet network and broader cyberspace environment (Ben-Asher & Gonzalez, 2015). A notable malicious cyberattack agent is the DoS used by intruders to launch attacks to network components such as webservers, memory processors, bandwidth, and physical network infrastructure (Pour et al., 2019). Pour et al. (2019) contended that the severe impact of DoS could include restricted access to the network and in worse case scenarios the cyberattack could cause a network to grind to a complete halt as well as exfiltration of intellectual capital (Ben-Asher & Gonzalez, 2015).

Optimal budgeting for cybersecurity is difficult to achieve (Fielder et al., 2016). This is hinged on the dynamic nature of the digital space characterized by a fast-changing digital environment and disruption of computerized systems' normal functioning, leading to major uncertainties that result in compromised integrity of security of intellectual capital in the cyberspace (Raban & Hauptman, 2018). Studies focusing on the limitations caused by conditions induced by DoS cyber threats to optimal budgeting have not received adequate scholarly focus in the cybersecurity body of literature (Ben-Asher & Gonzalez, 2015).

The purpose of this qualitative study was to explore and describe cyber-threat conditions caused by the DoS cyberattacks that compromise cyber resilience by creating network instability, interruption, and vulnerability to the digital data and information assets.

Literature Search Strategy

The literature search strategies included in-depth searches in all Walden University Library databases, including ProQuest and all EBSCOhost databases such as Academic Search Premier, Thoreau Multi-Database Search, government policy and legislative documents, as well as the website for Cyber Security Operations and National Cybersecurity Hub network system located within the DCDT, government of South Africa, search engines, ICT for Peace Foundation, Business Source Complete, USA, Homeland Security Digital Library, International Security and Counter Terrorism Reference Center, SAGE Premier, and SocINDEX.

Cybersecurity OR cyber security, cyber-security attacks, Systems Thinking OR *General Systems Theory (GST), budgeting for cybersecurity, critical infrastructure,* and *threat landscape* terms search combinations yielded the most desirable results. The key search terms that I used to find relevant reading material for literature review related to cybersecurity included *Cybersecurity + Cyberspace adversaries + Cyber-threats* and *cyber-attacks + Denial-of-service attacks + Optimal budgeting for cybersecurity in the public sector + Systems Thinking theory, Information + Communication* + and *Technology (ICTs) & Cybersecurity,* And *South African government Cybersecurity Policy Framework.* Relevant websites of international organizations were also consulted as important resources for the cybersecurity domain. Additionally, cybersecurity resources from the United Nations Office of Counter-Terrorism UN Counter-Terrorism Centre (UNCCT) were reviewed. Consistent with the phenomenon under investigation and the problem identified, the UNCCT was a relevant resource for this research because

its key policy area is cybersecurity and new technologies that aim to enhance capacities of member states and private organizations in preventing and mitigating the misuse of technological developments by terrorists and violent extremists. The UNCCT website reported recent cybersecurity activities undertaken in the United Nations (UN) subregional geographical locations:

- In 2019, the UN Office of Counter-Terrorism implemented Phase I of the Cybersecurity Programme for South East Asia and Bangladesh, delivering an awareness raising workshop for the 11 beneficiary Member States. A pilot in-depth training workshop was also organized for Thailand, Brunei, Philippines, Bangladesh, and Lao PDR.
- In 2020, the UN Office of Counter-Terrorism implemented Cybersecurity Phase I for East Africa, Horn of Africa and the Sahel (https://www.un.org/counterterrorism/cct/programme-projects/cybersecurity).

Another key online resource on cybersecurity was the ICT for Peace Foundation, which has a mission of promoting a secure and peaceful cyberspace. Flowing from this mission, cybersecurity was a relevant resource for the phenomenon under investigation because its key programming policy thematic areas for ICT for Peace Foundation focus on international cybersecurity policy and diplomacy capacity building. This resource resonated well with the current study because it focused on supporting the capacity of the United Nations member states including African countries to develop national cybersecurity policy frameworks and national cybersecurity strategies including

government planning and budgeting for sole purpose to enhance Cybersecurity at country level (ICT for Peace Foundation,2019).

Theoretical Foundation

Origin of the Theory

Ludwig von Bertalanffy (1972) is credited for originating general systems theory in 1937, refining it in 1949, and revitalizing it in 1972. General systems theory, which has evolved to be commonly known as systems thinking, has been applied in the social and natural sciences (Quinn et al., 2011). The theoretical constructs pivotal to the understanding and application of systems theory include function, process, and structure (Saber, 2016). Systems thinking as an approach and conceptual framework is better understood when contrasted with scientific reductionism advanced by Descartes who projected a notion that the best way to understand phenomena is to reduce and break them down into simpler parts (Shaked & Schechter, 2017). Contrary, systems thinking theory places high emphasis on the holistic approach in relation to the interrelationship and interdependence of all parts systemically working together as a whole in a network pattern including the feedback loops (Shaked & Schechter, 2017). Systems theory offers tools of analysis and an interrogative framework with transformative enablers to overcome reductionist and linear worldviews (Glenn et al., 2020).

Systems theory is the lens through which a researcher considers existing things (e.g. government cybersecurity unit) as systems that are characterized by interconnected parts that combine to form cause-effect feedback loops (Arnold & Wade, 2015). Plack et al. (2018) elucidated that in a system, each constituent part is crucial yet not individually

self-sufficient to fulfil the systemic aims that require holistic interdependence of each part to produce the whole. Drawing from systems theory's dynamics insights, I leveraged the central notions of holistic thinking, interconnectedness, and interdependence to explore and describe cyberspace and the frequent changes and uncertainties and subsequent influence on the budgetary difficulties for cybersecurity policy intents (see Patton, 2015).

Cyber-threat conditions associated with DoS and dynamics concerning the uncertainties within the digital space (system) were explored with a view toward understanding its systemic effects on financing of government cybersecurity units (see Drack & Schwarz, 2010). The suitability of employing general systems theory for this study was derived from the theoretical thrust on complex systems, a construct that resonated well with cyberspace that is a complex system and a central phenomenon for this study (see Mulej et al., 2004).

The area of systems thinking expanded rapidly during the 1970s, 1980s, and 1990s with the development of alternative systems approaches. Several researchers entered the field and enriched systems thinking reasoning through a plethora of definitions and methodological practices. In the absence of a single definition, systems thinking researchers offered diverse interpretations. Despite the absence of one universal definition, there is wide acceptance that diverse definitions culminate into two epistemological underpinnings: seeing the whole beyond the parts and seeing the parts in the context of the whole.

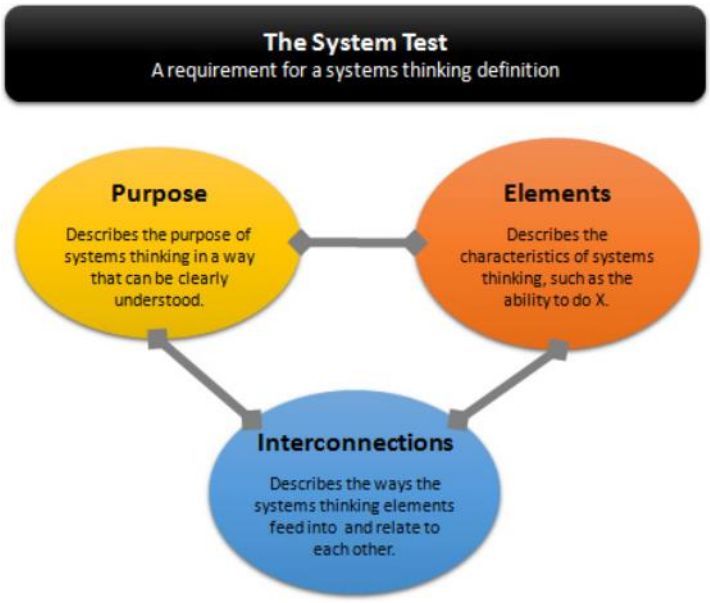
Systems Thinking Related Constructs

The epistemological worldview of systems thinking major theoretical constructs are anchored on a notion and assumption of studying and understanding phenomena from a holistic perspective (Flood, 2010). Drawing from this antecedent thought, Arnold & Wade (2015), provided a philosophical explanation that systems thinking is a framework of processing thought about systems. Taking this view, it can be cogently stated that, what informs the primary concern of systems thinking paradigm is how the whole of the phenomena interact with its contextual and environmental conditions (Checkland, 1999). The theoretical constructs of systems thinking provide a theoretical framework by which the interconnected, interdependent and interrelated elements of phenomena and their constituent parts can be investigated in a holistic method (Yawson, 2012). Senge (1990), explains that Systems Thinking is a framework that is with distinct parameters allowing seeing interrelationships as opposed to see standalone things, patterns of change are illuminated and feedback loops play a major role in understanding the behavioral patterns of the phenomenon. Further explication on systems theory posits that the constituent parts of a system cannot be defined outside of the whole and vice-versa. Stated differently, in systems thinking tradition, the part in whole structure of systems inherently incorporates emergent interrelationship between the whole and constituent parts of a phenomenon (Cabrera et al., 2015). Ryan & Tomlin (2010) opined that Systems Thinking adopts a broad perspective which gives scholars a theoretical foundation based on assumption that phenomena and events occur in nonlinear complex web of systemic recursive interrelationships.

Arnold and Wade (2015), contend that for the definition of Systems Thinking to be plausible, it should be tested against the Systems Test (Figure – 1). In this regard, Arnold & Wade (2015) assumed that a plausible definition on theoretical proposition of Systems Thinking should comprise of the elements, interconnections and purpose. To this end, throughout the literature, there is sufficient convergence of ideas among scholars on epistemological posture that Systems Thinking as a discipline with worldview lens for seeing whole and simultaneously be able to recognize the interconnections between interacting agents in a system (Senge, 1990). For instance, a simplified functioning of computerized mediated communication (CMC) comprises of hardware (PC or laptop), software, sever and network system. Another system could be a water reticulation system composed of a dam, big pipes to city and reticulation pipes channeling water along the streets and into individual building or house.

Figure 1

System Test-A Requirement for a Systems Thinking Definition



Note. The System Test (adapted from Arnold &Wade , 2015). Function, purpose, or goal should describe the purpose of systems thinking in a way that can be clearly understood and relates to everyday life. Elements will manifest as characteristics of systems thinking. Interconnections are the way the elements or characteristics feed into and relate to each other.

Building on von Bertalanffy theoretical framework, researchers have come up with plural theoretical paradigms of systemic thinking reasoning in an evolutionary trajectory. A corpus of literature highlights plurality as one of the key features of Systems Thinking (Cabrera et al., 2015). The explication of this notion is captured in multiplicity of Systems Thinking theoretical contracts, including the following:

- von Bertalanffy who is credited for recognizing and originating a theory around the term “systems” advanced the notion that “systems” consist of interconnected and interacting different constituent parts and components of a phenomena (Fischer & Richards, 2017).
- Barry Richmond (1987), credited with coining the term Systems thinking followed the line of reasoning that a system should have three dimensions: elements, interconnections and a function or purpose. The latter being the most crucial in determining the behavior of the system (Arnold & Wade, 2015).
- The central theoretical contract of Systems thinking accentuates the notion to view the world or phenomena through a lens which recognizes a set of interacting constituent parts, that exhibit concerting properties and make a whole (McMahon & Patton, 2018)
- Systems thinking is predicated on the notion of holistic approach that places emphasis on how the constituent parts of the system interact and interrelate within surrounding environment (Yawson, 2012).
- There is a considerable amount of emphasis of distinction between holism and reductionism in the literature. Set in juxtaposition and contrast with reductionism, Systems thinking approach involves both braking elements down into constituent parts and clustering the parts into larger wholes of the system (Cabrera et al., 2015).

- Systems thinking draws its basic concepts, fundamental constructs and ideological standpoints from various disciplines (Jackson, 2003). The pluralistic nature of Systems thinking emanates from its ability to encapsulate diverse methodologies of application and practice which are transdisciplinary and interdisciplinary (Fischer & Richards, 2017).
- One major aspect that has received considerable attention of researchers is complexity nature of system arising from interaction of its constituent components (Sweeney & Sterman, 2000). Literature further elaborates that the holistic orientation and complexity and emergent dynamic nature of systems is attributable to the causality, non-linearity, ever interacting constituent parts of the system (Meadows, 2008).
- Until to date, there is extensive corpus of work on the lens of viewing world as a complexity system (Checkland, 1981). Through the complexity theory, the researchers were able to highlight the theoretical view that phenomena evolve perpetually, interacting, non-linear and events can occur in an unpredictable manner. The field of cybernetics has been widely used to explicate the systemic heterogeneity of interacting components in a given system (Meadows, 2008).
- The literature on Systems thinking illuminates the iterative nature of events resulting from causality behaviour of interacting, interdependent elements including their feedback loops (Sanfilippo & Valle, 2013).

- A systemic perspective is framed on reasoning anchored on holistic approach based not only on inquiry about the unified whole, but also take into consideration various constituent parts with a specific context (McMahon & Patton, 2018). Far from linear action, systems theory pursues a line of reasoning that the different parts of the whole phenomenon are systemically interconnected and interdependent in a relational networked iterative action (Sanfilippo & Valle, 2013). A slight interruption in a system has potential to alter the fundamental role of each internal variable and cause the combination of their properties leading to emergent synergistic outcome in a system (Shaked & Schechter, 2017).

The prism of Systems thinking carries as key theoretical features traits of pluralistic and complexity constructs. The construct of complexity in systems thinking sharply contradicts and forms key antithesis of reductionism approach credited to the proponent who lived in the 17th century, Rene Descartes (Shaked & Schechter, 2013). In Systems Thinking paradigm, complexity denotes that phenomena are essentially a property of self-adaptive network of elements producing interrelated interactions which makes a whole (Guerard et al., 2012). Reasoning about the systemic logic of complex systems brings about recognition of system behavior characterized by feeding dynamic interactions of interrelated and self-adaptive system with emergent properties (Mesjazs, 2006).

Application of Systems Thinking

The rudimentary influence of Systems Thinking is biological science credited to Bertalanffy' (1968) seminal work. General Systems Thinking (GST) advanced the line of thinking which persuaded scholars that the theoretical contracts of system theory could permeate other fields of endeavor such as human sciences (McMahon & Patton, 2018). Corroborating to this notion, Systems Thinking theory has footprint and has influenced a wide range of disciplines, including philosophy, psychology, engineering, physical sciences, business studies, environmental sciences & ecology, developmental studies, etc.

Systems thinking approach has evolved rapidly into various tributaries of theoretical strands which proves its inherent nature of methodological pluralism (Cabrera et al., 2015). Checkland (1981), one of the leading researchers in the field, described Systems thinking as a meta-discipline approach, meaning its application and practices transcends various domains (Mingers & White, 2010). Be that as it may, the literature reveals that the taxonomy of theories in Systems thinking is organized and anchored on three broad methodological paradigms: hard, soft and dynamic systems (Yawson, 2012). Each paradigm is based on its distinct methodological taxonomy, application and practice in the field of Systems thinking (Fischer & Richards, 2017).

Main Systems Thinking Paradigms

Hard Systems

Operational research draws its framework of reasoning from the systems thinking dimension classified as hard systems (Yawson, 2012). Feature prominently in the operational research, is the utilization of the logical framework analysis which

investigates the transformation of inputs and outputs into outcomes in relation to obtaining certain goals (Yawson, 2012). In practice realm, hard systems leverage computerized simulations and quantitative methodological analysis to figure out solutions to real life problems (Yawson, 2012). At another level hard systems thinkers refer to the inputs injected in the system as stock and regard the systemic changes as the flows (Arnold & Wade, 2015). The stocks and flows are invariably affected by the variables or not constant parts of the system such as the maximum rate, force, size or quantity of the stock. For instance in water ripple system, the small waves that form water ripples (flows) depend on the volume of water (stock) that was involved in starting the ripples. In this system, the size and number of water ripples formed is affected by maximum interacting and changing internal force and energy (variables) resulting to few or multiple water ripple system (Arnold & Wade, 2015). In this regard hard systems sub-paradigm is mostly instrumental and applicable in analyzing problems that can be quantified (Yawson, 2012).

Soft Systems

In its pluralistic nature, Systems thinking employs Soft systems paradigm to process problems that are less quantitative in nature (Checkland, 1990). Soft systems is associated with human activity and human behavior phenomena such as meeting dialogues, emotion, conversations and attitudes (Shaked & Schechter, 2017). Checkland (1990) pioneered Soft System Methodology (SSM) paradigm as a sub-branch of systems thinking geared towards analysizing the complexity associated with human action (Zexian & Xuhui, 2010).

Dynamic Systems

The systemic behavior of constituent parts based on their traits and properties give rise to interaction and interconnections between elements culminating to Dynamic systems (Arnold & Wade, 2015). The utility of Dynamic systems paradigm draws from the ability to analyze three inherent characteristics of that informs the theoretical position of Dynamic Systems: The first is feedback loops - observance and collation of information on non-linearity of closed causal loops which influences change in the system, the second trait is computer simulation – rigorous computerized modeling of behavior of the shifting interplay of causal loops in a system culminating to a causal network with properties too complex for cognitive capability (Lane, 2000). Third, is focusing on mental models – the social behavior is influenced by interplay of dynamic ideas, judgment, debating and decision making (Lane, 2000).

Utility of Systems Thinking Theory

The literature identifies several real life situations illustrative of gainful utilization of System Thinking theory. Vast array theoretical constructs of both qualitative and quantitative paradigms have been utilized by scholars to transform theory to practice (Glenn et al., 2020). Abounding body of knowledge on the utilization of Systems Thinking approach is widely documented. Recognizing the complexity of health problems and interrelationships of vast heterogeneous units and groups operative within constantly changing environment and also working in realm of multiple interrelated strategic functions, the research in health domain has used Systems Thinking approach not only to harness comprehension of complex situations by gaining a holistic perspective

through seeing the whole interconnected interaction behavior and patterns of the constituent (Glenn et al., 2020).

Multiple tools offered by Systems Thinking are utilized to analyze complex management problems through testing and challenging preexisting challenges. In organizational development for instance, the quest to improved communication or to assess change patterns between different units in order to gain efficiencies and effectiveness, is evident in the studies which have utilized Systems Thinking tools such as feedback loops or systems dynamic modelling (Glenn et al., 2020). Public policy and administration research and practice shows that the policy makers have leveraged the various Systems Thinking key tools to identify cause and effect between interacting elements shaping behavioral patterns responsible for driving outputs (Plack et al., 2017). Accentuating this point, McMahon and Patton (2018), reflected upon the utility nature of Systems theory and characterized it as a multidisciplinary approach. Additionally, McMahon and Patton (2018), highlighted an example that career development theories are underpinned by Systems theory. Furthermore, Churchman (1987) pursued research which focused on investigating the utility of Systems theory in realms of problem solving and planning. The literature further sheds light those numerous scientific areas has emerged since the World War II, these include computerized mediated communication, systems engineering, logistics and supply chain, cybernetics to mention a few – systems thinking permeate all of them (Eriksson, 2003).

Systems Thinking has prominently featured in the conceptualization and description of complexity feature of biological ecosystems occurring in physical

environment. The tools and methodological dimensions of Systems Thinking are instrumental in teasing out interrelationships and interactions of numerous organisms and species occurring in a self-organized manner with a particular habitat (Garavito-Bermúdez et al., 2016). Thought leaders in organizational leadership and organizational change management, learning and development have leveraged Systems Thinking paradigm (Senge, 1996; Chekland 1981; Jackon 2003; Ackoff & Flood, 1999). In their academic pursuits, these scholars have curved alternative pathways thinking on leadership discourse and which places high importance on plural world views, diverse ideas and experiential learning in organizations through systems thinking approach (Caldwell, 2011).

Cybersecurity Domain Utilization of Case Studies

Cybersecurity literature extensively utilizes the case study research strategy. To recapitulate, a case could be an individual, a role, a small group, an organization, a community, or a nation (Miles & Huberman, 1994). The case in point is the research conducted by Armenia et al. (2018), which involved the case study of a nation, the Italian National Cyber Security Framework. Through the application of Systems Thinking, Armenia et al. (2018), were able to isolate the synergistically causal interrelationships between parts involved, identify the patterns and behavior and subsequent changes, including the impact of cyber-threats for Italian National Cybersecurity. Bell et al. (2003) alluded to a crucial point regarding the symmetrical trait of case study approach and Systems Thinking theory that the two are inclined to the description of interrelationships that exist within a given system or an organization. Therefore, this allows the research

enquiry on hand explore the interrelationships within the identified unit of analysis in respect to malicious events conditions vis-à-vis optimum budgeting for cybersecurity.

Featuring prominently among the well referenced cyber space risks cases across the literature on Cybersecurity include the United States of America (USA) terrorist attack of September 11, 200, STUXNET computer virus that was used as cyber-attack to critical infrastructure in Iran 2010, (Patrascu, 2018). Increasingly, the discourse on cybersecurity features prominently in the individual countries' national security strategy mix (Moghior, 2018). Notably, cybersecurity scholars among many approaches utilize countries as case studies to assess the policy posture for cybersecurity national policy development and budgeting. A case in point, Moghior (2018) conducted a cybersecurity study with a focus on exploring the characteristics of cybersecurity strategies in selected countries as case studies: Netherlands, Russia, and China.

Ostensibly, cybersecurity research relies heavily on case studies from corporate and government sectors to bring scholarly evidence to bear. Related to this, Pandey et al. (2019), documented some of the recent cyber-attacks events experienced by different firms: Tesco Bank, was a victim of cyber-crime activities. This case occurred in 2016, a cyber-attack which was classified as cyber-heist led to fraudulent withdrawal of money amounting to 2.5 Euros. Leoni AG, is the largest manufacturer of wires and electrical cables in Europe. In 2016, fake email was used by cyber criminals to deceive the Chief Financial Officer of the Leoni AG, to pay by electronic transfer $45m. In 2016, Hyundai and Kia cars were targeted by hackers by obtain propriety information from the control system including the code for the car keys and addresses of stolen cars. After accessing

the codes the hackers were able to steal cars and smuggled them to the West Bank. The German Steel Manufacturer in 2016 experienced cyber-attack similar to 2010 STUXNET intrusion. The cyber-attack destroyed software, took over the control system, severely damaged the infrastructure and brought the plant into a grinding halt. The cybersecurity industry calls 2017 with regrettable memories, recalling the damaged caused by the Wannacry ransomware which infected 150,000 computers in 150 countries within national healthcare systems (NHS). Malicious attack blocked access to critical patient information and the hospital services experienced major interruption.

Rationale for the Choice of Systems Thinking Theory

The rationale for choosing Systems Thinking is influenced by the fact that its methodological approaches allow pluralism, dynamism, iterative, causal feedback loops, and evolutionary features inherent in this theoretical framework. Central to the theoretical proposition of Systems Thinking is the notion and emphasis on complexity of systems, such traits are suitable and complementary to Systems thinking methodologies which integrate the use of technologies such Internet of Things, digital space, computers for simulating and modelling the dynamic behavior of parts interacting within a system (Lane, 2000). This trait locates Systems Thinking as a viable platform within which to conduct cybersecurity research investigation which also occurs in Computerized Mediated Communication and IoT systems. This enquiry will occur within the context of cybersecurity sub-discipline. The literature depicts cybersecurity as a subject not only characterized with complexity but also has dynamic dimensions (Zoto, et al., 2019). Multiple norms, standards and multilayered stakeholders composed of government levels

including international, national and provincial as well as the private sector play key roles in cybersecurity governance, making it a complex phenomenon which can be investigated utilizing Systems Thinking approach (Carr & Lesniewska, 2020). Furthermore, studies in cybersecurity cogently lay bare the that it is a function of interaction and interrelationship of not only wide-ranging networked technologies and communication information, but these elements also interact in agile and evolving realm and in a highly pluralistic manner (Wilner, 2018). In this regard, cybersecurity is inherently a complex phenomenon occurring within a complex environment (Bell, et al., 2003). Such attributes are compatible and complementary to Systems Thinking methodologies which provide an ability to explicate complexity dynamics and multimodal systems such as cybersecurity paradigm (Woo, 2013).

This study investigated the dynamic and rapid emergence of DoS which creates cyber space vulnerabilities and instability that subsequently culminates to enormous difficulties for optimal budgeting and financing of cybersecurity. Investigation on DoS cyber-threat and associated threat landscape conditions will be done in juxtaposition with the difficulties caused by these frequently changing cyber threats and the resultant complex conundrums to government fiscal planning and budgeting for cybersecurity. The exploration will be conducted through the qualitative methodology to describe and contribute to knowledge and understanding of cyber risks and conditions associated with DoS which constrain the ability of organizations to determine optimal budgetary allocations and investment for cybersecurity in order to prevent and protect the digital data and information assets.

Relationship Between Systems Thinking and the Present Study

Systems thinking theoretical thrust is anchored on the notion and ability of seeing the world or structures (e.g. cybersecurity government unit) as whole system characterized by an interplay of separate but interconnected and interdependent parts (McMahon & Patton, 2018). The phenomenon under investigation involves exploration and description of dynamic changes and uncertainties caused by cyber-threats and its subsequent influence to the budgetary difficulties for cybersecurity government function (Zexian & Xuhui, 2010). In this regard, the holistic paradigm offered by Systems Thinking theoretical framework provides viable methodological approach which resonates with the research question which seeks to investigate multi-dimensional aspects including various types of causes and effects of Denial-of-service cyber-attacks as well as the responses by the government unit under investigation (Arnold & Wade, 2015). Thus systems thinking holism and pluralism is instrumental to investigate complex causal interrelationships and dynamic interconnected parts of cybersecurity vis-à-vis optimal budgeting for cybersecurity (Eriksson, 2003). The Systems Thinking theoretical constructs resonate with the research questions which seek to investigate the interrelationship and effects of emergent properties of Denial-of-service within the cyber space (Zexian & Xuhui, 2010).

Literature Review

The 21st century has seen the rapid evolution of Information, Communication and Technology (ICTs) and the creation and expansion of cyberspace. Major investments, development of modern and advanced technologies, innovations coupled with the

proliferation electronic instruments, altogether led to expansion of digital space (Pătrașcu, 2018). The public and private sector dependency on cyber space medium, catalyzed by Internet of Things (IoT) has exponentially increased to greater proportions (Ogut et al., 2011). The nations of the world, governments cannot function outside cyberspace, yet socio-economic dependency on the complex of digital networks and internet deployed in critical infrastructure is inevitable and indispensable (Armenia et al., 2018).

Having recognized the ubiquitous nature and the extent to which cyberspace an Internet of Things are inextricably interwoven, it is necessary to employ Systems Thinking approach in order to explore other concomitant aspects and factors of this complex system. Amongst many factors associated with cyberspace is the vulnerability caused by exponential increase and rapid emergence of cyber intrusion, cyber-attacks, cyber-crime, cyber-threats events (Islam et al., 2018). Congruently, the importance of cybersecurity is taking centre stage in organizational planning and budgeting functions, in order for governments and organizations to prevent or mitigate unprecedented and prevalent cyber-attacks (Fielder et al., 2016).

Situating Cybersecurity in Global Governance Architecture

The scale and scope of cybersecurity challenges transcend global governance architecture and to some extent international relations. The discourse on cybersecurity and cybercrime is gaining traction, with global concerted efforts undertaken to create more sensitization and awareness-building among organizations and governments to take a proactive pro-cybersecurity policy posture and put considerable efforts to protect digital infrastructure and information systems in public and private sectors (Dor & Elovici,

2016). Notably, the United Nations, Office of Counter-Terrorism Centre (UNCCT), has proffered a fully fledge Programme on Cybersecurity with an objective to enhance capacities of Member States and private organizations in preventing cyber-attacks carried out by terrorist actors against critical infrastructure (UN Counter-Terrorism Centre [UNCCT], 2017). In recent years the international geopolitical multilateral organizations such as the African Union (AU), Association of Southeast Asian Nations (ASEAN), United Nations, Organization of American States (OAS) and many other regional blocs have all convened technocrats and diplomats for training on the Cybersecurity Policy and Diplomacy. This is considered as an efficient transmission of information and knowledge to affiliate countries and governments which bear sovereign responsibility for citizenry's safety and security including the cyberspace and digital platforms (ICT4Peace Foundation [ICT4Peace], 2017).

At a global scale, cyber-attack events are rapidly increasing, devoid of geographical restraints and limitations (Pătrașcu, 2018). To this end, increasingly, nations across the globe are strengthening offensive cyber-capabilities as a measure to mitigate potential cyber-attacks which in the recent past have been rapidly increasing at a transnational scope and scale (Comizio et al., 2015). Reviews of global giants including United Kingdom, United States of America and European Union reveal singleness of purpose in the international area to collectively tackle cyber-threats which pose significant vulnerability to global security systems across multiple sectors (Comizio et al., 2015).

Cyberspace and cybersecurity has brought to bear the reality of global village and globalization. That increasingly, the world fundamentally and existentially operates within digital domain is not an overstatement. The interconnections of complex different IT systems and IoT has capabilities and agility transcending global scale with a potential to cause vanish of geographical boundaries (Eling & Schnell, 2016). It is against this backdrop that the Internet is widely accepted as the global public driving interconnections between nations of the world (Celik & Gurkaynak, 2019)

Role of Policy Frameworks on Cybersecurity

Invariably, governments have inherent bear duty to protect their respective States and citizenry. Research has extensively revealed that the national security complex has shifted drastically due to the proliferation and expansion of cyberspace (Margulies, 2017). Increasingly, cyberspace bears tremendous importance for the national security and this is evident in the rapid increase of countries adopting cybersecurity national policy frameworks and strategies (Moghior, 2018). Corollary, a number of countries recognize that national security and defense can no longer be restricted to the military might only, but the importance of cybersecurity domain has rapidly increased (Pătrașcu, 2018). The cybersecurity national policy frameworks provide not only the guidelines from which actors both in the public and private sector draw inspiration, but also stewardship and governance in respect to sector coordination for prevention, mitigation and recovery in contexts of cyber-attacks events (Siponen, 2013).

Cyberspace coupled with the Internet are shared public network systems with a dynamic character through which government and firms operate their business. However,

simultaneously the digital space is replete with cyber risks of great proportions requiring government sound policy framework (Panday & Singh, 2019). In the world over, governments have a mandate to come with policy frameworks which respond to emerging challenges. Cyber threats and malicious cyber events are on the rise, thus government regulatory frameworks and minimum standards are indispensably required to prevent, mitigate and recover the cyber-attack induced malicious events (Srinivas et al., 2018). Typically, a number of countries have developed Security Policy Frameworks (SPF) which spells out minimum measures to be effected to protect digital assets, services and infrastructure in the context of cyberspace (Srinivas et al., 2018).

Socioeconomic Sphere of Cybersecurity

The discourse on cybersecurity always ensues in juxtaposition with cyberspace infrastructure and modern ecologies of technological equipment and gadgets (Islam et al., 2018). Modern socio-economic life is closely intertwined with digital space, as such Internet connectivity is regarded as a public good (Margulies, 2017). The network complex of Internet, ICTs and technological gadgets deployed and operating in systemic manner and simultaneously within digital space creates perpetual every day access to digital space and flow of information and data is a fast paced mode (Pour et al., 2019). Consequently, the digital space turns to have indiscriminate socio-economic impact to the everyday life at the level of organizations and individuals. Markelj and Zgaga (2016), argued that the effects of ecological and sophisticated digital space trigger unprecedented quickening pace of life. The impact of the digital landscape to the socio-economic realm oscillates between good and bad due to cyber intrusion and cyber-attacks lurking in the

digital space and yet its catalytic power and speed orchestrates incredible efficiency in business operations in both private and public sectors (Srinidhi et al., 2015). It is in this context that cybersecurity discourse has been indispensable for the socio-economic strata of life. Laboring on this point, Markelj and Zgaga (2016), clearly explains how much ICTs and Internet has socio-economically engineered life at communities and organizations levels. To this end, virtually young and old across the globe, have profile footprint in the Internet (Markelj & Zgaga, 2016). Stated differently, at a global scale, the friendships are maintained through communication gadgets connected in the cyberspace. This is evident the spiral growth of the social media in recent decades (Markelj & Zgaga, 2016). Similarly, the evolution of the Digital Age increasingly stimulates fast-paced economic and business transactions. Wilner (2018), found that Internet banking and mobile money, mobile computing are the classical examples of the impact ICTs, IoT and networked information and communication on the socio-economic strata of life, and as a result societies are facing a greater cyber security risks associated with the cyberspace environment more than before (Lia, et al., 2018). Human economic activity such as transferring money, banking and international trade occurs in great speed due to the digital capabilities. While these integrated technologies have stimulated a historical revolution in human life, however, an equally tremendous cyber-threat, cyber-risks occurring in the digital space has a detrimental and adverse impact on both information and technical (physical and software) as well as the socio-economic spheres of life at an unimaginable magnitude and proportions (Carr, 2013).

Cybersecurity and Information Communication and Technology

Cyberspace and Information Communication and Technology network creates virtual and critical infrastructure complex of great magnitude. The 21st century, also regarded as the digital age has seen governments and organizations leveraging and procuring digital capabilities through high degree of connectivity Internet of Things (IoT) to facilitate real time communication from end-to-end (Pandey & Singh, 2019). The ICTs ubiquitous connectivity cyberspace networks integrated by software with systems integration abilities creates highly complex interconnected digital infrastructure (Lees et al., 2018). On the same breath, Pour et al. (2019), pointed out that, increasing the critical infrastructure sector is experiencing heavy deployment of IoT and the two are integrated to create complex dynamic communication network. Expanding the same thought, Pandey and Singh (2019) postulated that the physical infrastructure and devises integrated by network systems and software embedded in computerized communication medium producing information reach ecosystem, altogether culminates to what has come to be known as the fourth industrial revolution (I4R) – the power behind "smart" technology (e.g. smart phone, smart TV, smart municipalities, smart factories, etc.).

Central to the notion of technological innovations, IoT, Artificial Intelligence (AI), quantum computing together with software products, is illustrative of the human creativity to create positive value of emerging technologies (Raban & Hauptman, 2018). The literature has extensively recorded the positive impact and revolutionary effects catalyzing business process and leapfrogging conventional way of life to digital culture (Margulies, 2017) – a fact that is illustrative by the 21st change of conducting business

both in the private and public sectors. Virtually, governments and organizations are continuously digitizing their operations with a view to improve business agility and efficiency and optimize cost (Pandey and Singh, 2019). Labouring on the same point, Pandey and Singh (2019) contend that deployment of ICTs and IoT to operational processes improved productivity and lead to sustainable development of organizations.

While advanced ICTs wide ranging technologies have revolutionized not only the digital space but also have dominated and bolstered capabilities of organization operations, these sophisticated technologies bring with them detrimental security risks and place organizations in the state of precipice and vulnerability (Ogut et al., 2011). Of interest, is the magnitude and inevitably harmful cyber-attack of myriad forms that organization perpetually face every day and that these could lead to a complete halt of operations or exfiltration of the organizations' intellectual capital and information assets (Pour et al., 2019). Alluding further, Eling and Schnell (2016), explain that each organization experience idiosyncratic exposure to malicious events, depending on resilience of the government specific parameters deployed in a form of technological equipment and ICTs network processes.

Numerous cybersecurity body of literature reveal that cyber-attacks are wide spread and in most cases the primary conduit through which malicious events are transmitted is the Internet (Eling & Schnell, 2016). Accentuating this point, Lia et al. (2018), observe that the proliferation coupled with complexity of internet infrastructure and mobile application gave rise to evolutionary and greater potential for malevolent cyber-threats in the cyberspace utilized by organizations and governments. Adversaries

operating in the cyberspace with malevolent intentions have a tendency to exploit the vulnerability of the digital space through launching cyber-attacks of various sorts (Lia et al., (2018). This is exacerbated not only by heavy dependence of cyberspace to ICTs, but also the proliferation of Internet coupled with its ubiquitous nature through which threat landscape is expanded leading to unprecedented levels of vulnerability to a plethora generation of cyber-attacks to the digital systems of organizations or governments units (Taewoo, 2019).

Budget Costs Associated with Cybersecurity

Cybersecurity in recent years increasingly become a strategic operational and management concern occupying high position among the priorities of organizations and government units. A recent survey found that the corporate boards' directors and CEOs expressed cyber risks are a major concern surpassing other forms of risks such as compliance (Islam et al., 2018). Governments have equally recognized the lurking cyber threats and have thus institutionalized the cybersecurity defense mechanisms by establishing dedicated cybersecurity units, developed cybersecurity specific policies and appropriated budgets in order to create resilience in their cyberspace against cyber-attacks and cyber criminality (Ogut et al., 2011). Notably, improving cybersecurity by introducing regulatory and policy frameworks, governments have recognized the centrality of Internet (Ben-Asher & Gonzalez, 2015). Thus, governments have pursued a dual strategy which includes protection of cyber space and improving ICT governance in recognition of inter-dependence between the two domains (Srinivas et al., 2018). Cybersecurity literature mentions a number first world and developing countries which

after experiencing devastating cyber-attacks have developed cybersecurity specific policy frameworks and strategies with a paramount objective to prevent recurrence of costly damage to the critical infrastructure and net loss of digital assets and data (Pătrașcu, 2018). The literature points out a direct proportion between deployment new technologies into the cyberspace and exponential increase cyber-threat risks (Eling & Schnell, 2016). Furthermore, the emergence of fourth industrial revolution technologies lead to positive multifold efficiencies to government and organization operations and has led to technological advancement of a plethora of smart operations (Cavelty, 2018). Conversely, the proliferation and integration of computerized mediated communication and Internet networking together with the critical infrastructure has exacerbated cyber risks (Pandey & Singh, 2019). Stated differently, there is a direct proportion between industrial revolution and evolution with pervasive radical expansion of cyber threat vectors (Pandey & Singh, 2019). Consequently, the public sector and private sector have had to face inevitable reality of sky rocketing budgetary costs, directly associated with efforts minimize adverse and catastrophic cyber-attacks digital assets and loss of data (Taewoo, 2019).

To this end, the costs associated with general security risks dimension and practice of protecting physical buildings and equipment of organizations are extremely expensive. Similarly, cybersecurity is considered by the organizations and governments as high security risk, to which substantial investments have been made to procure specifically cybersecurity-enhancing assets (Srinidhi et al., 2015). Efforts to cope with cybercrime has arbitrarily forking out substantially huge sums of money to enhance

cybersecurity, without which the digital assets of government units or organizations such as intellectual capital could be eviscerated (Srinidhi et al., 2015). It is against this background that the cybersecurity insurance sub-industry is growing fast, since a considerable number of organizations and government are compelled to take sustainable security posture by deploying security-enhancing technologies, in order minimize their digital space vulnerability to the intrusion of the cyber threats (Dor &Elovici, 2016). Congruently, Eling and Schnell (2016), contend that insurance for cybersecurity sub-industry is not only flourishing, but is it increasingly becoming exorbitant, thus demanding alarmingly large percentage of the government and organization budget (Dor & Elovici, 2016). Consequently, the costs associated with cybersecurity are on a spiral increase, this is exacerbated by unpredictable and uncertainty nature of cyber-threats. Characterized by highly fast paced, dynamic, and fast changing, the cyber space environment also contributes to the difficulty for experts to quantify precision the costs associated cybersecurity (Pandey & Singh, 2019). The organizations cannot predict with certainty the type and scale of potential cyber-attack, meaning it is extremely difficult to quantitatively and qualitatively analyze the levels of vulnerability or cyber risk of governments and organization (Fielder et al., 2016).

Given the high volatility caused by rapid changes which culminate to uncertainty of the cyber space, estimating the costs associated with wide ranging cyber threats and lack of accepted source is extremely difficult (Pandey & Singh, 2019). Notwithstanding the experts in cybersecurity sub-industry have come up with computation algorithm. Essentially, estimating overall costs involves gathering and collating two types of data

dimensions: (1) costs per incidence, and (2) costs per data breaches (Eling & Schnell, 2016). Cybersecurity research estimates that in 2019 alone, businesses in one country faced the cybersecurity costs to tune of *US$2 trillion* (Juniper Research, 2015). While the global estimates vary substantially, it is generally agreed that *US$100bn* figure for cyber risk costs. MacAfee (2014) put forth *US$2.1toUS$3.8* estimate for cost per data breach and the costs generated by loss of each record is estimated to be between *US$217* to *US$956*. These estimates are applicable at one jurisdiction. Future scenarios studies according to the World Economic Forum (2010) estimate that, the breakdown of critical infrastructure at 10% probability could amount to *US$250* financial losses due to complex and increase in interdependent cyber connections across the globe. Similarly, the cost of procuring cyber insurance for the physical infrastructure and the software is estimated at gross annual premium of US$2.7bn in America, while in EU cyber insurance costs was estimated at US$1bn in 2018 (National Association of Insurance Commissioners, 2013) and lastly, the premium volume for the Swiss is expected to reach US$5.9bn by 2023 (Swill Re, 2014). A total amount of US$20trillion economic loss would be incurred by 2020 (Srinidhi et al., 2015).

Cybersecurity Optimal Budgeting and Financing Difficulties

Cybersecurity has evolved to become a recognized domain in the public and private sectors (Celik & Gurkaynak, 2019). Mounting cyber threats have propelled the cybersecurity industry into one of the most important security aspects of governments and organizations budgeting priorities (Raban & Hauptman, 2018). Cyber-attacks is regarded as the gravest threat to nations and governments in the modern times. While

larger percentage of the critical infrastructure is owned by the private sector, public sector has experienced malicious cyber events (Paul & Wang, 2019). Consonant, to this, the spiraling potential cyber-threats and potential loss poses danger requiring resilient cyber defense. Consequently, governments and organizations are seized with developing policy frameworks and strategies with ultimate aim to deploy tools with security enhancing capabilities (Fielder et al., 2016). The rapid surge of malicious attacks to governments' cyberspace across the globe, has placed the question of how much budget is required to procure formidable cybersecurity defense mechanism in a center stage (Paul & Wang, 2019). A surge of research has emerged to determine evidence based optimal budgeting for cybersecurity domain. Research shows, considering on which dimensions of cyber defense should be receive budgeting seems to be a prerequisite for government agencies and practitioners in the cybersecurity domain (Kissoon, 2020). Celik and Gurkaynak (2019), find that among the priority cybersecurity parameters given high budget considerations by industry leaders are prevention, detection and recovery safeguards. Be that as it may, optimal investment and budgeting to effectively and efficiently avert malicious attack remains a difficult call. Kissoon (2020), find that this phenomenon is exacerbated by the swift changes in ICT and Internet networks coupled with rapid threats requiring frequent changes in cyber defense strategies (Kissoon, 2020).

Impact of Denial-of-Service Cyberattack

Denial-of-service (DoS) cyber-attack, its name is suggestive and descriptive of how DoS attacks intentionally sabotage the computers or network. Furthermore, once the malicious attack is launched by an adversary, the resultant effect is blockage of access to

cyber network resources or computer culminating to a temporary or permanent dial of service (Pandey and Singh, 2019). DoS attack is not one the worst forms of cyber-attacks, rather it compromises the ability of the user to access data at the time when it is needed. The moderate DoS malicious event also does not cause permanent damage to data, rather the user would be denied access to the network (Pandey & Singh, 2019). Ordinarily, adversaries launch DoS after gaining access into the network system (Ben-Asher & Gonzalez, 2015). The literature is abounding with convergence of opinions that DoS occurs in two scenarios: The first involves flooding through sending large quantities communication resulting to increased traffic load within the network leading to very slow processing of information rendering the system essentially unavailability for protracted periods of time (Ben-Asher & Gonzalez, 2015). Secondly, large volumes of traffic load can create saturation or an overflow of the targeted network until it collapses to a grinding halt leading to essentially a crashed networked (Ben-Asher & Gonzalez, 2015). Both the first and second scenarios shows that DoS malicious events can effectively create a situation which either halts productivity or slows it down to a level where it is rendered essentially unavailable resulting to denial of service.

Research work aimed at understanding the mechanics of DoS attacks shows that the malicious attacker agents to the network are three pronged: outsider, insider or both. The research further reveals that, often times, inside and outside malicious attacker agents collude and launch most severe damage to the network (Cho & Qu, 2013). On the other hand, the scope of the outsider attack is limited to jamming the communication channel referred to as a physical layer attack resulting to physical defects to the wireless sensor

networks (WSN) deployed within the network to prevent hostile outside attacks (Saghar et al., 2016).

At another level, Denial-of-service attack, has caught the attention of researchers and has inspired interest to investigate the motives and circumstances under which the DoS is employed. Stated differently, the research intended to explore why the adversaries mount DoS attacks on the websites and servers of governments and organizations is on the rise. Stemming from this, Lutscher et al, (2010) opined that DoS can be a tool and digital weapon employed in politics and public information domains. From a political point of view, anecdotal evidence shows that DoS attacks have been employed by repressive governments to undermine and cause outage on the websites of antagonist non-state actors with a view to censor information and gain political mileage through tilting political playing field to their advantage (Lutscher et al. 2010). Ordinarily, the victims DoS attacks orchestrated by non-democratic government can be, TV stations, newspapers, NGOs, and any other active outlet reporting against government (see Lutscher et al. 2010). Furthermore, the literature narrates qualitative and qualitative evidence of the exponential increase of frequency of the occurrence of DoS attacks during national elections in various jurisdiction. Documented examples of DoS attacks that took place during elections periods include: Russian elections in 2011, Turkey in 2015, Malaysia in 2011, Australia in 2011 (Freedom House, 2017). As revealed by research another important dimension regarding utilization of DoS attack is its cost effectiveness and agility.

However, the literature observed an increase of costs for preventing adverse DoS attack on among the non-state actors due to hosting of their website and servers by external agencies (Goncharov, 2012). As the act of protest and offensive move against oppressive policies or elections of nondemocratic governments, opposition groups or non-state actors can employ DoS attack against government network to incapacitate the website or server with a view to inflict harm to the image, credibility and interrupt the channel through which the government disseminating information (Ben-Asher & Gonzalez, 2015). Conversely, ICTs and Internet has expanded the repertoire of protest tools for pressure groups, social activists and civil disobedience action (Sauter, 2014). Notably, it has also been observed that oppressive governments also turn to use the DoS attack to arbitrary silence or impose censorship to mass media and the opposition or non-state actors which challenge government policies or government elections (Lutscher et al., 2010).

Application of Systems Thinking in Cybersecurity Domain

Twining of application of Systems Thinking approach and case study research strategy to investigate the Cybersecurity dimensions has been pursued by researchers operating in this domain to explore for instance, the interplay of technological components (software, hardware), processes, data and people (Armenia et al., 2018). Congruently, Yin (2003) underscored that the distinctive advantages inherent in utilizing the case study research strategy, is that researchers are able to meet investigative needs arising from the desire to gain holistic understanding of for instance complex organizational and managerial process in real life contexts. In this regard, scholars have

leveraged Systems Thinking paradigm to analyze specific cased studies of cybersecurity multifaceted dimensions and complex interplay of interrelated components (Armenia et al., 2018). The oscillatory interrelationships between the components within for instance cybersecurity system as well as the feedback loops, as underscored by Senge (2006) take prominence in the Systems Thinking paradigm.

In sharp contrast to the linear and reductionism theories, Systems Thinking theory gives prominence and pays a lot of attention to nonlinearity, complexity, dynamic systems and pluralism (Kensler, 2011). Corollary, leveraging Systems Thinking paradigm algorithm and characteristics, such as its inherent nature of recognizing interconnections, identifying feedback interrelationships and understanding dynamic behavior (Plack et al., 2017), researchers have optimized this paradigm cybersecurity domain to develop cyber security evaluation tool (CSET), which allows systemic assessment and analysis of dynamic nonlinear interrelationships within the cyber network (Woo, 2013).

The strength of the utilizing Systems Thinking finds resonance in the fact that both Cybersecurity and Systems thinking are domains predicated on traits such as natural science rudimentary background, pluralism, dynamic complexity, causal effect relationship, and interrelationships and iterative in nature (Eriksson, 2003). Based on philosophical and theoretical assumptions of Systems Thinking paradigm, exploration of the cybersecurity rapid and fast changing conditions such as the Denial-of-service attacks to the ICTs networks domains such as the websites is possible (Woo, 2013).

Cybersecurity

Cogently, in scope and scale, cybersecurity discourse has become a microcosm in the domain of global security (Comizio et al., 2015). The proliferation of modern technology especially the Internet of things (IoT), the ubiquitous nature of the cyberspace and the speed of technological advancement catapulted the world into a digital epoch which create complete dependence on computer mediated communication, virtual critical infrastructure and digitized operations – all enabled by the cyberspace capabilities and abilities (Ben-Asher & Gonzalez, 2015). The nations of the world have recognized the paradigm shift in the global security debates and policy discourse. The United Nations, NATO and other security-focused structures which all are symbols of global security architecture, well known for deploying physical military weapons are all seen to shifting to develop high tech military equipment optimizing with ability to optimize the digital space (Celik & Gurkaynak, 2019). Flowing from these assertions, it is therefore a logical thing to conclude that the economies of the world existentially depend on the capabilities and virtual tools of cyber space infrastructure in which IoT is deployed.

Cyber Threats, Risks, Vulnerability, and Uncertainty Conditions

The forgoing discussion cogently highlighted how the world has been transformed to the mode of complete existential dependence of literally every domain upon modern technology, i.e. cyber space, ICTs, IoT, devices, gadgets, hardware and software, to name a few (Pandey et al., 2019). On the other hand, ample evidence abounds that a plethora of cyber-attacks and threat vectors breed cyber risks conditions, uncertainties and vulnerabilities in the cyberspace (Pour et al., (2019). The literature also contends that

large threat landscape is orchestrated by proliferation of IoT deployed in networked devices or systems of critical infrastructure and that this is more prevalent and apparent in this era of rapidly emerging 4IR (Markelj & Zgaga, 2016).

Denial-of-service is counted among the common malicious types of cyber-attack agents used by intruders or adversaries to orchestrate interruption in network components such as webservers, memory processor, bandwidth, physical network infrastructure (Saghar et al., 2016). The DoS cyber-attack is arguably motivated not only by criminal purposes, but it is intentionally employed as a weapon or a tool for subverting political rivalries or as a form of political protest against undemocratic actions of government (Lutscher et al., 2020). Corroborating with this contention is considerable anecdotal evidence in several countries showing frequency of DoS attacks around the election periods (Lutscher et al., 2020). Inevitably, governments are confronted not by choice whether to allocate budget for cybersecurity policy area, but the vexing matter is optimal budgeting to strengthen cyber defense and resilience. The intended inquiry will employ qualitative paradigm as a means to describe the phenomenon of uncertainties in cyber space and its concomitant effects to budgetary processes in the domain of cybersecurity as it unfolds in natural settings of cybersecurity the public sector for South African government (Ravitch & Carl, 2016).

Cybersecurity and the Role of Government

The governance architecture of cybersecurity is described as a *"polycentric"* system in which rules and norms are made by multiple actors of government authorities strata at provincial or national levels (Carr & Lesniewska, 2020). The cybersecurity

discourse, gives rise to scholars' analysis that distinguishes between good or bad dichotomy of cybersecurity configuration and approach. Corroborating this line of thought, Wilmer (2018) acknowledged the state of flux in cyber space ecological complex. Qualifying this assertion, Wilner (2018), further reiterated the fast paced trait of the digital space and identified as contributory factors, the multiplicity of technological innovations and digital information in domains such as artificial intelligence (AI), IoT, ICTs, cloud computing, big data analytics, quantum mechanics and other several software products entering the market. Owing to the spiral increase of cyber threats, governments are compelled to build resilient cyber defense mechanisms, informed by distinct aspects: people, processes, physical and technology (Chatfield &Reddick, 2018). Recognizing the wide ranging detrimental impact of cyber threats, governments are seized efforts to secure cyberspace infrastructure. To this extent, governments are grappling with vexing questions such as: What is cyber risk? What type of security controls are required? How to respond when the incident occurs?

At least 75% experts consider cybersecurity as a priority, however only 16% confirmed by estimation that their government cybersecurity architecture would be able to adequately handle cyber-threat challenges (Pandey et al., 2019). Stated differently, in a number of jurisdictions, the cybersecurity is by and large underfunded, a situation that expand cyber risks for governments and technology consumers. Efforts of governments are underscored by the development of security national policy frameworks, to systematically respond to the increasing incidents of cyber-criminal activities perpetuated

intentionally by intruders or adversaries or unintentionally by systems operators who would have failed to adhere to cybersecurity algorithms (Srinivas et al., 2018).

The literature unequivocally underscores that a number of governments are engaged in efforts geared towards the paradigm shift caused by recognition that modern economies are driven by information and technology. The rapid rise, spreading and sophistication intrusion of adversaries operating in the cyber space, demand of governments the deployment of most robust and agile cybersecurity systems (Carr & Lesniewska, 2020). This is illustrated by the efforts of governments to build formidable cyber space defense mechanisms (Rudasill & Moyer, 2004). Stated differently, the cybersecurity government posture to decisively deal with potential harm to the network, computers and critical infrastructure caused by cyber-attacks is illustrated by the depth and breadth of cyber space security details deployed by government (Dor & Elovici, 2016). Government efforts to insulate their cyber space from potential cyber-attacks has direct proportion to the increasing government investment, the more cyber spacey defense equipment and software deployed the more financial resources are required (Kissoon, 2020).

Cybersecurity Dual Impact: Technological and Socioeconomic Effects

By and large, the literature on cybersecurity extensively brings to bear the extent of technological impact of cyber-attacks and malicious events to cyber space. A great deal of research in cybersecurity domain focuses on explication of technological tools utilized by the adversaries and intruders to launch cyber-attacks, such as the types of malware, array of cyber-threats as well as the resultant vulnerabilities and conditions. To

this end, considerable quantitative and qualitative research provides empirical literature on technological intricacies in cyberspace spectrum in the domains of hardware and networked systems enabling virtual information flow and communication (Taewoo, 2019). In this regard, a great deal of scholarly work deals with the nexus between technology and cybersecurity which involves the interplay between cyber-threats and a repertoire of modern technologies including, ICTs, IoT, smart technologies, hardware and software, smart manufacturing, physical systems of critical infrastructure to mention a few (Zoto et al., 2019). Stemming from this, cyber defense, cybersecurity enhancing, and cyber resilience has taken center stage in cybersecurity efforts by governments.

Ostensibly, the rapid rise of the ubiquitous nature of cyberspace technology, ICTs and IoT, has a simultaneously and drastically altered the socio-economic terrain by creating fast paced economic transaction and exchange of information (Taewoo, 2019). For instance, to date, the explosive growth of utilization of mobile computing cannot escape mention as catalytic enabler for technology-human activity interface (Boyce et al., 2011). In sharp contrast, the proliferation of technology and expansion of digital space together with networked communication, information systems and gadgets have inadvertently led to an increase in cyber-crime and has increased cyber-risk and vulnerability at individual, society, organization, and government levels (Boyce et al., 2011). The literature has established adequate evidence that the cyber-threats and all forms of cyber-crimes have far reaching adverse consequences to technical and socio-economic domains (Zoto et al., 2019). Recognizing this this fact, the literature has adopted a cardinal principle that seems to enjoy wide consensus among the academic

proponents working within cybersecurity domain as an emerging sub-discipline, that to create a strong cybersecurity infrastructure with potential to effectively avert subversion of digital transactions, the design of cyber-defense mechanism should ensure interface between people, technology and processes (Boyce et al., 2011).

Summary

Scholars have converging opinions on the fact that cybersecurity body of knowledge is still evolving and therefore the literature on this milieu is expanding and new streams of knowledge continue to emerge (Wilner, 2018). While the literature on cybersecurity continues to grow, however very scanty focus has been devoted to optimal budgeting for cybersecurity. The literature further juxtaposes the complexity of addressing cybersecurity as a consequence of expanding threat landscape induced by the evolving and dynamic advent of the 4IR characterized by ubiquitous expansive interconnectivity parameters, algorithms, and platforms provided IoT, social media, cloud technology and AI technologies, software and hardware (Wilner, 2018). Augmenting, Rogers (2016), postulated that serious policy considerations intertwined with the proliferation of social media platforms including WhatsApp, Facebook, Twitter, and Instagram, have impetus on creating real-time constant connectivity which has far reaching implications on cybersecurity governance for organizations (Rogers, 2016).

The exigency for securing cyberspace induced by the rising cyber-attacks fuels cybersecurity concerns and associated negative impact on key aspects of governments and organizations. This is evident in global scale social change driven by widespread digital connectivity and recalibration of international geopolitical/economic governance,

power dynamics, operations domain, and financial structure and services (Comizio et al., 2015).

Corollary, the literature reviewed in Chapter 2 contains large volumes of growing scholarly narrative reiterating the rapid emergence of cybersecurity global concerns. The reviewed literature also underscored considerable fundamental literature gap in the phenomenon of concern identified by this study. Furthermore, Chapter 2 attempts to provide broad explication of the phenomenon of concern and also illustrates concomitant nexus with identified the theoretical framework employed. Specific attention in Chapter 2 was given to capture the discourse and public debate on cyber threats, increasing risks and associated challenges with particular reference to optimal budgeting for cybersecurity as well as the impetus of this impact on governance of organization (Rudasill &Moyer, 2004). The mechanics of study design, definition of participants targeted by the study, instruments for data collection and data analysis plan is elaborated in the subsequent Chapter 3 which provides detailed structure of the research methodology of this study.

Chapter 3: Research Method

The focus of this qualitative study was to explore and describe cyber-threat conditions caused by the DoS cyberattacks that compromise cyber resilience by creating network instability, interruption, and vulnerability to the digital data and information assets. Drawing from the case of the South African, Cyber Security Operations and National Cybersecurity Hub, a unit charged with the responsibility for national cybersecurity coordination, I explored the phenomenon of DoS and cybersecurity budgetary implications. I investigated the dynamic and rapid emergence of DoS, which creates cyberspace vulnerabilities and instability that culminate in difficulties for optimal budgeting and financing of cybersecurity. Investigation on DoS cyberthreats and associated threat landscape conditions was done in juxtaposition with the difficulties caused by these frequently changing cyber threats and the resultant complex conundrums to government fiscal planning and budgeting for cybersecurity.

The exploration was conducted through the qualitative methodology to describe cyber risks and conditions associated with DoS that constrain the ability of organizations to determine optimal budgetary allocations and investment. Qualitative inquiry allows research on a phenomenon of concern to be conducted in its natural setting (Patton, 2015). The geographical location of the study was the South African government, Chief Directorate unit charged with national mandate for Cybersecurity Operations and serves as the National Cybersecurity Hub within the DCDT. This research contributed to the deeper understanding of the nexus cybersecurity and budgeting in the public sector. In this chapter, the methodology is explained (see Ravitch & Carl, 2016). This includes the

rationale for the research design, the role of the researcher, the methodology, and matters of credibility.

Research Design and Rationale

Qualitative methodology was considered as a design anchor for this inquiry. Qualitative research has evolved into a multidisciplinary paradigm that employs inductive dimension to pursue exploratory, explanatory, and discovery expeditions to understand social phenomena (Saldaña, 2016). Consistent with this inquiry's purpose and research questions, qualitative methodology was appropriate for the inquiry (see Ravitch & Carl, 2016). The qualitative approach resonated with the purpose of the study, which involved exploration and description of cyberspace uncertainty conditions and events that create challenges for budgeting and financing cybersecurity policy implementation for the South African government unit responsible for cybersecurity operations.

This study was guided by combining the purpose of the study and the research questions to investigate the phenomenon of concern and close knowledge gap on the nexus between the rapid emergence of cyber threats and their effects on budgeting in the government setting. In this study, I was the primary data collection instrument as the sole researcher. I also conducted data analysis and interpretation in line with the qualitative approach parameters including displaying poise and comprehensiveness (see Leedy & Ormrod, 2015).

In the domain of research, the case study design has been leveraged to conduct both qualitative and quantitative research expeditions. The design of the current inquiry was the case study approach to build on the great work of several researchers across a

range of disciplines (see Dooley, 2002). Yin (2003) observed that case studies resonate with the purpose to investigate and understand complex phenomena. Burkholder et al. (2016) noted that case studies allow researchers to confine the inquiry within a real-life setting of a contemporary phenomenon with a view to understand holistic interrelated interactions of different parts within a bounded environment.

Case studies are types of research enterprises that are instrumental in investigating events, social units, or organizations through intensive and detailed analysis in a descriptive and explanatory scientific inquiry (Burkholder et al., 2016). The design of the current study consisted of the following research questions to understand the complex and dynamic phenomenon of cybersecurity and budgeting challenges:

RQ1: What are the various Denial-of-service cyber-threat events and response coordinated by the National Cybersecurity Hub unit in South African national government?

RQ2: How does the rapid emergence of Denial-of-service cyber-threat conditions cause challenges for optimal budgeting and financing for cybersecurity operations managed by the Department of Communication and Digital Technology in South Africa?

Role of the Researcher

A researcher plays a critical role in discovering new knowledge in any scientific research process. Creswell (2013) postulated that there is a range of methods in which researchers can work with participants in a research enterprise. For instance, participants can be engaged as observer participants, observers, or participants (Creswell, 2013). In the current study, participants identified for interviews were identified according to their

relevance, information, and experience in the phenomenon of concern (see Burkholder et al., 2016). I assumed the role of observer and documenting agent during the process of conducting interviews to collect data. My interest in cybersecurity was motivated by the quest to contribute to cybersecurity discourse, which has become a topical policy and diplomatic subject in multilateral domains within which I was working at the time of this study.

I work for the African Union, which can be described as an African equivalent to the European Union. The African Union considers cybersecurity as a strategic governance and policy area that should be a high priority for the continent to safeguard ICT with related infrastructure and to protect socioeconomic sectors. To this end, at African Union cybersecurity policy work has been identified and listed among flagship projects. As the African Union policy expert, I was participating in diplomatic and public policy cybersecurity workshops and projects geared toward supporting the African Union countries to integrate cybersecurity into nation policies, plans, and budgets. The motivation and interest for focusing on the phenomenon of concern emanated from my professional association with and exposure to the phenomenon of concern.

This research took place immediately after the COVID-19 pandemic, which was declared by the World Health Organization as a pandemic of global concern. The geographical jurisdiction identified to conduct interviews was South Africa. I was staying in Addis Ababa, Ethiopia, which was my duty station at the time of conducting this study. Therefore, the distance was a considerable factor that required me to weigh options pertaining to conducting interviews for data collection. This challenge was compounded

by the reality that postpandemic period had been characterized by steep costs for traveling by air. As a result, traveling regularly from Ethiopia to South Africa to conduct face-to-face interviews became difficult. I took advantage of the emerging working method of virtual platforms to conduct interviews. I identified a virtual platform used widely by a number of organizations and government officials to hold meetings for business continuity, the Zoom virtual platform. The Zoom platform provided an option to conduct and record interviews with the participants. This facilitated effective and efficient data collection and documentation.

Methodology

The basis for selecting the qualitative research method for the current study was derivative of the purpose and research questions to which the inquiry aims to provide possible answers (Khan, 1994). The qualitative method is compatible with the purpose of the current study which was to explore and describe cyber-threats conditions caused by the Denial-of-Service (DoS) cyber-attack which compromises cyber resilience by creating network instability, interruption and vulnerability to the digital data and information assets. Combined with the qualitative research method and design, exploratory case study which inherently provides a scholarly methodological paradigm with tools to examine the central phenomenon in order to gain a comprehensive understanding of the unit of analysis was utilized. In this regard the case study was considered in this current study to be the most appropriate qualitative design to utilize to carry out the study (Burkholder, et al., 2016). Furthermore, the research was located in the public sector population, specifically the employees within South African government

Cybersecurity Operations Hub and Government Communication and Information System which constituted the unit of analysis for this study (Patton, 2002).

Participant Selection Logic

A cardinal principle underpinning participant sampling in naturalistic research is that the participant sampling resonates with the question at hand (Rubin & Rubin, 2012). The basis for identifying the participants for this study was the unit of analysis which is South African, Cyber Security Operations and National Cybersecurity Hub including Government Communication Information System. Purposeful sampling was appropriate for qualitative studies to collect data from participants who are knowledgeable about the research topic (Elo et al., 2014). Accordingly, the target population from which the participants for this study were drawn was the pool of the employees of the National Cybersecurity Hub including Government Communication Information System (Rubin & Rubin, 2012).

Participants

Well-reasoned decision for choosing respondents from whom insight was generated to provide plausible answers to the research question is a crucial consideration for any researcher utilizing the qualitative method (Ravitch & Carl, 2016). Given the vital importance of sampling strategy, as a researcher I had pre-conversation with senior officials of the Government Communication Information System and National Cybersecurity Hub, South Africa to obtain insight on the Cybersecurity government unit sub-structures from which potential participants' profile will be reviewed and drawn. Identification of participants was guided by purposeful focused-sampling strategy, this

facilitated the selection of participants with sufficient and rich information on the phenomenon under scrutiny. In the same vein, Kumar (2014), emphasized that qualitative research studies are characterized by purposeful selection of 'information-rich' respondent who can bring to the inquiry information specific to the phenomenon of concern. In the quest for rigorous data collection, participants with industry and sector specific experience and sufficient information were drawn from the site which is a case study and unit of analysis, the National Cybersecurity Hub in South Africa including the Government Communication and Information System through semi-structured interviews. Multi-perspectival and deeper insight was achieved by expanding the scope of information/data collection was achieved through referencing the archival material in the form of annual reports, information sourced from the dedicated website of the cybersecurity Hub national Cybersecurity policy framework, legal instruments, social media platforms and budget reports identifying participants within the Cybersecurity Hub, however in a typical stratified government hierarchy, it follows that the potential participants were operating at different positions and responsibilities which is a positive element that will arguably infuse diversity element to the collected data and contribute to rich information while taking into consideration the locality, contextual, macro-sociopolitical factors with a bearing to the phenomenon of concern (Ravitch & Carl, 2016). Gaining access to the potential participants and documentation was informed by a strategy of requesting the senior government officials including the Deputy Minister for Department (Ministry) of Communications and Digital Technologies, Director General, and the senior administrators of the National Cybersecurity Hub including the

Government Communication Information System, first to give permission for the researcher to conduct research within the government directorate that work at a policy and operational level on matters pertaining to cybersecurity (Burkholder et al., 2016). Furthermore, part of the strategy was to secure individual personal details, the name, contact number and email address to facilitate direct correspondence with participants to obtain appointments to undertake interview sessions on the Cybersecurity Hub as the unit of analysis (Burkholder et al., 2016). Consequently, I established a working relationship with confirmed participants, this included obtaining individual preferred communication method which I scrupulously observed in order to mount trustworthiness, transparency and respect in order to sustain unhindered access to the participant throughout the study (Wolgemuth et al., 2015).

Sample Size

Patton (2000) postulated that the qualitative inquiry is not a hard ruled based methodology when it comes to sampling, this includes the decision of sample size. To this end, the most important dimension to consider and strive for, in this research was to find respondents from the Cybersecurity Hub including Government Communication Information System holding senior, middle and lower levels of operational level to get an in-depth and reliable information and examine key documents such as annual reports and sector meetings reports as well as Ministerial budget vote statements and reports. Inferentially, these identified categories of participants represent the envisaged diversity and thus landed the inquiry into its data collection saturation point, which subsequently determined the sample size (Kumur, 2014). Ostensibly, in qualitative research, a sample

size within a range of 10 to 14 is typically sufficient, it resonated with the collection of an in-depth and reliable information which was instrumental to scientific exploration of the case study. Respectfully, the sample size for this study ranged between 10 to 14 participants for interview and matched the purpose of this inquiry (Reybold et al., 2013). Stated cogently, a minimum of 10 and a maximum of 14 of respondents was a reasonable sample size. However, the process involving onboarding of participants for interviews took into consideration open approach in so far as exploring opportunities to conduct more interviews until attaining saturation. True to the purposeful sampling, and typical of the case studies' samples, the size of this study was small in line with circumscription of the case study (Yin, 2014). In addition to the interviews, archival documents formed part of the data collection and were analyzed such as 1) annual reports, 2) national policy framework on cybersecurity, 3) Ministerial speeches, 4) legislative documents and 5) information from the website. Excluding the national policy framework on cybersecurity, the analysis will comprise of four retrospective years period starting from the current year. For instance, 2023, 2022 and 2021, 2020 Ministerial budget speeches were retrieved and analyzed.

Instrumentation

The literature showed that in a qualitative research case study inquiry such as this one, the research participants' contextual experiences and localized insight is fundamental in determining information-rich data. Thus, the data gathering instrument identified for this qualitative inquiry which facilitated rigorous and thorough answering of the research questions by the participants drawn from the unit of analysis was

interview strategy and analysis of archival material associated with the phenomenon under investigation (Ravitch & Carl, 2016). Specific questions (Appendix A) were prepared and the type of an interview approach that was instrumental to explore the central topic for this inquiry is the semi-structured interview (Rubin & Rubin, 2012). In this qualitative case study research, I was the primary data collection instrument with the semi-structure interviews being the secondary instrument. An interview protocol as another instrument elaborated in an interview transcript laying out real time and rigor nuances for primary data-collection considerations (Ravitch & Carl, 2016). Anchored on the purpose of the study the broader research questions were broken down as an instrument for investigative questions prepared to be posed during the semi-structured interview to obtain rich information about the phenomenon of concern (Rubin & Rubin, 2012). As a primary instrument in scheduled interviews, I had control of posing questions in a poised manner and flexibility to make follow through to obtain rich information and gain insight into the subject under study to fulfill the purpose of the study (Kumar, 2014). In a case study research design, the importance of specific contextual milieu factors comes into play, therefore the unit of analysis was a defining characteristic and an epicenter for drawing empirical information to inform the inquiry (Burkholder et al., 2016). Congruently, the content validity of the interview protocol which was part of the instrumentation of this study, was established through formulation of accurate and resonating sub-questions corresponding to the purpose of the research project (Burkholder et al., 2016).

Validity

Robust rigor and quality of the study is referred to as validity in qualitative research (Ravitch & Carl, 2016). Commenting on the critical importance of the construction of the research tools in a research inquiry Kumar (2014), accentuated that the underpinning principle is that the instrument gives credence to the alignment and validity of the data collected to the central purpose of the study. The seminal scholars in qualitative research have sharply raised centrality of rigor, quality, trustworthiness reliability of the findings of any research enterprise (Ravitch & Carl, 2016). Therefore, to address potential incongruence that may arise in the findings and appear to contradict the actual experience of the participants, the qualitative scholars underscore the paramount importance for researchers to strive to attain the highest levels of rigor in order to comply with validity standards which is an established yardstick, standards and criteria in qualitative research tradition.

Therefore, the validity in this study was established through ensuring that the participants identified are relevant and possess demonstrable deep knowledge on the topic of the inquiry. This means, through purposeful sampling, the participants were drawn from the unit of analysis which is the South African National Cybersecurity Hub within the Department Communication and Digital Technology including the Government Communication and Information System. Furthermore, to apply descriptive validity as a primary instrument for data collection in this study I made an effort to operate recording and transcription of factual accurate data (Ravitch & Carl, 2016). Establishment of the validity of interview questions in this inquiry was predicated on

synchronizing conceptual congruence of the purpose of the study and research questions as well as the case study approach which relies heavily on description and explanation on phenomena (Yin, 2014). The interview questions probed into the phenomenon of concern and explored dimensions that are related to the purpose of the study. The broader research questions as well as the interview questions were presented in an interview protocol by myself as the primary researcher using the language understandable to the participants devoid of academic jargon and sophisticated technical terminology (Rubin & Rubin, 201). Guided by the interview protocol, clearly sequenced questions and uniformity in posing of questions requesting participants to share their experiences and insight on the phenomenon of concern ensured coherent and systematic approach and consistency, thus achieving validity of interview questions (Ravitch & Carl, 2016).

Procedures for Recruitment, Participation, and Data Collection

Collection of data in qualitative paradigm is often underpinned by a fundamental question: Where is the interview data going to come from? This question provokes the need for a researcher to logically think about the respondents possessing current insight who can spare time for an interview on the topic under investigation (Babbie & Mouton, 1998). Simply put, data collection defines a process of gathering and analyzing information in response to the research questions (Ravitch & Carl, 2016). In the quest to optimize inherent experience and insight endowed among the employees of the government of South Africa operating within the systems responsible for cybersecurity across job grades and rank, my request directed at the South African National Cybersecurity Operations Hub including and the Government Communication and

Information System regarding conducting interviews expressly mentioned the desire to have interviews with officials with relevant insight on the topic, drawn from different categories of positions rank levels and line functions. Accordingly, my request to the Cybersecurity Hub and Government Communication and Information System, specifically indicated a desire to interview information-rich participants from senior representation and Chief Director, Director, Assistant Director levels and Cybersecurity technical experts for technical strata (Burkholder et al., 2016). Considering that this inquiry is located within the ambit of the Public Policy and Administration discipline, the sources of data included examination of archived documents and publicly available digital information assets including Nation Cybersecurity Policy Framework, annual reports and reports directly associated with the phenomenon being investigated and relevant legislative instruments and well as the social media platforms and dedicated website respectively. Qualitative case study research method provides latitude for utilization for multiple sources of data (Yin, 2014). This assertion is corroborated by Burkholder et al. (2016), they postulated that various sources such as archival records, reports, interviews and relevant documents can be used in a case study inquiry as evidence. Therefore, to collect data for this inquiry, two sources were utilized: 1) interviews and 2) archived documents including data domiciled in the digital assets such as website. Thus, I conducted interviews, and examined the National Cybersecurity Policy framework and archived reports and digital platforms pertaining to the Cybersecurity Hub for South Africa. Exclusively, considering that Cybersecurity phenomenon occurs within the domain of ICTs, I also surfed through the dedicated South

African website to examine and extract information that may be of use to respond to the research questions for this inquiry.

Owing to iterative nature of interviews coupled with methodological several multiple stages, I constructed an interview protocol as a guide for logical undertaking of interviews with different interviewees (Rubin & Rubin, 2012). Accompanied by the invitation letter to the participants, the layout of the interview protocol clearly outlined preliminary actions and interview aspects (e.g. details of the interviewee such as the designated position, the level of authority or responsibility, date of the interview, location, contact details etc.) name required prior to the interview session and milestones expected including introductory as well as closing remarks that I made as a researcher (Burkholder et al., 2016). To attain robust record keeping and documentation of responses during interviews, I utilized the combination of online-field notes taken during the interview via Zoom online platform and audio recording of all interview sessions conducted (Patton, 2002). In an iterative qualitative inquiry, combining data types facilitates the means to revert back to the transcripts and audio data and pick up some aspects of data that could have been overlooked (Patton, 2002). The interview sessions with each participant were planned to occur only once and the duration was 40minutes.

While the face-to-face interviews are a conventional method for the researchers, the proliferation of technology is fast changing the normative method. The capability and capacity of modern technology including virtual platforms which became more popular during Covid-19 have become part of daily and normal working methods. In this regard a choice to utilize Zoom online platform to meet, connect and conduct interviews with

participants. The choice of utilization of Zoom is determined by the fact that it is widely used by organizations, groups and even family members to hold meetings in circumstances where in-person is not possible. I also have Zoom account and I utilize it very often at my workplace to conduct meetings, therefore I am familiar with the platform and it was possible for to troubleshoot when technical glitches arose and posed potential to distrust the flow of an interview. The time line of 30 minutes duration is adequate for a decent interview session, ***Zoom*** online platform provides 40 minutes free connectivity time. Working within the confines of this virtual system, I used the last 10 minutes of 40 free minutes to wrap up an interview with each participant. The advantage of utilizing ***Zoom*** online-face-to-face was that the participant could choose a suitable and comfortable location and time. On the other hand, the disadvantage was that online meeting platforms such as ***Zoom*** are entirely dependent on internet availability and strength of connectivity. As such and as anticipated, concerning 3 participants who opted to do interviews online, the internet intermittently lapsed and impeded the flow of interview session, thus interrupted clear conversation which led to a follow through by phone call in order to conclude the session – a situation that caused increased frequency of interview sessions per respondent.

Data Analysis Plan

Reflecting on the data analysis in broad terms in contexts of qualitative research, encompasses consideration and making sense of data set compiled with a view to tease out and construct recurring themes which subsequently become findings of the inquiry (Ravitch & Carl, 2016). Buttressing this point, both Celano (2014); Sargeant (2012),

postulated that with a bigger scheme of qualitative research, data analysis is a critical steppingstone upon which researchers anchor data interpretation and ascribe sensible meaning in an endeavor to respond to the research question.

Notably, in qualitative inquiry data analysis is characterized by a series of activities including inductive action which is transformed into deductive corpus of documented insights that are key in responding to the research question. To this end the nexus between the data collected and the research question illustrates mutually exclusiveness, and conceptually congruency to identified themes which are processed into data categories that subsequently produce meaningful sets of information for data analysis (Lodico Spaulding; & Voegtle, 2010; Merriam, 2009).

Accordingly, in this exploratory case study inquiry significant corpus of data was collected and analyzed in an iterative and recursive manner utilizing semistructured interview as the main strategy (Ravitch & Carl, 2016). Utilizing qualitative data analysis techniques, significant patterns in the data was identified and a framework to convey the essence of findings was constructed (Patton, 2014). Data collection through in-person interview strategy for this study was constituted of two steps: the first one was semi-structured face to face interviews and he second one was conducted via ***Zoom*** online meeting platform. Initiating the first contact with identified participants, I sent a request and attached the invitation note approved by the IRB together with the ethical clearance approval to secure an appointment with already identified participants. Concerning the interviews conducted online, I booked individual online meetings and forwarded the link through the email with clear time lines for the interview meetings (Rubin & Rubin,

2012). The second step involved reviewing the archived organizational documentation such the main policy frameworks, relevant reports as well as reviewing pieces of digital information in the dedicated website of the South African Cyber Security Operations and Cybersecurity Hub and GCIS. Additionally, more information about the identified unit of analysis was drawn from annual reports, dedicated website of the cybersecurity hub, legal instruments, social media platforms and budget reports.

Qualitative data analysis included data organizing, reduction, categorizing and presentation of the corpus of information generated from semi-structured interviews conducted through posing a set of questions aimed at exploring certain aspects of the topic under investigation. Synchronized with this notion, is the assertion of Burkholder et al., (2016) emphasizing that, ordinarily, in semistructured interviews, researchers construct interview questions that resonate with the research question to distill the findings. Stemming from the foregoing, this inquiry was anchored on the following main research questions:

RQ1: What are the various Denial-of-service cyber threat events and response coordinated by the National Cybersecurity Hub unit in South African national government?

RQ2: How do the rapid emergence of Denial-of-service cyber-threats conditions cause challenges for optimal budgeting and financing for cybersecurity operations managed by the Department of Communication and Digital Technology in South Africa?

Data analysis for this study was done through performing coding based on the corpus of data collected which involves categorizing some words, concepts and phrases

as well as identifying some patterns of phrases and sentences which formed certain themes with some similar meaning (Saldana, 2016). As further pointed out by Saldana (2016), the data analysis for this small-scale research inquiry was done through performing automated coding through NVivo software powered with capability to enhance data analysis for qualitative research paradigm. Accordingly, after compilation of field notes of this qualitative case study, a series of processes including editing data, transcription of data recorded in Zoom platform will be carried out. As aforementioned, the automated stage involved utilization of NVivo software for data analysis in order to achieve rigor, trustworthiness, and validity (Gibbs, Friese, & Mangabeira, 2002). Utilizing the computer-assisted qualitative data analysis (CAQDA) software enhances the rigor and quality as well trustworthiness and credibility of the study (Smith & Hesse-Biber, 1996).

A plethora of research enterprises in the domain of qualitative research approach, have used NVivo software to facilitate data coding into common reoccurring themes (Edwards-Jones, 2014). Along with coding of qualitative data, clear and concise code definitions were assigned to data sets to generate systematic sorting of data, interpretation, and assigning of meaning to content to facilitate analysis (Ravitch & Carl, 2016). In pursuit of rigorous data analysis explicated in coding framework advanced by Saldaña's (2016), I used a combination of descriptive coding and values coding to leverage opportunity to ascribe labels to qualitative data gathered through conducting interviews and reviewing the documents pertaining to the unit of analysis case study (Saldaña, 2016). Furthermore, for the purposes of achieving rigor while conducting

coding during data analysis, researchers utilizing qualitative interviews often engage in iterative and repetitive processes to enable identification of recurring themes and concepts (Ravitch & Carl, 2016). The literature reveals that values coding is instrumental in virtually all the qualitative research inquiries to capture the complex interplay among actions occurring in a natural milieu such as the selected unit of analysis – in this case study, the Cybersecurity Hub, South Africa (Saldaña, 2016). To facilitate values coding, the archived documents and digital information pertaining to the unit of analysis was examined to extract recurring patterns in actions and expressions. The data generated from interview and turned into values coding was processed through the NVivo software for analysis to arrive at recurring thematic perspectives (Saldaña, 2016). The data collection and analysis comprised the sources of data as follows:

- Data generated from interviews
- Annual reports of the National Cybersecurity Hub
- National Policy framework on Cybersecurity
- Legislative instruments
- Ministerial speeches focusing on the phenomenon of concern (including budget speeches);
- Documented relevant reports information in the website

Coding is a technique available to qualitative researchers to organize and label data for subsequent data analysis (Ravitch & Carl, 2016). Accordingly, each of the documents identified as sources of data above are organizational dossiers already formatted into paragraphs and arranged in sub-themes. Given this fact, excerpts of sub-

themes pre-coded by highlighting, were run through the computer-assisted qualitative data analysis software (CAQDAS), in this case, the NVivo software for an automated identification of recurring themes (Saldaña, 2016). The coded themes identified from the organizational documents were integrated with the coded themes generated from the interviews to constitute amalgamated data. Altogether, the coded themes from data generated from the interviews and data distilled from the organizational documents were processed during data interpretation for the formulation of the findings of the inquiry.

Issues of Trustworthiness

Credibility

In qualitative research, credibility refers to the rigor and level of congruency of findings with the real situations in reality which in most cases is established through a technical application of reflexivity (Creswell, 2013). The primary concern of the reflexivity is self-examination of a researcher to ensure preconceived ideas about the topic and personal biases that may lead to subjectivity are cast off to avoid projecting these to the research project (Creswell, 2013). Correspondingly, as a researcher and a primary agent of data collection, I conducted self-examination and ensured that my preconceived ideas were removed from the research process to ensure credibility of the research findings.

Transferability

The extent to which the research findings can be replicated in other real-life situations is referred to as transferability or external validity. In respect to this particular inquiry, it is to be noted that the topic on cybersecurity is a relatively new and it is an

emerging phenomenon that still require extensive research. As a researcher, I was working on assumption that, given the specific angle of focus for this study and the fact that cybersecurity is a global phenomenon, transferability was achieved through a number of organizations and governments which might wish to refer to the findings of this study to enrich their policy discourse on public financing of cybersecurity.

Dependability and Confirmability

Future research projects should be able to depend on the research findings of this enquiry. Based on this assertion, it therefore follows that meticulous and logical documentation and recording of the research process became a pivotal technical undertaking that as researcher I vouched and committed myself to and I hereby assumed responsibility to produce findings that can be dependable. The dependability of this research involved conducting audit trails in order to capture all aspects of the research process. Stated categorically, this means the meticulous recording and documenting of interviews, correspondence with participants, audio-recordings, interview protocol and transcripts and all other artifacts utilized during the interview. The foundational and seminal research framework also played a major role in achieving dependability of the study. This meant articulating well the problem statement, proffering of prospectus, literature review, research design, data collection instrument and data collection process, data analysis plan and strategies as well as interpretation of the findings.

Pertaining to confirmability, Lincoln and Guba (1985) postulated that this refers to a process for ensuring the objectivity of the research findings, meaning the extent to which the findings of the study are shaped by the respondents' views as opposed to the

researchers' biases and motivations. Researchers have utilized audit trails and reflexibility to achieve confirmability with an ultimate aim to discard potential biases and motivations as well as paying attention to consistency to ensure coherence in coding of data and generation of data sets (van den Hoonaard, 2008). Emulating this well-established method in this inquiry, the audit trails were utilized to establish high sense of confirmability of the findings.

Ethical Procedures

Ethical protection and addressing ethical concerns is a critical aspect of scholarly research involving human respondents. This research inquiry drew inspiration from the Walden University (2015) Research Planning Ethics Worksheet which provides a template for preliminary assessment and identification of potential ethical concerns in the research enterprise. Accordingly, I submitted the Research Ethical Review application to the Institutional Review Board (IRB) for consideration and decision. The key documents that accompanied the application for Ethical clearance included interview questions, consent form and confidentiality agreement and invitation letter prepared for the potential participants. Subsequently, my ethical clearance application was approved by IRB. The approval # is 03-13-23-074250.

As stated in the foregoing discussion, the IRB application form was accompanied by the consent form which detailed the key aspects of the study and the elements of the interview process. This assisted to provide detailed information to potential participants and eased access thereof. Guided by the IRB, I secured a consent through signing of the consent statement during face-to-face interviews and by email for interviews conducted

through Zoom platform during the introductory moment with participant. The content of the consent form among other things provided description of the details of the research topic, processes of data collection and clarification of confidentiality and the voluntary nature of the participation in the study as well as benefits and risks where necessary (Khan, 2014). Congruently, Grossoehme (2014), suggested that the preliminary findings of data analysis should be shared with the participants. Hence, I forwarded the initial research findings to participants for validation of accuracy in order to ascertain and confirm the meaning of captured responses.

Summary

At the core of qualitative research, conducting interviews has an underpinning goal to explore deep, rich, contextual and targeted insight of purposely selected individuals who possess deep understanding of the topic of the central phenomenon under scrutiny. This qualitative inquiry was conducted by utilizing exploratory case study strategy in order to meet investigative needs stemming from the desire to explore and gain holistic understanding of phenomenon under scrutiny (Dooley, 2002). In line with the established traditions of the qualitative paradigm expounded upon by Burkholder et al. (2016), this research considered the identified research questions and constructed interview questions in synch with the purpose of the study. Consistency while interviewing different interviewees was ensured through developing, reviewing and updating the interview protocol (Burkholder et al., 2016).

Congruently, the research design of this inquiry provided the modalities to explore and understand the impact of Denial-of-service cyber threat events to the optimal

budgeting for cybersecurity. The research design was anchored on the tenets of case study research tradition. Carrying this study required me to assume the role of being an interviewer including objective documentation of all the content according to the account given by the interviewee on their work experiences, leading to accomplishment of data collection stage. Following the IRB ethical clearance approval, the face-to-face interviews were conducted and the online interviews mediated by the virtual platform, ***Zoom***, facilitated capturing the perspectives, experiences, motivations and insight of the administrators within the establishment of the South African government, Department of Communications and Digital Technologies and Government Communication and Information System. Additionally, data analysis plan included coding through using NVivo software application.

Accordingly, IRB procedures set out by Walden University while conducting research were followed. Drawing from the methodological design articulated in the Chapter 3 above, Chapter 4 will delve into the key aspects which informed data collection including the setting surrounding the participants and demographics and present the findings of the study and address all the quintessential data assessment parameters including data analysis and trustworthiness of the same.

Chapter 4: Results

The purpose of this qualitative case study was to explore and describe cyber-threat conditions caused by DoS cyberattacks. I explored cyberattacks' adverse impact on CMC systems and budgeting challenges. This study was aimed at investigating negative effects of DoS on cyber resilience and vulnerability to the digital data and information assets as well as the resultant conundrums to government fiscal planning and budgeting for cybersecurity. The purposeful sampling method led to the identification of the administrator experts considered to be insightful on matters concerning national cybersecurity and budgetary processes within the realm of policy and practice within the South Africa government cybersecurity policy discourse.

During semistructured interviews guided by open-ended questions outlined in the interview protocol (see Appendix), I captured and chronicled an assortment of organic responses from the identified professionals during the data collection interviews for the study (see Rubin & Rubin, 2012). Consistent with the methodology outlined in Chapter 3, data were processed through NVivo, which is software for qualitative data analysis. The data analysis was done in accordance with the qualitative paradigm to explore and describe phenomena under investigation. The qualitative case study design was used to answer two research questions:

RQ1: What are the various Denial-of-service cyber-threat events and responses coordinated by the National Cybersecurity Hub unit in South African national government?

RQ2: How does the rapid emergence of Denial-of-service cyber-threat conditions cause challenges for optimal budgeting and financing for cybersecurity operations managed by the Department of Communication and Digital Technology in South Africa?

Semistructured interviews were used to collect data from the participants. This chapter includes an overview of the data collection and data analysis procedures of the study. The research questions served as a basis for the development of open-ended interview questions outlined in the interview protocol (see Appendix). Also, I present the results from the data analysis and explain how these findings answered the research questions. This chapter also includes the setting or organizational conditions that influenced the participants at the time of study, demographics, data collection process, and dimensions of data analysis including coded units and categories and themes. The last section addresses trustworthiness of the data.

Setting

The Walden University IRB approved the research proposal on March 13, 2023. This initiated the process of contacting the partner organization, Department of Communications and Digital Technologies for the National Cybersecurity Hub, regarding identifying and scheduling interviews with participants. Although I was a South African at the time of conducting interviews, I was working outside the country in Ethiopia, which required planning with the partner organization to obtain a good measure of precision of scheduling appointments with the participants. During this study, a severe cyberattack incident occurred on March 3, 2023, which affirmed the adverse reality of detrimental effects of an interrupted cyberspace. Although I was persuaded of need for

research within the domain of cybersecurity, I did not have personal experience of the organizational impact of a cyberattack. The severity of the cyber-attack at my workplace led to a grinding halt of computerized communication within the organization. Due to the cyberattack, the server, computer network, and email system stopped functioning, leading to the collapse of CMC. Staff could not send or receive emails using the organization's Outlook emails. The severity of the cyberattack persisted for more than 2 months, a situation that adversely impacted the productivity of the organization.

Conducting interviews in Zoom was advantageous in that it was easy to persuade participants to consider an online interview because in-person interviews proved to be difficult. This allowed flexibility for leveraging online media, which worked to my advantage because I was living outside of South Africa. IRB approved the use of the Zoom platform to conduct interviews for this study. I conducted video calls, which allowed me to have an online face-to-face interview. In some instances, the interview seemed to consume too much bandwidth, so I asked participants to continue the interview without video to avoid connectivity glitches. The option to conduct either in-person or online interviews was communicated through an invitation and consent form shared with participant. Depending on the individual's circumstance, both options worked well.

I noticed that most of the participants were not comfortable doing online interviews because cybersecurity is considered a security issue by the South African government. Of the 10 participants, only three took online interviews. Conversing with participants beforehand allowed me to address their concerns and increase my traveling budget to travel from Addis Ababa, Ethiopia, which was my duty station at the time of

conducting interviews, to Pretoria, South Africa, which was the site of government administration headquarters. Traveling frequently to South Africa during the data collection period required efficiency in planning. I also had to intensify communication with the participants to ensure that each appointment honored their commitment.

In this regard I was able to address the concerns of some participants who had expressed discomfort in doing online interviews given the potential breach of cybersecurity information, which is a domain and function of South African state security. I allayed the concerns of the participants by informing them that personal identifiers would not be made public; instead, participants codes would be used to guarantee confidentiality. In accordance with Walden's IRB ethical guidelines, each participant signed the consent form, and I requested from each participant to record all interviews. Where interviews were conducted via Zoom, an built-in recording mechanism was used to record the conversation with the participant. During the in-person interviews, I used two recording devices: the dictaphone voice recording device and cell phone. This assisted me in documenting the conversation, which I used to produce transcripts from each interview.

Demographics

The participants were 10 professionals sampled from technical public administrators in the middle- to upper-middle management levels working in the government domain of cybersecurity. The participants were a group consisting of women and men of ages ranging from 40s to 50s working at various sections responsible for ICT and cybersecurity with the department. Participants had substantial hands-on

management experience in their respective responsibility. The work position titles for each participant were captured; however, codes were allocated to each participant to maintain confidentiality. The codes facilitated easy tracking of data and analysis, which led to identification of data codes that were processed to data categories with subsequent emerging themes. Chief among the characteristics of the participants was a wide range of ranks or work positions according to levels of responsibility with varying experience. I noticed that participants were drawn from two ICT subdomains, both of which address cybersecurity: ICT infrastructure and network and systems.

Archival data was harvested from the Department of Communication and Digital Technology; official website: www.dcdt.gov.za, under documents e-repository. In accordance with the type of sources of data specified in Chapter 3, the following documents archived in website of the partner organization were gathered as an integral part of data collection for this qualitative study. The documents collected to be examined include: Annual reports of the Department (Ministry) for Communication and Digital Technology (DCDT) National Policy framework on Cybersecurity, legislative instruments, Ministerial speeches focusing on the phenomenon of concern (including budget speeches), departmental strategic plan (2020-2025) and relevant information on cybersecurity that was contained in the website.

Table 1

Demographic Details of Participants

Participant ID	Age	Gender	Experience (years)	Position/rank	Ethnicity
P1	52	Male	25	Chief director, cybersecurity hub - DCDT	Indian
P2	45	Women	18	Director, IT infrastructure – DCIS	African
P3	47	Male	20	Deputy director, IT support – DCIS	Coloured
P4	42	Male	17	Deputy director cybersecurity - CSIR DCDT	African
P5	45	Male	20	Assistant director ICT expert, DCIS	African
P6	38	Female	12	Assistant director, cybersecurity hub	White
P7	43	Female	19	Assistant director, ICT support – DPSA	African
P8	50	Male	22	Deputy director, IT systems – DPSA	African
P9	53	Male	26	Director, information technology – government information technology officer (GITO) DPSA	African
P10	44	Female	21	Assistant director, ICT security DPSA	White

Data Collection

The steps for data collection started in earnest subsequent to the granting of ethical clearance by the IRB. The partner organization to which the unit of analysis was domiciled had already granted permission to conduct the study and contact person identified with contact details shared with me. Accordingly, I shared the relevant documents including the recruitment letter and consent form to the contact person at partner organization to facilitate initiation of the process of recruitment of participants. In consonance with the research tradition of purposeful sampling technique and the purpose of the study pivoted on exploring the nexus between rapid occurrence of cybersecurity with budgeting as a public policy, it became imperative to meticulously describe the profile of interviewees that were fit-for-purpose to guide the selection and recruitment of participants to the study. Eventually, a total of ten public administrators participated and

constituted the primary source of data for the study. Three-tier method in line with the methodology outlined in Chapter 3, was utilized to collect data: face-to-face in South Africa at the offices offered by the department responsible for Communication and Digital Technology where the National Cybersecurity Hub is domiciled, as well as via Zoom online platform. Of the ten participants only 30% took interviews online, the rest 70% was conducted face-to-face. In each interview, I used the introduction segment to describe the study for the understanding of the participant and outlined the required step to sign the consent form. The semi structured interview sessions both online and in-person were each allotted 60 minutes however, none of the interviews took the entire hour, all were completed within a range of 40-55minutes. The frequency of interviews was limited to only one session. An interesting trend emerged showing all the online interviews lasted for shorter period compared to the in-person interviews.

The third method of data collection consisted of gathering of relevant archived documents of the partner organization containing information relevant to the topic under investigation. The assembled documents included the National Cybersecurity Policy Framework, Annual Reports on cybersecurity, Strategic Plan (2020-2025) for the partner organization, Ministerial budget vote speeches, Public Service ICT directives for and legislative documents, e.g Cyber Crime Act (2021). Data collection utilizing the archived documents was necessitated by the need to achieve methodological triangulation through examining these documents to extract information related to the topic.

Data collection process was synchronized with the goal and purpose of this study which is to conduct a qualitative case study research and to explore and describe cyber-

threats conditions caused by the Denial-of-service (DoS) cyber-attack respectively. The data collection procedure approved by the IRB included interviews and review of archived documents extracted from the partner organization, the Cybersecurity Hub within the Department of Communication and Digital Technology (DCDT) including Government Communication Information System (GCIS). In line with methodological data collection procedure outlined in Chapter 3, purposeful sampling strategy was utilized to identify participants for interviews. Guided by the principles outlined in the consent form the partner organization was requested to assist in identifying the potential participants for this study. As postulated by Onwuegbuzie & Leech, (2007), large sample size is not a requirement in qualitative research, but of paramount importance is, the sample should constitute threshold adequate to provide an in-depth and richness of information and insight to inform the study. In this particular instance, the minimum number of required participants in accordance with the IRB approval is the minimum of 10 and 14 participants as maximum. The profile of participants targeted included: the public administrators working for the partner organization within the domain the domain of Cybersecurity under Information, Communication and Technology (ICT) section, possessing experience and insight in respect to South African cybersecurity planning budgeting, policy, practice and operations. The objective of conducting interviews and examination of archived documents of the partner organization was to obtain the viewpoints and insight of participants and extract the documented information to inform and chronicle a qualitative narrative towards answering the research questions of study.

Data Analysis

In scholar research practice, data analysis stage presents the researcher with an opportunity to undertake explanatory analysis beyond literal response to the research questions, in essence data analysis component in the research project involves conducting deeper searching of broader understanding of data in the context real life vicissitudes in the society at large (James, 2012). In line with the traditions of phenomenological approach, the study explored the practice and experiences of the participants in their real-life in relation to the topic, that facilitated collection of in-depth descriptive data. Subsequently, through utilization of NVivo 14 qualitative data analysis I was able to carry out categorization of data which led to identification of emerging themes (Creswell, 2013).

The audiotaped recorded interview transcripts served as the primary data for the study and after an iterative process of reviewing the transcripts the final version provided me with deeper understanding of participants' perceptions and insights of their lived experiences (Ravitch and Carl, 2016). The process of transcribing the recorded data which emanated from interviews included allotting alphanumerical code labels of *P*-series of *P1* to P10 as depicted as codes in Table-1. Upon the completion of the consolidated transcript, I imported the summative data composed of all the participants' perspectives on the research topic into NVivo qualitative data analysis software application to leverage its capability to organize and code data and ultimately formulate themes (Creswell, 2013). Based on the imported data of each participant into NVivo qualitative data analysis platform, the software application linked each transcript to

corresponding participant. The alphanumerical code I utilized to denote a participant was "P" and added a number of a participant next to "P" according to the sequence in which the participants participated in the interview sessions, from #1 to#10. Eventually a list from P1 to P10 was generated. The "P" series enabled easy tracking of data after I imported the transcripts of each participant to the NVivo software platform. As presented in Table-1, the participants were listed in a series of *P1* to *P10*, which in the NVivo application is referred to as project data files. This was followed by restating research questions one (RQ1) and research question two (RQ2) in the NVivo software tool. This paved the way to further synthesize the data by identifying significant information from each participant's transcript related to both research questions one and two. The NVivo qualitative data analysis tool capability enabled the creation of a data matrix that gave me a panoramic view of data collected, synthesized and broken down under question one and two, this assisted me have identify emerging congruencies among threads of data leading to categorizing the content into manageable and meaningful parts (Beekhuyzen, Hellens, & Nielsen, 2010).

Utilizing the NVivo software applications, I identified short statements as significant information, utilizing the data coding process I transformed data into categories of threads of coded information. Accordingly, this led to formulation of what is referred to as data containers which was holding categorized captioned significant data geared towards answering first and second research questions of this study. Similarly, the archived data identified was imported into NVivo platform. This was followed by further analysis of transcript-based data already uploaded into NVivo, this led to identifying

significant information in relation to RQ1 and RQ2 of this study. At this point the coded data containers for both research questions had already been framed and explicitly outlined under and in congruence with the two research questions – referred to as coded data containers for the purpose data sorting and analysis. In ensuring that all data under each alphanumerical code (P1-10 series) was reviewed and analyzed, I followed the sequential order to capture significant information and uploaded selected data into each data container codes already created under RQ1 and RQ2 within the NVivo software tool.

Guided by methodological triangulation determined in Chapter 3, I conducted the second aspect of data analysis utilizing significant information derived from the archived documents. In order to process the archived information, the computer-assisted qualitative data analysis software (CAQDAS), NVivo tool for qualitative was also utilized given that the software has a capability to hold secondary data in various formats including PDF files and pictures. Several selected archived documents ware thus imported into NVivo platform. Following review, examination and scrutiny of each archived documents, identified significant information was transformed into data codes which were uploaded into already existing coded data containers under each RQ in tabulated format within NVivo tool. The computer-based data analysis powered by NVivo is extremely useful to sort and arrange data into categorized coherent streams of corpus of information however it has limitations, its functionality is strictly analyst-driven and does not have live ability to interface with the computer controls. Recognizing this fact, I decided to transpose all the coded data under RQ1 and RQ2 into the excel for further analysis. Given that by design Excel provides table format, therefore a matrix of

tabulated data was produced in the Excel page. In order to gain more flexibility and control to further analyze data transposed from NVivo I copied the Excel data table into a Microsoft Word document to produce separate data table for both research question. The two separate matrix of coded significant information was sorted into clusters with similar connotation, leading to the formulation of coded broad thematic areas. The two Microsoft Word tables with coded data with five themes each were imported back to NVivo tool. During this point, in the NVivo platform I had significant data collected from information points specified in Chapter 3 as sources of data (interviews and archived documents) altogether coded into clusters of themes forming matrices under RQ1 and RQ2 as emerging findings of the study. As noted in the foregoing coding of data in qualitative research inquiry is an essential mechanism sorting and breaking down data into granular pieces to enable deeper understanding to inform attribution of meaning. The summative 10 set of themes with five under RQ1 and RQ2 respectively emerged as the preliminary results of the research project at which point had been transformed into distilled and deductive threads of significant coded information pertinent in answering the research questions (see Table 2).

Table 2

Themes for Research Questions

RQ1	RQ2
Building, monitoring and assessing cyber-defense system	Budgeting and financing cybersecurity
Creating and providing cybersecurity assistance and training	Experiencing rapid cyber-threat incidents and uncertainties
Developing and promoting cybersecurity policies and guidelines	Facing global markets price pressures for cybersecurity devices
Promoting global cooperation for cybersecurity response	Lacking advanced cybersecurity technology
Promoting national cooperation for cybersecurity response	Minimizing risks of cyberattacks in the network

The themes under both research question of this study which were generated from the data collection and analysis through NVivo software, constitute the main pillars upon which the presentation of the findings of the research project will be anchored.

Evidence of Trustworthiness

In pursuit of trustworthiness as aptly required in the qualitative inquiry, the following central tenets are employed by qualitative researchers to demonstrate research rigor and quality: credibility, transferable, dependable, and confirmable. These parameters are utilized by the qualitative fraternal in determining the accomplishment of trustworthiness. (Korstjens & Moser, 2018). Mindful that this inquiry is of a qualitative case study nature, I used interviewing as an instrument for data collection. As noted by Yin (2014) the interviews strategy is considered as an essential data collection approach.

Credibility

Credibility is a crucial aspect of trustworthiness; it is a determinant and yardstick of whether the research findings are believable and reliable to the reader. In qualitative

research, credibility refers to the rigor and level of congruency of findings with the real situations in reality which in most cases is established through a technical application of reflexivity. I used various measures for this research to be synchronous with credibility. Among these and considering that the nature of this study is qualitative exploratory case study, I utilized internal validity data analysis method of inquiry to ensure that the data collected for this study congruently resonated with the study purpose are credible. I intentionally cultivated good rapport with the participants to build mutual trust, and employed flexibility and made them aware of option of withdraw from the interviews at any time. Lincoln & Guba (1985), noted the importance of establishing credibility about gathered data on the phenomenon under investigation when conducting qualitative case study. Therefore, in relation to the process of data gathering, credibility for this study was established through reviewing data with participants by requesting them to provide feedback on transcripts that I produced based on the interviews conducted. Through repeated debriefing with participants, I crossed-checked the interview field notes which were already transformed into transcripts to ensure that the notes are in conformity with original statements made by the participants. In the quest to ensure credibility I employed participant member checking strategy; thus, the participants were requested to review the transcripts emanating from their respective interview responses. No discrepancy, no misconceptions or misrepresentation of facts were reported by the participants after reviewing manuscripts. This was one of the measures I undertook to ensure that the documented responses of participants which was emerging as findings of the research were reliable and credible. Triangulation approach that I employed involved reviewing

archived documents, which enabled establishment of validity of the responses provided by the participants which led to increased credibility**.**

Transferability

In a nutshell, transferability is another aspect of trustworthiness, concerning the extent to which the research findings can be applicable to other settings and contexts (Greene, 2014; Sutton & Austin, 2015). Transferability is viewed by scholars as aspirational findings of a research project. In the same vein, Peterson (2019), contends that another way to achieve transferability is through rigorously outlining the context of the study to enable future research undertakings to replicate it in similar situations.

Various research strategies were utilized to achieve transferability, and chief among these were literature review in Chapter 2 which provided broad spectrum of scholar research body of knowledge which can be used in future studies on the topic under investigation, the demography of participant was presented to clearly show the profile of public administrators who were part of the study. Additionally, the foregoing Chapter 4 provides granular details of the setting and conditions that may have influenced data collection. Another dimension that will facilitate transferability in this Chapter is description of location, mentioning of devices used for recording interviews, frequency and duration of data collection process. Altogether, these units of information enable the reader to be able to make associated comparison, inference, and comprehension of the research results of this study which enhances opportunities for transferability to other contexts. The type of software utilized which is NVivo and how it was used for data, importation, coding and formulation of themes was described to enable transferability of

the study findings. Cybersecurity is an emerging area of research; therefore, it was imperative to ensure transferability of the findings in order to lay foundation for future research projects and close the knowledge gap.

Dependability

Trustworthiness in research enquiry is also composed of dependability. This is a crucial aspect that establishes the consistency and reliability of the findings of the research project (Sutton and Austin, 2015). Of great importance in qualitative research is the extent to which the data collected enables research findings to be repeated while it resonates with future research projects. Stated differently, dependability' key traits are consistency and reliability of data collected for the study (Forero et al., 2018). Furthermore, dependability entails the replication of research findings with consistent results (Sutton and Austin, 2015)

The technique I used to ensure dependability was to keep audit trail of data collection process through documenting and maintaining interview transcripts, the interview audio recordings, and archival data to facilitate replication of research in the event a need arises and to sure consistency of the results. Another technique I applied during the interview is follow up questions to ensure accuracy and consistency in the data collection process for replicability of results.

Confirmability

Ordinarily, the last step to determine trustworthiness is confirmability which refers to the degree to which research findings can be verified, confirmed and repeated by other qualitative researchers. (Moon et al., 2016). Stated differently, confirmability

concerns itself with the extent to which the results of the research are representative of the participants views and insights. Confirmability also minimizes potential biases, improves accuracy and guarantees impartiality of the research study. Data presentation also determines the degree of confirmability of research findings. (Bengtsson, 2016). In this regard I pursued confirmability through analyzing data in a cogent, logical and consistent manner while ensuring adequate details were presented to achieve credibility. I also employed triangulation approach to collect and analyze data from interviews and archival documents to minimize biases and ensure contrasting and comparability of research results and achieve confirmability. Additionally, documentation of data collection process throughout the research process as part of audit trail enabled cross-checking of accuracy and consistency of responses of the respondents. Utilizing NVivo software for coding of data derived from both the interviews and archived documents to produce composite of schematic codes and patterns of analysis, altogether contributed to the confirmability of research results. The URR and my dissertation supervisory committee provided institutional framework for review and audit of trustworthiness of the study in line with the strategies stated in Chapter 3 on methodology of the study. Altogether these techniques contributed to deferring prejudgments, illumination and elimination of biases while sustaining the objectivity such replication of the data collected and analysis possible for future studies.

Results

The purpose of this qualitative case study was to explore and describe cyber-threats conditions caused by the Denial-of-Service cyber-attack which compromises

cyber resilience of computerized systems by creating network instability, interruption and vulnerability to the digital data and information assets vis-à-vis the resultant impact on budgeting for cybersecurity. In line with the methodology outlined in Chapter 3, a total of 10 public service administrators with experience and insight in the field of Cybersecurity and ITC were identified through purposive sampling and invited to participate in the semi-structured interview. Guided by the interview protocol (see Annex-1) I held a conversation with the participants and encouraged them to express and project their perspectives, insights and knowledge openly to inform the study. Utilizing triangulation strategy to complement data collected during interviews, archived documents were reviewed, analyzed and the insights distilled and battery of codes and themes were framed in the NVivo tool in order to respond to the research questions.

This study was premised upon the following two overall research questions:

RQ1: What are the various denial-of-service cyber threat events and response coordinated by the National Cybersecurity Hub unit in South African national government?

RQ2: How do the rapid emergence of denial-of-service cyber-threats conditions cause challenges for optimal budgeting and financing for cybersecurity operations managed by the Department of Communication and Digital Technology in South Africa?

As aforementioned, data sorting, analysis and formulating codes and eventual construction of a battery of themes was enabled by NVivo software platform. (Maher et al., 2018). This enabled generation of a scheme of several coded data out of which a total of 10 main themes emerged. This was subsequent to the process of data collection

through interviews and review of archived documents of the partner organization. Under each research question a total of 5 themes emerged and imported directly from NVivo software platform as presented in Table 3.

Table 3

RQ1 and RQ2 NVivo-Coded Themes

RQ	Theme	Category
RQ1: Response to DoS cyber threats	Building, monitoring and assessing cyber-defense system	Building strong cyber-defense system
		Conducting network assessment to prevent and mitigate cyber-threats
		Establishing and set-up cybersecurity sector structures to respond to cyber attacks
		Mitigating severe impact of cyber-threats
		Monitoring the network to identify cyber-threats timely
	Creating and providing cybersecurity assistance and training	Advising organs of government on cybersecurity issues
		Creating cyber-threat awareness
		Providing assistance in collective capacity
		Training youth on cybersecurity skills
	Developing and promoting cybersecurity policies and guidelines	Defining policy guidelines and protocols on cybersecurity
		Developing scenario planning about cyber-threats
		Promoting cybersecurity measures
	Promoting global cooperation for cybersecurity response	Liaising with global cybersecurity bodies for cooperation
	Promoting national cooperation for cybersecurity response	Allowing public and private sectors to cooperate on cybersecurity issues
		Coordinating cybersecurity activities at national level
		Mobilizing industry sectors to exchange information on cybersecurity
		Procuring cybersecurity service providers
RQ2: Challenges of budgeting for cybersecurity	Budgeting and financing cybersecurity	Delegating budget allocation decision across tiers of government
		Encountering financial constraints
		Estimating required budget for cybersecurity
		Investing in cybersecurity
		Motivating to justify spending on cybersecurity
	Experiencing rapid cyber-threats incidents and uncertainties	Experiencing rapid cyber-attack incidents
	Facing global markets price pressures for cybersecurity devices	Facing global markets price pressures for cybersecurity devices
	Lacking advanced cybersecurity technology	Lagging behind technology advancement
	Minimizing risks of cyber-attacks in the network	Handling uncertainties of cyber-threat events
		Minimizing risks of cyber-attacks in the network

Research Question 1: Coded Themes

In essence, the first research question concerns itself about the response government action in response to cybersecurity threats particularly the Denial-of-Service (DoS). Stated differently the RQ1 probes into the relevant national policy frameworks and legal instruments, the strategies and typical activities that the government relies on and undertakes to respond to cyber threats. As illustrated in Table-1, the participants offered a spectrum of answers in response to RQ1, this evident in themes and subthemes coded out the interview responses. The composite matrix of themes and subthemes includes the coded data emanating from the review, analysis and coding of significant information from archived documents related to cybersecurity for South African government.

Theme 1: Building, Monitoring, and Assessing Cyber-Defense System

The theme on building, monitoring and assessing cyber-defense system was distilled from the s expressions of the participants composed of administrative experts working within the technical, operational and administrative domains of cybersecurity defense system. The views of the participants extracted during the interviews were corroborated by the archived documents The core tenets expressed by the participants through this coded theme is the concrete measures required for the South African government to ensure strengthened cyber-defense. The concomitant subthemes (see Table 2) provide refined actions that according to the participants and archived documents, the government has put in place as formidable strategies to assess, monitor and build strong cyber-defense system for South Africa government context. Underscoring this point

during the interview, P8 pointed out that "DoS nature occur regularly however regular testing of the network allow us to respond proactively if there are suspicious cyber events."

In consonant with P8, P5 indicated that it is important to do "monitoring on cybersecurity environment infrastructure to see if there is no anomality or suspicion of malicious attack in the organizational IT infrastructure." These assertions of the participants about the need to monitor, assess and build strong cyber-defense were corroborated by the review archived documents. The findings also have strong congruence with the literature examined in this study which underscores the indispensable requirement for organizations to deploy strong technical capability for monitoring and carrying regular assessments of computer networks as a measure to build strong cyber-defense to prevent cyber-attacks. Linked to RQ1 and coded in NVivo platform under Theme-1, building, monitoring and assessing cyber-defense system are four sub-themes: 1) Building strong cyber-defense system, 2) Conducting network assessment to prevent and mitigate cyber-threats, 3) Establishing and set-up cybersecurity sector structures to respond to cyber-attacks, 4) Mitigating severe impact of cyber-threats and, Monitoring the network to identify cyber-threats timely. Altogether, the sub-themes represent the insights of the participants (*P1-P10*) and the significant corroborating data coded from the archived documents.

True to the understanding of the role played by the coded information at triggers and prompts and somewhat invokes a range of significant phenomenological account contained in the archived documents as secondary data and also noteworthy information

expressed by the participants during the interviews. According NVivo software analysis, the sub-themes mentioned above, were largely influenced in terms of coded information sources, by various archived documents and to some minor extend by the data collected from participants through interviews. In line with a cluster of sub-themes explicitly stated above, the Directives on cybersecurity document published by the South Africa government Department responsible for Public Service and Administration directed that "operating system updates and application updates are performed at least once a month or more regularly through a patch management process" This excerpt highlights the efforts of government to build strong cyber-defense system through regulating the utilization of the computer network systems and the directive to an extent of providing the time line in terms of the frequency within which the directive should be applied by the public service employees. Reinforcing this point the directive document shows the instructions that "Bi-annual vulnerability scans and vulnerability remediation are performed through a vulnerability management process" Furthermore, in consonant Theme-1: building, monitoring and assessing cyber-defense system and the concomitant cluster of sub-themes aforementioned, the Directives document instructs that "New software, portable media, and information in electronic format from external sources are scanned for malicious program code before being introduced into the department network" The Public Service Department Directives document also contains an instruction that "Penetration testing, vulnerability scans, and threat risk analysis are part of the departmental cybersecurity initiatives". The National Cybersecurity Policy Framework (2012), (NCPF), which provides policy direction and action for the public and private

sectors in South Africa, was one of the archived documents which provided corpus body of secondary data with strong resonance with the cluster of sub-themes coded in NVivo platform and imported to this study. In this regard, some significant corpus excerpts with strong correlation with the need for monitoring and assessment of cyber space with an aim of building strong cyber-defense were noticed in the text on NCPF: "Establishing the National Cybersecurity Advisory Council (NCAC) to advise the Minister of Telecommunications and Postal Services on policy and technical issues, and other matters pertinent to Cybersecurity pursuant to building confidence and trust in the secure use of ICTs." The data extracted from the NCPF is also instructive that "The continuous monitoring, review and assessment of regulatory frameworks that support cybersecurity."

Precise policy directives contained in the NCPF asserts that "Ensure, in consultation with the relevant stakeholders, the establishment of the Cybersecurity Response Committee, Cybersecurity Centre and proper function of the existing RSA Government CSIRT." This illustrates government' strong emphasis on Theme-1 pertaining to building strong cyber-defense system as a measure to respond to cyber-attack events which is a matter that the RQ1 is mostly concerned about from the perspective of the government.

Buttressing the points highlighted in excerpts extracted from the archived documents in the forgoing, *P1* stated that "the government cybersecurity Hub was instrumental in getting the Communications Risk Information Centre set up, that is the sector CSIRT for the mobile operators, then collectively there is capacity in the mobile sector to look at cyber-threats collectively." Augmenting information on the significance

of building strong cyber-defense, *P2* informed that "So we do have security software in place that helps us protect, prevent and detect the cyber-attacks." The assertions of the participants cited in the foregoing, provide compelling congruence with the notable data extracted from the archived documents.

Synthesized and coded in NVivo software from the large blocks of text contained in the Directives document and NCPF, as well the cited excerpts extracted from the participants' interview transcripts, altogether represent evidence of the administrative and regulatory measures the government took as well as phenomenological account on building strong cyber-defense system to circumvent adverse impact of cyber-threats such as DoS cyberattacks events. Strong connection between the literature review constructs and the themes coded in NVivo, highlighting the importance of cyber-defense system was also established. In the same vein, a notable solid concordance stemming from the excerpts extracted from NVivo-coded data emanating from the archived documents and the participants interviews also demonstrated notable correlation with the literature condensed in Chapter 2 section.

Theme 2: Creating and Providing Cybersecurity Assistance and Training

The cybersecurity policy action expressed in Theme-2: Creating and providing cybersecurity assistance and training emanates from NVivo-based datal analysis of interview responses transcript of the participants and from the reviewed archived documents data corpus that blended well with the Theme 2, under RQ1 of this study. This theme highlighting policy action focusing assistance and training on cybersecurity, resonates with the literature review carried which underscores the importance for

government to take a leading role to assist stakeholders in public and private sectors to put cybersecurity measures in place as empower public service with requisite skills to prevent and mitigate cyber-attacks. In respect to cybersecurity assistance to the stakeholders, the literature further points out two distinct dimensions of government interventions which is technical and social aspects. In consistence with the cybersecurity culture to safeguarding the network system of organizations employees ought to undergo training on basis knowledge on cybersecurity to cyber-threats (Ben-Asher & Gonzalez, 2015).

In response to RQ1which probes into the South African government response to cyber-threats, Theme-2 reinforced the facts established in the literature review in Chapter 2, explicating the need for government role to support the efforts to protect organizations against the cyber-attacks such the Denial-of-Service which has a potential to cause restricted access to the computer network and in worse case scenarios the cyber-attack could cause a network to grind to complete halt as well as exfiltration of intellectual capital. Accentuating this point, *P6* explained that "Accordingly the CSIRTs is an instrument to galvanize sectors to share risks and information about cybersecurity." The point of *P6* was further corroborated by *P10* who emphasized the need to "train employees to recognize & report cyberattacks (phishing, baiting, tailgating, etc)." Explaining further, *P10*, also informed that "training on information security awareness including security awareness or skills training targeted for specific roles including system

administrators, web application developers, and the helpdesk administrators focusing on cybersecurity measures."

In consonant with the point of view established during the literature review in Chapter 2, *P6* and *P10* shed light that government established the Computer Security Incident Response Team (CSIRT) to coordinate sharing and dissemination of strategic information of public and private sector actors as well as the need to conduct training with a view to prevent and mitigate cyber-threats. RQ1, Theme 2 is composed of sub-themes that emerged from data collection and analysis process through NVivo software: 1) Advising organs of government on cybersecurity issues, 2) Creating cyber-threat awareness, 3) Providing assistance in collective Capacity and, Training youth on cybersecurity skills. These clustered sub-categories are further pronounced in the excerpts extracted from the data collected from the one of the archived document selected for this study, the Guide for the National Digital and Future Skills Strategy, affirmed the assertion of P6 on government's role on cybersecurity assistance and training stated above that "One of the most important initiatives for the evolution of a secure digital economy in South Africa is the intermediate and advanced education and training in cybersecurity." Another archived document, the government Directives (2022) on cybersecurity was also on the affirmative pointing out that "The Department Information Security Officer (DISO) develops and implements a continuous information security awareness program to reduce cybersecurity risks from employees in the department." Congruently, the NCPF also ventilated on the importance of cybersecurity assistance and training in the following excerpt, "Development of capacity building strategies to address

South Africa's, specific skills requirements to meet the ever-increasing challenges of addressing Cybersecurity threats."

Theme 3: Developing and Promoting Cybersecurity Policies and Guidelines

Juxtaposing Theme-3 with the Systems Thinking which is a theoretical framework adopted in this study provides a worldview of seeing cybersecurity which is a phenomenon of concern through the lens of the interconnected, interdependent and interrelated elements of constituent parts can be investigated in a holistic method (Checkland, 1999). The Systems Thinking theoretical construct of non-linear instead pluralism is illustrated in the clustered corpus data sub-themes drawn from NVivo platform out of which the themes under consideration were formulated 1) Defining policy guidelines and protocols on cybersecurity, 2) Developing scenario planning about cyber-threats, 3) Promoting cybersecurity measures. Several proverbial traits of interconnected threads of instruments in the sub-themes including guidelines, scenario planning, measure which are interdependent for the policy action propagated by the themed under scrutiny.

This being the case, it follows that cybersecurity policies and guidelines should seek to systematically and holistically address cyber-threats to respond to RQ1 which probes into the types of measures that the South African government has put in place to respond to cyber-attack events with particular reference to Denial-of-Service malware.

Validating Theme-3, Developing and promoting cybersecurity policies and guidelines, participants' views included:

P10: "The policy assists to standardize the priority aspects of the cybersecurity."

P2: “we get guidelines or directives; we get what is called corporate governance information technology policy framework.”

P2: “understanding of it is still lacking with some administrators… the cybersecurity frameworks set out by government also has gaps… there is no perfect policy or framework hence there are guidelines are regularly issued.”

P3: “The National Cybersecurity Policy Framework provides the guideline and minimum-security framework on cybersecurity.”

P5: “the policy guidelines which prescribes the steps to take when encountering malicious activities.”

P6: “The National Cybersecurity Policy Framework (NCPF) is the ambarella instruments for both the public sector and the private sector.”

P7: “We are also guided by the policy to source support from outside support from outside bodies to assist in order to minimize the risks that are threatening the government network system.”

P8: Management of incidents and risks to our ICTs caused by cyber-threats is guided by the policy guidelines is elaborated by DPSA and distributed across organs of government.”

While a large number of participants expressed affirmative views about the policy actions espoused by Theme-3, Developing and promoting cybersecurity policies and guidelines. However, as documented above, P2, pointed out that government cybersecurity policy and legal frameworks are not necessarily a complete remedy they have gaps, and further mentioned that it is for that reason that the government regularly

issues guidelines for public service administrators. Accordingly, in line with the RQ1, P2 provided a phenomenological account of the action of government in regards to the policy action taken to ensure policy frameworks are responsive to the emerging exigencies of cybersecurity.

Anchored on triangulation methodology specified in Chapter 3, the archived documents examined demonstrated strong congruence with the insights of participants in relation to the theme under discussion. For instance, an excerpt extracted from the NCPF (2012) states that "NCPF is intended to provide a holistic approach pertaining to the promotion of Cybersecurity measures by all role players and will be supported by a National Cybersecurity Implementation Plan"

Another notable information pertaining the policy action espoused by this theme cited in NCPF (2012) is "it is also important to improve the legal framework against cyber-attacks, to enhance international and institutional co-operation." Additionally, the NCPF (2012) also documented another point aligned to Theme-3 that "Promote compliance with appropriate technical and operational Cybersecurity standards". There is synchronous alignment in the statements of participants and the text extracted from the archived documents. Phenomenologically, altogether, the data corpus collected affirmed, the theme: Developing and promoting cybersecurity policies and guidelines, as a policy action practiced by the government to respond to the cyber-threats events.

Theme 4: Promoting Global Cooperation for Cybersecurity Response

The main sub-theme captures and summarizes collected and coded data under Theme 3 is 1) Liaising with global cybersecurity bodies for cooperation. Inherently,

cybersecurity is a global phenomenon. This is corroborated by the literature examined in the foregoing sections of this study particularly Chapter 2, in which the facts on scale and scope of cybersecurity challenges transcending global governance architecture were expounded (Comizio et al., 2015).

In relation to Theme 4, *P4* reported that "South Africa is affiliated to the international cybersecurity structure called Forum for Incident Security Response Team (FISRT)." Commenting on the benefits of affiliation to FISRT, *P4* explained that "By virtue of the National Cybersecurity Hub being the member of FISRT it is possible to check the phishing website hosted from anywhere in the world using the international footprint through FISRT."

Connecting deliberate measures of South African government to liaise with global players in the field of cybersecurity resonates with the Systems Thinking theoretical construct cited in the foregoing, which advances the notion that cybersecurity requires a worldview relying on interrelated interdependences paradigm such as one illustrated in the cooperation of South African cybersecurity actors with FISRT to mount a systemic monitoring of cyber space in its complex nature within the Internet of Things with extensive plural interrelated and interconnected parts to proactively identify DoS ransomware which is a particular concern of RQ1 of this study.

As the main reference document guiding actors within the cybersecurity domain, NCPF (2012) largely pronounced itself on the policy action pertaining to the theme, promotion of global cooperation for cybersecurity response. Excerpts extracted directly from NCFPF (2012) include:

"Promotion and development of Cybersecurity measures in relation to this NCPF bear in mind the international instruments and measures that may be relevant."

"Facilitation of interaction, both nationally and internationally, including through international memberships to organisations such as the Forum for Incident Response and Security Teams (FIRST)."

"Recognizing the need for global collaboration on matters regarding Cybersecurity, South Africa is required to collaborate with relevant and appropriate international organizations and governments."

"Affiliate to relevant international organizations in order to promote a coordinated in the Cybersecurity front."

Affirmative to the expressions of the participants and inscriptions in the archived documents, particularly the National Cybersecurity Policy Framework (2012) as detailed above, the need for the global cooperation for cybersecurity, highlighted by Theme 4 is an integral part of governance of cybersecurity. Congruently, there is abounding consensus that cybersecurity domain transcends the international landscape of the cyber space. Much aligned to the literature review in Chapter 2, the extensive proliferation and ubiquitous Internet of Things (IoT), and types of technological advancement is governed through international cooperation of nations.

Theme 5: Promoting National Cooperation for Cybersecurity Response

In response the RQ1 that seeks to investigate the type of response of South African government to ubiquitous cyber-attacks such as Denial-of-Service, the participants and the data collected from the archived documents and analyzed through

NVivo software culminated to the Theme 5: Promoting national cooperation for cybersecurity response, which highlights one of the strategies to avert adverse impact of cyber-threats. Affirming Theme 5, *P1*, observed that the national cooperation for cybersecurity "allows the banks to cooperate around the issues of Cybersecurity where there is no reputational damage, they can share information and risks. Additionally, *P1*pointed out that "the Cybersecurity Hub gets information from other national Computer Security Incident Response Team (CSIRT) and then disseminate information on incident among the sector CSIRTs so that's the purpose of the cooperation. At another dimension *P2*, underscored the role of cooperation with the private sector and stated that "the department often get external independent service providers to come and do cybersecurity assessment" Emphasizing the tenets espoused by Theme 5, *P3*, expressed that "collaborative learning between government entities is important to strengthen cybersecurity domain "Another point expressed by *P4* pertaining to promotion of national cooperation for cybersecurity was that "The cybersecurity Hub also has a role to coordinate Public Private Partnership to create the bridge between the private sector and government state organs" Buttressing the points of other participants, on Theme 5, P6 reported that, "accordingly the CSIRTs is an instrument to galvanize sectors to share risks and information about cybersecurity.

Coded and analyzed together with the participant's responses in the NVivo software, archived NCPF (2012) stated that "acknowledging that Cybersecurity is everyone's responsibility, public sector, private sector and civil society"

The views expressed by the participants above echoes the perspectives elaborated in the literature review in Chapter 2, which emphasizes the importance of the role of government to deploy national strategies to address a challenge to determine preventive measures, proffer national cybersecurity policies and provide budget to build strong cyber-defense system against cyber-threats such as the Denial-of-Service.

To this end, the aforementioned excerpts extracted from the transcripts and archived documents and analyzed through NVivo software also strongly resonate with theoretical construct adopted in this study, Systems Thinking which is predicated on holism, interrelationship and interdependence of all parts working together in a system (Shaked & Schechter, 2017) A proverbial example is illustrated in the excerpts emphasizing the importance of cooperation among different facets of national actors operating in public and private sectors working together to prevent and mitigate cybersecurity as expressed in Theme 5.

- Augmenting the aforementioned phenomenological perspectives in the foregoing, is the following clustered codes which culminated to Theme 5:
- Allowing public and private sectors to cooperate on cybersecurity issues
- Coordinating cybersecurity activities at national level
- Mobilizing industry sectors to exchange information on cybersecurity
- Procuring cybersecurity service providers

Overall, the Themes 1-5 in the foregoing highlight profound phenomenological perspectives emanating from the semi-structured interviews of participant's including the

significant information extracted from archived documents in response to the RQ1of this study.

Research Question 2: Coded Themes

The second research question for this study sought to investigate and probe into the challenges concomitant with the optimal budgeting and financing for cybersecurity. Gordon et al., (2018) elucidated that budget for cybersecurity consist of the total expected annual outlay allocated for capital expenditures related to mitigating cyber threats. Accordingly, while scrutinizing the challenges that impede efficient investment and allotment of financial resources for securing and installing effective cyber-defense systems, particular reference to peculiar effects of DoS to the network will be reviewed and juxtaposed to the responses of the participants and the documented perspectives distilled from the archived documents that were reviewed. A spectrum of coded statements emanating from the interviewed participants including significant information extracted from the archived documents and coded through NVivo software were framed in a form of coded themes and sub-themes and presented in Table-1in line with the concern of RQ2 for this qualitative study on optimal budgeting for cybersecurity in the case of South African government.

Theme 1: Budgeting and Financing Cybersecurity

Aptly, questions relating to efficient budgeting for cybersecurity were posed to the participants to tap into their knowledge, experiences and understanding of the budgetary consideration in respect to allotment and investment on cybersecurity. Equally, archived documents were reviewed. Responding to RQ2 in line with the Theme under

scrutiny, the Directive on Public Service Information Security issued by the Department of Public Service and Administration. (2022). The Directive document provided a broad the justification for budgeting for cybersecurity explaining that "The current digital era has seen the increased importance of data and information, thus giving it the status of being the economy's raw material. It has brought the importance of protecting data and information to ensure its confidentiality, integrity, and availability" Meanwhile the literature review in Chapter 2 advanced the argument that efficient and optimal budgeting for cybersecurity is difficult. Among the conundrums that were cited in the literature was the enormity of cyber space uncertainties manifesting in spontaneity of various cyber-attacks rendering the network system vulnerable to numerous risks. Corroborating this sentiment, *P1* stated that "It's true for organizations it is difficult to budget for cybersecurity." Furthermore, *P1* commented that the ability to recover and respond is a function of how much the company has invested" Responding to the challenges espoused by RQ2, Theme 1, *P2* made a range of observations:

"The initial investment is high but once the organization gets a right system there is ability to do frequent disaster recovery tests"

The finance part of it is that the higher solution or availability replication costs a lot of money"

"Government does not have money; some requests have not been honoured because investing in cybersecurity is an expensive enterprise

Government does not have money, some requests have not been honoured because investing in cybersecurity is an expensive enterprise."

"Closing the cybersecurity gaps means financial investment to improve cyber defense."

"Limited budget is the limiting factor for optimal budgeting for the cybersecurity…limited budget for cybersecurity prevents the organization to procure services"

Elaborating on Theme-1, *P5* stated that "So budget wise the costs are fluctuating you cannot put a fixed amount or fixed budge it varies" Affirming the views of *P5, P6* explained as follows, "At my level of operation, I am aware that to build a strong cybersecurity defense, healthy budget is required".

The statements made by the participants on the theme under consideration were corroborated by an archived document which was reviewed, analyzed and significant information coded through NVivo, the National Integrated ICT Policy (2016) of South Africa contended that "The disadvantages of the current broad incentives are that they have to be competed for against established and capital-intensive industries. They do not apply a budget quota system to ensure that all the sectors can benefit."

The literature review in Chapter 2, recorded a strong case that on the aspect of rapid emergence of cyber-attacks leading to highly uncertainty within the cyber-space, thus causing a complex and complicated policy option which makes it difficult to achieve optimal budgeting, participants made the following observations:

P7: stated that "it is difficult to know when cyber-attack will occur and how many time a week, a month or a year."

P8: "Government has limited budget for cybersecurity. It makes it difficult to attain optimal budgeting for the cybersecurity."

P8: "The rapid nature of cyber-attacks complicates budgetary process and makes it difficult to estimate budget in most efficient manner."

P9: "While the fiscal demands are increasing the GDP is declining meaning the economy is not growing. This creates limitations and prohibits government to adequately invest on cybersecurity."

Juxtaposing the above participant's views with the Systems Thinking approach which is a theoretical framework predicated on holism providing a lens which enables researchers to have a worldview in which the different parts of the organization are working together in an interrelated and interdependent manner.

The participants responses are illustrative of the Systems Thinking theoretical framework adopted in this study. By cogently affirming the RQ2 Theme-1on the challenges on cybersecurity budgeting, the participants demonstrated in their statements, the interrelationship between rapid emergence of cyber-threats which cause uncertainty, exacerbate vulnerability within network and computerized systems, and the difficulty all these parameters create making it difficult for the government to allocate optimal budget for cybersecurity. Plack et al., (2018) give a precise explanatory point on how the Systems theory outlines the systemic interrelationship of each constituent part playing its crucial role yet not individually self-sufficient to fulfil the systemic aims which require holistic interdependence behavior of each part to produce the whole. Following this line of thought, the participants mentioned a plethora of dimensions concerning operational

parameters of cyber security which creates a dynamic and complex system with rapid changes and rapid emergence of cyber-threats which make it difficult to have fixed and optimal budget. For instance, *P8* elucidated that "The rapid nature of cyber-attacks complicates budgetary process and makes it difficult to estimate budget in most efficient manner." Being a theoretical framework premised on complexity, interrelated and interdependent systemic approach, the Systems theory resonate with this inquiry on cyber-space and cybersecurity which is in all its facets inherently complex with various interacting parts. It is in this context that through Systems Thinking theory, it is an established fact which is vehemently corroborated by the participants and the archived documents, that optimal budgeting and financing for cybersecurity is extremely difficult due to plurality of factors and rapid emergence of cyber-attacks. This situation was explained by the participants a recurring risk management consideration posing complex policy challenge for South African government as it is the case for other organizations.

The data analysis through NVivo platform enabled the formulation clustered codes which constituted diverse perspectives of the participants which were broken down into sub-themes outlining the types of challenges associated with the optimal budgeting for cybersecurity: 1) Delegating budget allocation decision across tiers of government, 2) Encountering financial constraints, 3) Estimating required budget for cybersecurity, 4) Investing in cybersecurity, 5) Motivating to justify spending on cybersecurity.

The dimension of budgeting challenge expressed in sub-theme: Estimating required budget for cybersecurity, was addressed by *P1* wherein he provided a solution to this constraining issue as follows, " There is a financial model called the Gordon-loeb

model which is utilized to measure the amount of budget allocation that might be required by the organization to spend on cybersecurity" Notably, while a number of participants expressed phenomenological accounts on difficulties for government to achieve optimum budgeting for cybersecurity, however *P1* .offered a solution stating that through utilizing Gordon-loeb model, the organizations can estimate budget allocation for cybersecurity.

In the context of government strata for South African vis-à-vis budget allotment for cybersecurity, *P1* revealed another dimension as part of challenges constraining efficiency gain. This is expressed in sub-theme pertaining to: Delegating budget allocation decision across tiers of government. This challenge evoked the need for the application of Systems Thinking theory which provides systemic a comprehensive and holistic consideration of interrelated components of government system including multi-tier government configuration and concomitant together with associated budgetary exigencies for each government level.

Theme 2: Experiencing Rapid Cyber-Threat Incidents and Uncertainties

As elucidated above, RQ2 is concerned about investigating the challenges which cause limitations to efficient and optimal budgeting for cybersecurity. The RQ2, Theme-2 represents the participants phenomenological reported that the rapid cyber-threats incidents and uncertainties impedes efficient allotment of resources for cybersecurity. In consonant, the literature review in Chapter 2, revealed that Denial-of-Service cyber-threats which are classified as active attacks, create cyber space network rapid and highly risky uncertainties, vulnerabilities and instability to digital data, information assets, and

ICT critical infrastructure thus creating enormous difficulties for the government to provide optimal allocation of the budget. Asked about the difficulties hindering optimal budgeting for cybersecurity, the participants responded as follows:

P1: "It is difficult to optimally budget for cybersecurity due to rapid emergency"

P9: "The unpredictable and rapid nature of cyber-attacks makes it very difficult know plan properly and budget, hence allocation of budget in a dynamic environment come with a lot of difficulty"

P10:" Cyber-attacks are highly unpredictable and rapid nature. This has an impact on budgetary process, first the budget allocation might not be adequate due to the dynamic nature of the cyber space"

Affirming the participants responses, one of the archived documents, the NCPF (2012), revealed that "The recurrence and growing incidence of cyber-attacks indicate the start of a new era in which the security of cyberspace requires a global dimension and the protection of National Critical Information Infrastructure must be elevated, in terms of national security"

The challenge impeding efficient budgeting for cybersecurity espoused in RQ2, Theme-2: Experiencing rapid cyber-threats incidents and uncertainties, is illustrative of complex situation consisting of rapidity and uncertainty with the cyber space. Typically, such conundrums are ubiquitous in the cyber space, as illustrated by *P1, P9* and *P10* responses above. According to the literature reviewed in Chapter 2, endovours to prevent, mitigate and recover from cyber-attacks are often compromised by the challenge revealed by the participants and extracted from the archived documents expressed in the

aforementioned Theme-2. Buttressing assertion, Islam et al., (2018), postulated that due to Internet of Things spectacular speed and expansive nature of cyber space, rapid emergence of cyber intrusion, cyber-attacks, cyber-crime, cyber-threats events are on an upward trajectory. Congruently, Quigley et al., (2015) underscored that staying ahead of the rapid emergence and uncertainties induced by the cyber risks, governments are required to address a challenge to instill preventive psychology among employees. This resonates well with the Systems Thinking approach which is elected as a theoretical framework for this study. The Systems Theory provides the systemic view which enables holistic monitoring of interrelated parts which can assist the government to be able to estimate the frequency of cyber-attacks in order to estimate budget allotment.

Theme 3: Facing Global Market Price Pressures for Cybersecurity Devices

According to the literature review in Chapter 2 in the foregoing, it is already an established fact that cyber space and ubiquitous IoT scope and scale transcend the international terrain making it a global public good (Pour et al., 2019). The letter and spirit of the Theme-3 focusing on global markets prices for technological equipment, accessories and devices to address cybersecurity illustrates that cybersecurity is a global phenomenon. To this end, the phenomenological accounts of participants providing scientific evidence and significant information distilled from archived documents and processed through NVivo software, revealed the following regarding the Theme under consideration:

P3: "Cybersecurity is driven by overseas strong international economies markets; this has an impact on price structure of the cybersecurity products and commodities."

P3: “Cybersecurity products are available in international markets and procuring the expensive.”

P4: “Governments usually procure outsourced service providers”

P7 “What makes cybersecurity more expensive is that other cybersecurity tools are not available in the South African market they are procured from abroad.”

P7 “Procurement costs of cybersecurity instruments is thus subjected to the volatile markets within high fluctuation of prizes.”

P8 “The cost of cybersecurity is driven by overseas strong currencies of international economies markets; this has an impact on price structure of the cybersecurity products and commodities”

P9 “The price structure also is difficult to predict since cybersecurity tools to strengthen back up and to update the systems are procured from abroad markets with high fluctuations”

The excerpts of participants above all together reinforced one of the dimensions which makes it difficult to achieve optimal budgeting for cybersecurity. On the other side, the theoretical construct which is predicated on utilizing comprehensive and holistic lens of understanding the behaviour of a system advanced by the Systems Thinking resonates well with the excerpts of interviews conducted among the participants. The excerpts of the participants reinforced the assertion postulated by the literature in Chapter 2, that revealed challenges associated with budgeting for cybersecurity created by volatility of international markets costs of equipment, gadgets and devices which are used in cyber defense infrastructure. In this regard and in line with the RQ2, Them-3, the

Systems Thinking theoretical construct which propagates monitoring holistic interrelationships between different parts within a system, offers what is could be construed as an approach to address the fluctuation and volatility of costs equipment and gadgets of cybersecurity in the international markets. Taking into consideration the pertinent points raised by P3, P4, P7, and P9, including the fact that the cybersecurity products are available in the international markets, costly, price is driven by strong international currencies from strong economies leading to the unpredictable price structure. Organizations can harvest value proposition by leveraging the theoretical construct propagating the interdependency and interrelationships of different parts working together in a systemic manner develop comprehensive and holistic monitoring systems to collect data.

Theme 4: Lacking Advanced Cybersecurity Technology

It is worth mentioning that Theme-4: Lacking advanced cybersecurity technology was distilled from coding of significant information derived from the archived documents on NVivo platform. Recalling the focus of RQ2 which aims to investigate the challenges associated with conundrums inhibiting government of South Africa to optimally budget for cybersecurity. The Theme under consideration highlights the deficit on advance technology required for cybersecurity as one of the difficulties inhibiting optimal budgeting for cybersecurity. This factor, was recognized and pointed out in the Budget Vote Speech (2022) of the Deputy Minister responsible for Communication and Digital Technology, he stated that, “Existing ICT skills are becoming obsolete, and this increases the demand for new digital skills. These changes require humans to be equipped with the

relevant and necessary skills to perform the new jobs" The Deputy Minister's contention was corroborated by the observations extracted from the Nation Cybersecurity Policy Framework (NCPF, 2012), that "The challenges of Cybersecurity are fueled by advances in technology. Consequently, there is a need to develop the requisite skills to exploit the opportunities of an information economy and meet the dynamic challenges of Cybersecurity and that…South Africa is a consumer of ICTs and depends on overseas manufactured technologies to secure its cyberspace" Apart from the challenge of deficit of advanced technology, as documented in the archival documents examined, another dimension of ICT skills among employees getting absolute due to the rapid technology advancement in the global markets was highlighted in the captioned excerpts in the foregoing section. High demand of ICT skills to deal with cybersecurity is a fact that is already stated under RQ1 section as one of the key conditions that government need to strengthen cyber defense. The RQ2, Them-4 focusing on lack of advanced cybersecurity technology, aligns with already established facts in Chapter 2 under literature review, that due to high frequency and dynamic advancement in the configuration of cybersecurity technologies, governments have a challenge to adapt and adopt technologies which are exorbitant to procure, adding to the already high demanding exigencies of embedding strong modern cyber defense devices and infrastructure (Fielder et al., 2016). Through embracing Systems Thinking theoretical paradigm which propagates the notion of leveraging plurality of elements working together in an interrelated manner, the governments stand a change consider all the emerging evidence in the foregoing

discussion to improve efficiency gains in order to achieve more with less to address the deficit of modern cybersecurity technologies.

Theme 5: Minimizing Risks of Cyberattacks in the Network

Several coded themes and sub-themes in the foregoing discussion under RQ2 section brought forth evidence various inhibiting conditions creating difficulties for the government of South Africa to achieve optimal budgeting for cybersecurity. Augmenting to numerous hinderances to efficient financing for cybersecurity are challenges exacerbated by difficulties of highlighted in RQ2, Theme-5: Minimizing risks of cyber-attacks in the network. Breaking this Theme further the two sub-themes were identified through coding in NVivo software: 1) Handling uncertainties of cyber-threat events, and

2) Minimizing risks of cyber-attacks in the network. The participants interviewed, expressed several diverse but coherent perspectives on the RQ2, Theme-5 vis-à-vis the difficulties created by the cyber-space rapid emergence uncertainties culminating to constraining force hindering optimal budgeting for cybersecurity:

P1: “uncertainty of cyber-attacks, which comes in various severity”

P2: “initial investment must cater for uncertainties”

P2: “software solutions must be constantly updated to fight against the uncertainties of potential cyber threats”

P3: “it is not always guaranteed to get such budget allocation to minimize cyber risk

P5: “make some contingent plan to minimize cyber-attack risks”

P7: “it is difficult to know when cyber-attack will occur and how many time a week, a month or a year”

P8: Limited budget for cybersecurity prevents the organization to procure services, anti-virus and back up services to address potential cyber-threats”

P9: “The rapid emergence, the depth of uncertainty as well as the vulnerability of cyber space to risks of and the multiplicity of cyber-attacks makes negatively affects planning and budgeting for cybersecurity”

P9: “The vastness of the cyber-space and rapid proliferation of software, tools infrastructure devises make cybersecurity space a highly volatile and dynamic making difficult to allocate financial resources due to ever shifting ground”

In consonant with Creswell (2013) assertion that phenomenological studies rely heavily on interviews, the above account on lived experiences of participants including P1, P2, P3, P5, P7, P8, and P9 provided evidence on challenges heaped by uncertainties in cyberspace causing cataclysmic failure for governments to be able successfully and consistently minimize the cyber-attacks thus compromising the ability of government to allocate optimal budget for cybersecurity. The participants’ interview excerpts above identify the key challenges inhibiting minimization of cyber-attack risks. Key among these is the rapidity, severity and vastness of cyber space, and proliferation of software which inadvertently creates large cyber-attack surface area exacerbating vulnerability of the network increasing proneness to cyber-attacks. The second aspect highlighted by the participants in the excerpts above is the synergistic connection to limited budget

rendering governments unable to have adequate financial resources to invest to procuring cybersecurity technological tools to minimize the cyber-attacks risks in the network.

Placing the RQ2, Theme-5 together with the stated perspectives of the participants in the forgoing, in juxtaposition to the Systems Thinking approach, and recognizing the plurality and complexity associated with cyber space rapid, and frequent emergence of cyber-attacks, brings to bear the compatibility and utility of the theoretical construct as it offers systemic and holistic world view to analyze the vulnerabilities within the network identify interrelated elements playing out, and determine requited mitigation measures to ultimately minimize the cyber-threat risks.

Summary

True to the notion that analyzing interviews from different participants could lead to the finding of shared or similar experiences that may be significant to address the research problem, Chapter 4 drew data from shared perspectives of participants' interviews. This being a qualitative case study focused was purposed to explore the impact of rapid emergence of cyber-threats with specific reference to the Denial-of-Service and concomitant challenges to optimal budgeting for cybersecurity. In Chapter 4, I utilized the two central research questions to formulate questions for data collection through interviewing participants and reviewing archival documents. The results discussed in Chapter 4 are to a large extent a function of the analysis carried out in the NVivo software tool. Consequently, following coding of data through NVivo software, a total of ten Themes composed of five coded clusters under each research question became the ultimate results as depicted in Table 2. Semi-structured interviews were

utilized to collect the participants insight, experience and knowledge to inform this study that focused on cybersecurity which included questions related to RQ1 and RQ2. The data was recorded in the voice recorder and the data collected was organized and transcribed to produce transcription containing all the responses documented during interviews. Two methods of interviews were utilized according to IRB approval, face-to-face and via Zoom online platform to collect data.

Triangulation was an integral part of the approved methodology for this qualitative cased study. Accordingly, several archived documents were identified as sources of data and were reviewed with RQ1 and RQ2 in mind. The review process culminated to identification of significant information, and excerpts were extracted and coded through NVivo software and coded statements were combined with the codes derived from the interviews to form the Themes that were the basis for data analysis in Chapter 4 in the forgoing

Upon transfer of coded cluster of ten Theme distilled as derivative of several significant statements of the study based of participants' explanatory accounts based on their phenomenological insights, knowledge experiences and perception. The data collected from semi-structured interviews and archived documents was then processed through NVivo software platform and transferred to this qualitative discussion as depicted in Table 1. Subsequently, the analysis ensued in a sequential order of RQ1 and RQ2 Themes respectively. Out of ten Themes which emerged after data coding process through the NVivo software, altogether an in-depth description of the study, data collection, data analysis was presented.

A framework of Theme-based analysis was adopted. Accordingly, following the logic of responding to each of the two research questions, I undertook an in-depth thematic analysis of the research findings in conjunction with the literature review in Chapter 2 and further examined the emerging findings against the context of the Systems Theory which was adopted as the theoretical framework for this study.

The study findings documented under both RQ1 and RQ2 showed strong congruencez with the hypothesis that was linked to the problem statement of this study and subsequently gave rise to the research questions that are well stated in the forgoing sections. Pivotal to RQ1 was a focus on the cyber-threat events with particular reference to DoS cyber-attack in tandem with the vital aspect of investigating the types of responses that were deployed by South African government to prevent, mitigate and, institute recovery in the event the cyber-attacks strike. Five Themes represented the findings derived from the data collected from the cybersecurity public administration experts who participated in the semi-structured interviews conducted face-to-face and via Zoom online platform. Triangulation method to achieve requisite vigor was utilized. Arising from this, several archival research was conducted to extract significant information and evidence in conjunction with RQ1of the study.

Central to RQ2 was investigation of rapid of emergence of Denial-of-service cyber threats conditions with propensity to inhibit optimal budgeting and financing for cybersecurity – the case of the Department of Communications and Digital Technologies, government of South Africa. Compelling evidence derived from the participants and archival research strongly affirmed the proposition propagated by the problem statement

which argued that the rapid emergence of cyber-attacks in the cyber space create complex scenarios with consequent repercussions resulting to difficulties to achieve optimal budgeting for cybersecurity.

Stemming from the findings discussed in this chapter, recommendations will be proposed in the subsequent Chapter 5 with a view to advance and propagate solutions detailed in the findings and efforts to strengthen cybersecurity architecture to prevent and mitigate adverse impact of cyber-threats events. Several proposals pertaining to viable strategies to circumvent difficulties with the achieving optimal budgeting for cybersecurity were documented in Chapter 4 of this study and concomitant recommendations will be presented in the subsequent Chapter 5 based on the insights and perspectives derived from participants' interviews and archival research.

Chapter 4 provided a thick description of the performed research methodology and its alignment to the research design described during this chapter. These descriptions supported the transferability of the findings by providing enough information for readers to determine if the results could be transferable to their knowledge settings.

Building on the research components including the setting, data collection and data analysis, trustworthiness and results which is elaborated in Chapter 4, the subsequent Chapter 5, will include the reiteration of the purpose and nature of the study. Characteristic of a qualitative study, Chapter 5 will also elucidate the results and provide analysis of how the study contributes to the body of knowledge in the cybersecurity discipline as the focal domain in conjunction with the literature reviewed in Chapter 2. The main sections of Chapter 5, will be constituted by the analysis and interpretation of

findings, which will be described in juxtaposition the theoretical framework adopted for this study, the Systems Theory. This will be followed by the recommendations and implications of the study to Social Change.

Chapter 5:

Discussion, Conclusions, and Recommendations

The purpose of this qualitative case study was to explore and describe cyber-threat conditions caused by DoS cyberattacks that compromise cyber resilience of computerized systems by creating network instability, interruption, and vulnerability to the digital data and information assets. Consistent with the research purpose and research questions, qualitative methodology was chosen for the inquiry. A qualitative approach resonated with the purpose of the study, which involved exploration and description of cyberspace uncertainty conditions and events that create challenges for budgeting and financing cybersecurity policy implementation for the South African government unit responsible for cybersecurity operations. A qualitative case study was conducted to capture the responses given by participants during the interviews and the significant information captured through archival research conducted as a triangulation measure. A total of 10 participants were identified through purposeful sampling, including government officials working in the field of ICT directorates focusing on cybersecurity within the Department of Communication and Digital Technology, South Africa.

Semistructured interviews were conducted to explore expert perspectives. The literature reviewed in Chapter 2 revealed a scholarly knowledge gap in cybersecurity and optimal budget allocation. Leveraging the systems thinking theoretical framework, I explored and described the cyberspace conditions caused by rapid emergence of cyber threats that compromise cyber resilience, and the extent to which these uncertain

conditions create difficulties for governments to achieve optimal budgeting for cybersecurity.

Interpretation of the Findings

Ascribing meaning to the data collected during qualitative research is a central phase of the research process. According to Lincoln & Guba (1985), a reflexive technique of plays a critical role during the pooling and analysis of different perspectives informed by significant information drawn from several data sources. My study was informed by blended data collected through participants' interviews and archival data.

The established research steps indicated that data collection should be followed by data analysis using techniques and tools at the disposal of researchers. I used NVivo software to analyze the data collected from the interviews with participants and through archival research. Using NVivo enabled me to transform the voluminous data into 10 themes with five themes for each research question. The findings for RQ1 and RQ2 were derived from the perspectives of the participants and the data extracted from archival documents. The findings central to this inquiry included South African coordinated responses to circumvent, prevent, and recover after cyber -threat events.

Findings for Research Question 1

The findings for RQ1 revealed that the South African government relies heavily on the internal (national) and external (international) cybersecurity governance machinery and architecture to respond and strengthen cyber-defense systems. The findings indicated that the national cybersecurity governance configuration is a competence of national government. The findings indicated strong congruence of the

cybersecurity governance approach of the South African government with the examples illustrated in the literature reviewed in Chapter 2. Similar to other organizations and governments, the cybersecurity institutional arrangements exemplified by CSIRT and the governance design including national policy frameworks (National Cybersecurity Policy Framework in the case of South Africa government), guidelines (issued to address evolving cybersecurity needs induced by rapid emergence of cyberattacks), and directives on cybersecurity advice for the public sector and private sector were noted as key findings. The frequency of issuance of directives was necessitated by the need to galvanize measures to match the dynamic and rapid emergence of cyber-events within the cyberspace to deliver a strong cyber-defense system.

Regarding cybersecurity governance, the findings indicated that the government established industry/sector-based structures composed of a network of CSIRT deployed to determine and calibrate the type of cybersecurity response in the public and private sectors and to operate as the focal points working closely with various industries. The primary functions of CSIRT, according to the key findings, were to galvanize cybersecurity cooperation including cyber-threat risk assessment, coordinating sharing and dissemination of strategic information among public and private sector industry actors, and determining required training needs to be conducted with a view to build capacity to prevent and mitigate cyber threats. Convergence of findings from participant interviews and archival data provided another key finding under RQ1 that DoS cyberattacks occur regularly. Regarding adverse effects of DoS, which compromise cybersecurity, the participants' perspectives showed firm alignment with findings from

the literature review in Chapter 2, which indicated that cyberattack worst case scenarios of DoS could lead to prohibition of access to the network by users, a network grinding to a complete halt, and exfiltration of intellectual capital (see Pour et al., 2019).

However, several targeted cybersecurity responses of the organizations that safeguard cyberspace digital asserts to strengthen cyber resilience to achieve threat circumvention and mitigation include the following:

- Organizations' regular testing of the network enables organizations to respond proactively if there are suspicious cyber events.
- Conduct regular monitoring on cybersecurity environment infrastructure to prevent potential anomality or suspicion of malicious attack in the organizational IT infrastructure.
- Conduct penetration testing and vulnerability scans.
- Carry out threat risk analysis, software, portable media, and information in electronic format from external sources scanned for malicious program code before being introduced into the department network.
- Conduct biannual vulnerability scans and vulnerability remediation performed through a vulnerability management process.
- Perform operating system updates and application updates at least once a month or more regularly through a patch management process.
- Develop and implement a continuous information security awareness program to reduce cybersecurity risks from employees.

Dual dimensions that include technical and social cybersecurity safeguard measures constitute typical government interventions; this is according to another recorded key finding of the study in relation to the South African government response toward building cyber-defense systems with a view to strengthen cybersecurity assistance in support of stakeholders. An additional finding was the affirmation that cybersecurity is a global phenomenon that requires cooperation with international interlocutors. Reinforcing this was the finding revealing the affiliation and reliance of the government of South Africa on the dedicated global cybersecurity facility referred to as the Forum for Incident Security Response Team (FISRT), which supports the affiliates with cyberspace monitoring and stopping adverse cyber-threat events.

Findings for Research Question 2

The second set of central findings were derived from the RQ2. Chief among these is the financial model known as the Gordon-loeb model which according to the participants' perspective, is utilized to estimate how much organizations should spend on cybersecurity. This study also discovered the influence of international markets in shaping the cost structure of cybersecurity products, tool, devices and commodities, thus driving the price to skyrocketing levels. According to the literature review in Chapter 2, there is an overwhelming acknowledgement by experts working in cybersecurity that due to complexity caused by high volatility and rapid changes in the cyber space it is difficult to estimate costs required for cybersecurity. Based on the arguments advanced in the literature review in Chapter 2, difficulties in estimating costs for cybersecurity is further exacerbated by instability, uncertainty and increase in interdependent cyber connections

within the Internet of Things and Computer Mediated Communications. During the interviews, the participants confirmed that the lack clear sources of data to compute cybersecurity costs, sparked more research. Efforts to respond to complex conundrums which create limited capacities and abilities for the experts in cybersecurity to optimally estimate required budget allotment for cybersecurity, have led to devising and innovating a computation algorithm composed of (1) costs per incidence, and (2) costs per data breaches. The findings which emanated from the interviews of the participants in Chapter 4, provided insight on cost factors of cybersecurity and affirmatively indicated that these two data types of cyber costs for cybersecurity domain is utilized by experts to feed into Gordon-loeb model which is utilized by experts to workout close to accurate estimates for the budget required for cybersecurity.

Evidence gathered in Chapter 4 revealed that owing to the disproportionate impact of the high performing currencies of overseas strong international economies, the exorbitant purchase price of cybersecurity infrastructure equipment and devices inhibits the organizations to acquire adequate cyber-defense tools due to high prices. In consonant with the assertion articulated in Chapter 2, Lees et al., (2018), the findings strongly concurred that the high price factor of cybersecurity equipment and devices driven and determined by international markets forces is an inhibiting dimension for South African government to achieve optimal budgeting for the cybersecurity.

Limitations of the Study

Recruitment and onboarding of participants identified for interviews was the most difficult aspect of the study. While the approved threshold of 10 purposely sampled

participants were successfully recruited and participated in the study, the maximum number of 14 participants which was submitted and approved by IRB was difficult to attain. This was a limiting factor to the study; more interviews could provide more perspectives and insights to enrich the study.

Notably, another dimension pertaining to the limitation of the study was the noted, it concerned a cogent inadequate literature and narrow body of knowledge on the specific area of concern which was investigated by the study which focused on the scrutinizing the cyber factors associated with conundrums of attaining optimal budgeting for cybersecurity.

As anticipated in Chapter 1, and expressed the fact that across the globe, cybersecurity is by and large considered as a domain with strong nexus with national intelligence and state security, the results of this study precisely illustrated that South Africa is not an exception. During the study, it came to light as expected that since participants will be drawn from government, there might be reluctant to share all information as a result of general understanding of information sensitivities associated with cybersecurity data. Recognizing this characteristic of cybersecurity which came out clearly in the results of this study, Celik & Gurkaynak, (2019) cogently elucidated that apart from the technical nuances and there is a social dimension cybersecurity with permutations pronouncing political and legal practices concerning national security concerns.

However, with further persuasion, the participants generously provided their perspectives which informed this inquiry. However, it was not possible to get more

information on cybersecurity as it was deemed by the participants as classified and under the purview and competency of the State Security Agency (SSA) of South Africa. In ideal circumstances the study would provide a vantage point with a panoramic view yielding much deeper and wider set of results and understanding of the phenomenon that was investigated, however, thirty percent of the participants did not completely fit the profile of working full time as cybersecurity experts, but they were generalists working as technicians under ICT directorate which covers Cybersecurity operations as well.

Recommendations

Despite these limitations that are elaborated in the foregoing, the results from the study and associated interpretations provided compelling reasons and basis upon which to predicate future research initiatives with multiple possibilities to generate genuine new interests to guide studies that further examine the potent aspects of cybersecurity as demonstrated by the findings and related interpretation in Chapter 4 and Chapter 5 respectively.

The preceding four Chapters of this phenomenological qualitative case study which was predicated on a purpose to employ the lens of Systems Theoretical construct to explore and describe cyber-threats conditions caused by the Denial-of-Service (DoS) cyber-attack which compromises cyber resilience of computerized systems by creating network instability, interruption and vulnerability to the digital data and information assets.

The study also covered the limitations caused by conditions induced by Denial-of-service cyber-threats to optimal budgeting. Furthermore, in Chapter 1, there was

recognition that notwithstanding the rapid growth domain of cybersecurity as an emerging discipline, the preceding study has not received adequate scholarly focus, hence the literature is limited (Ben-Asher & Gonzalez, 2015). This being the case, it was clear in foregoing discussion that cybersecurity as an emerging sub-discipline and new research stream, can benefit immensely if various policy thematic areas and permutations can receive further research scrutiny, that is if those aspects can be pursued further. Pursuant to the strengths and limitations of this study, consequently a set of recommendations were formulated as articulated in the subsequent sections pointing to the areas for future research.

Recommendations for Researchers and Academicians

Cybersecurity is certainly an existential common factor in numerous futuristic studies predicting and projecting two dimensions which is technological and socio-economic needs at organizational and individual levels. It is thus recommended for the future studies in cybersecurity to delve deeper to scholarly investigate the dual effects on technological and individual dimensions. This line of research is particularly important given the fact that cybersecurity sub-discipline keeps on evolving and characterized by dynamism. The research may have to focus on teasing out permutations of adverse impact of cyber-attacks at micro (individual) and macro (organization or government) levels.

Drawing from the lesson learned from this study pertaining the profile of participants vis-à-vis the credibility of the study which is an aspect of trustworthiness, it is recommended to expand the number and utilize larger sample size of participants

which specifically focus on cybersecurity operations government function in order to increase changes for securing relevant and impeccable information during data collection. At the centre of successful data analysis for this study was the NVivo software qualitative data analysis tool. Utilizing the software analysis enabled a systematic, coherent and logical approach to data analysis for this inquiry. Therefore, drawn from the pragmatic experience associated with this study, I recommend for the future qualitative researchers to strongly consider utilizing available software tools for data analysis.

At the level of choosing the Theoretical Framework for future cybersecurity related case study qualitative studies, the Systems Thinking theoretical construct is recommended. In respect to this study, the Systems Thinking theoretical construct which recognizes systemic interrelationships and interdependencies resonated with the study. It enabled and facilitated consideration and studying complex relationships in-between cyber-threats feedback loops of various parameters, elements and outputs of the phenomenon that was being investigated. Pursuant to this explication, Systems Thinking is recommended for scholars wishing to pursue a qualitative case study on cybersecurity.

Recommendations for Organizations and Governments

The policy propositions that arose from this study are relevant for both government and private sectors. Fragmentations and incoherent policy coordination for cybersecurity operations with the South African government was apparent during the research process. Such inconsistences were pointed out by the participants, it was observed that that the National Cybersecurity Policy Framework (NCPF) was developed by the South African, State Security Agency (SSA) however the cybersecurity policy

coordination seems to be the competency of the Department for Communication and Digital Technology. Within the same Department a National Cybersecurity Hub was established, however according to the participants perspectives, the Hub is poorly resourced in terms of the budget and human resources. Exacerbating the cybersecurity ecosystem complex is the fact that regular government directives on cybersecurity guidelines for the public sector is issued by the South African Department for Public Service and Administration. Evidence confirming cybersecurity policy coordination responsibility which is sparsely distributed to across numerous administrative government entities manifested more prominently in the archived documents reviewed as triangulation approach for this study. Thus, in line with cybersecurity governance approach highlighted in the literature review in Chapter 2, it is recommended that organizations and governments should set up a well-defined, well-resourced government structure to ensure clarity is cybersecurity policy coordination and mobilization of whole of government approach to effectively and efficiently govern cybersecurity policy issues.

According to the findings of the study, the Computer Security Incident Response Team (CSIRT), was construed as vital aspect of the cybersecurity architecture that enabled policy coordination and strategic information exchange in order to circumvent devastating effects of cyber-attack events for public and private sectors. In this regard, the recommendation pertaining to the CSIRTs is for the government to commission more studies on the utility of CSIRTs structures and extent to which government and industries are able to leverage these to strengthen the national cybersecurity.

Stemming from the RQ2 which sought to investigate the conundrums concomitant with inability to attain optimal budgeting for cybersecurity, the findings of this study revealed a financial model known as the Gordon-loeb model which is utilized by experts to estimate costs related to cybersecurity. In conjunction with this, and considering that the financial models might be a solution, it is recommended for future studies to focus methodological approach employed in the Gordon-loeb model in order to gain insight and develop more models which could be used to estimate the budget required by organizations for cybersecurity operational function organs.

Implications

The foregoing study illustrated how convergence of ICTs such as computer mediated communication, the technological advancements such as IoT, AI and blockchain create a virtual global ecosystem of network of digital systems. Rapidity and ubiquity characterize cyber space with far reaching implications to society, organizations and individuals.

Individual-Level Implications

Measures to build strong cybersecurity does not only improve infrastructure to benefit the society but technology is experienced at individual level as well. Gadgets such as personal computer and sell phones are good examples of individualized consumption and utilization of technological advancements. Unless efforts to circumvent cyber-threats and which cause individuals to operate in secure cyber space, impact of cyber-attacks event can be detrimental to individuals.

This study highlighted several positive social change implications at an individual level. The universal truth that information is power epitomizes the positive social change in the context of this study which revealed that the government conducts regular awareness to sensitize the individuals on the perils of cyber-attacks with emphasis on prevention and appropriate measures to be taken by individuals in order to mitigate damage to personal technological gadgets.

Societal-Level Implications

In accordance with the literature elaborated in Chapter 2, cyber-attack events have devastating effects to the digital assets of organizations. This study provided explication on how Denial-of-Service cyber-threat can bring the computer network operations of government to a grinding halt. Developing and promoting cybersecurity policies and guidelines was one of key findings affirming a positive social change at a societal level. The study offered several propositions of practical measures for building strong infrastructure for cyber-defense to mitigate severe impact of cyber-threats.

At a different level, the findings of the study underscored another dimension of positive social change at a societal level through providing cybersecurity assistance and training for stakeholders in public and private sector. The intervention of government to enhance safeguarding the network system of organizations through making training of employees a mandatory undertaking to deepen their knowledge on cybersecurity in order to minimize cyber-threats which may adversely affect the service delivery for both the public and private sector. Ordinarily the purpose of designing and conducting training in the workplace to drive change with a view to increase effectiveness and obtain efficiency

gain. It is in this regard that training and assisting all stakeholders to safeguard the network system is regarded as an act of social engineering which provides positive social change to the society.

Implications for Theory

The qualitative case study methodological design and approach had a positive facilitative implication to the research process. Phenomenological tradition for research approach resonated well with the study, it enabled the sampled participants to provide evidential and experiential insights on cybersecurity practices as a social phenomenon but also as evolutionary technological issue influencing the Fourth Industrial Revolution (4IR).

Pursuing phenomenological approach in a qualitative case study made available data significant to the problem through the participants' perception and lived experiences. Hence the phenomenology approach had a positive implication to increased access to information-rich cases drawn by utilizing the purposeful criterion sampling strategy.

The theoretical implication included application of the Systems Thinking theoretical construct as a lens for the interpretation of the findings in Chapter 5. The implication of utilizing Systems Thinking theoretical framework is that it provided a medium through which analysis of cybersecurity parameters and dimensions could be examined in line with the purpose of the study. The significant implication is the empirical evidence presented in the findings of the study which is a representation of the contribution to the body of knowledge which also provides data which can inform future studies on cybersecurity.

Conclusions

Cybersecurity is a new domain that is yet to be fully regularized through integration into relevant policies. The literature review in Chapter 2 painted a bleak picture on the state of affairs pertaining to the national policies on cybersecurity. Countries, particularly in the developing world are still developing national policies on cybersecurity. geared towards protection of the digital assets and safeguarding the cyber space. Meanwhile the literature cogently postulated that the upsurge of cyber-attacks and exfiltration of digital data has seen exponential increase at detrimental level, thus creating a precarious cybersecurity governance vicissitude exacerbated by the total dependency of private and public sectors on modern ICTs such as computer mediated communication, IoT, AI and constituent devices (Kazemi et al., 2012).

Sufficient affirmation and recognition that cybersecurity governance is an exorbitant enterprise was well established in the preceding discussion. Employing Systems Thinking theoretical construct, it was possible to examine and illustrate to some extent the complex interconnections emanating from extensive proliferation of Industry 4.0 (4IR) and IoT. Inadvertently, cyber-attack surface area and cyber-threat landscape expand as a result of additional infrastructure and devices in the network thus predisposing cyber space to expanded vulnerability and risk in terms of frequency and severity of cyber-attack events. Pursuant to these plethora dynamics embedded within cyber space ecosystem, the cost to adequately address potential subversion of the cyber space systems would be extremely exorbitant. Sufficient evidential data reinforcing conundrums for government to attain optimal budgeting for cybersecurity was collected

and analyzed. The findings affirmed the problem statement of this study which assumed that the cost of cybersecurity operations is very high creating difficulties for government to achieve required budget allocation. Inference can thus be made that the findings of this study made a considerable contribution to the body of knowledge to bridge the gap that existed in the literature, theory, and practice.

The findings of this study illustratively validated the fact that application of Systems Thinking theoretical construct found resonance with the process of analysis and examination of cyber space character of digital dimensions, elements and interconnected constituents thereof. Application of the Systems Thinking theoretical lens enabled robust and scrupulous examination of the phenomenon of concern while expanding perspective on the conceptual frameworks while incorporating perspectives on interrelationships of constituent elements which have an impact on cybersecurity. For instance, through applying Systemic Thinking approach, it was possible to discover the arbitrary influence of international markets on the cost of cybersecurity commodities and devices for building infrastructure for cyber networks and digital systems.

Chief among the key contributions of the study, was that it provided strategic information and strategies which organizations can apply to mitigate and circumvent the impact of cyber-threat events such as Denial-of-Service cyber-attach to strengthen the cybersecurity. The experts in cybersecurity in government and private sector with responsibility to protect their organizations from cyber incidents can derive lessons from the findings of the study. Subsequently, the hope is for the cybersecurity industry to find the strategic information contained in the findings of this study useful and applicable to

service delivery, accessibility to secure, and efficient cyber network services to support daily operations for respective organizations.

Stemming from RQ2, one of the key concerns of the study was to investigate the challenges which inhibit organizations to achieve optimal budget allotment for cybersecurity. The literature showed that studies on financing and budgeting for cybersecurity are still evolving. Notwithstanding, a financial instrument, the Gordon-loeb model which is utilized by experts to estimate required budget for cybersecurity is among key finding for this study. The financial model provides a functional solution from which experts and practitioners can draw inspiration to further improve planning and budgeting for cybersecurity.

References

Andreasson, Kim, ed. Cybersecurity: Public Sector Threats and Responses. Boca Raton: CRC, 2012. Print.

Anfara, V. A., Jr. (2008). Theoretical frameworks. In L. M. Given (Ed.), *The SAGE encyclopedia of qualitative research methods* (pp. 870–874). Thousand Oaks, CA: Sage

Armenia, S., Fanco, E. F., Nonino, F., Spagnoli, E., and Medaglia, C. M. (2019). Towards the definition of a dynamic and systemic assessment for cybersecurity risks. *Systems Research and Behavioral Sciences, 26*, 404–423. https://doi.org/10.1002/sres.2556

Arnold, R. D., & Wade, J. P. (2015). *A definition of systems thinking: A systems approach*. Elsevier B.V.

Asllani, A., White, C. S., & Ettkin, L. (2013). Viewing cybersecurity as a public good: The role of governments, businesses, and individuals. *Journal of Legal, Ethical and Regulatory Issues, 16*(1), 17–14.

Babbie, E., & Mouton, M. (2008). *The practice of social research* (8th ed.).

Baxter, P., & Jack, S. (2008). Qualitative case study methodology: Study design and implementation for novice researchers. *Qualitative Report, 13*(4), 544–559. DOI: 10.4236/jss.2021.95020

Bell, G. A., Cooper, M. A., & Qureshi, S. (2003). *The Holon framework and software process improvement: A radiotherapy project case study*. John Wiley & Sons https://doi.org/10.1002/spip.155

Ben-Asher, N., & Gonzalez, C. (2015). Effects of cyber security knowledge on attack detection. *Computers in Human Behavior*.48, 51-61 https://doi.org/10.1016/j.chb.2015.01.039

Bengtsson, M. (2016). How to plan and perform a qualitative study using content analysis. *Journal of Nursing Plus Open*, *2*(2016), 8–14. https://doi.org/10.1016/j.npls.2016.01.001

Boyce, M. W., Duma, K. M., Hettinger, L. J., Malone, T. B., Wilson, D. P., & Lockett-Reynolds, J. (2011). Human performance in cybersecurity: A research agenda. *Precedia Manufacturing* 3(2), 5301-5307 https://doi.org/10.1177/1071181311551233

Burkholder, G. J., Cox, K. A., & Crawford, L. M. (2016). *The scholar-practitioner's guide to research design*. Laureate Publishing.

Cabrera, D., Cabrera, L., and Powers, E. (2015). A unifying theory of systems thinking with psychosocial applications. *Systems Research and Behavioural Sciences*. 32 (5), 534 – 545 . https://doi.org/10.1002/sres.2351

Caldwell, R. (2011). Leadership and learning: A critical reexamination of Senge's learning organization. *Systemic Practice and Action Research*, *25*, 39–55. https://doi.org/10.1007/s11213-011-9201-0

Caplan, N. (2013). Cyber war: The challenge to national security. *Global Security Studies*, *4*(1), 93–115. https://www.jstor.org/stable/26270542

Carr, J. (2013). The misunderstood acronym: Why cyber weapons aren't WMD. *Bulletin of the Atomic Scientists*, *69*(5), 32–37

.https://doi.org/10.1177/0096340213501373

Carr, M., & Lesniewska, F. (2020). Internet of things, cybersecurity governing wicket problems: Learning from climate change governance. *International Relations*, *34*(3), 391–412. https://doi.org/10.1177/0047117820948247

Cavelty, M.D (2018). Cybersecurity research meets science and technology studies. *Politics and Governance*, (6) 22–30. DOI: 10.17645/pag.v6i2.1385

Chaudhuri, S., & Ghosh, R. (2012). Reverse mentoring: A social exchange tool for keeping the Boomers engaged and Millennials committed. *Human Resource Development Review*, *11*(1), 55–76. doi.org/10.1177/1534484311417

Celano, L. (2014). 6 Methods of data collection and analysis. *Monitoring, Evaluation, Accountability and Learning (MEAL)*, 1–30. https://doi.org/10.1111/j.1096-3642.1949.tb00873.x

Celik, S., & Gurkaynak, M. (2019). The new front in global insecurity: Cyberspace. *International Journal of Social Enquiry*. 12(2), 545 - 566 https://doi.org/10.37093/ijsi.659014

Checkland, P. (1981), Systems Thinking, Systems Practice, John Wiley, Chichester.

Checkland, P. (1999). Systems Thinking, Systems Practice, Soft Systems Methodology: A 30 year Retrospective. John Wiley, Chichester.

Chermack, T. (2011). Scenario Planning in Organizations. How to create, use and assess scenarios. Carlifonia: Berrett-Koehler Publishers, Inc.

Cho, Y., & Qu, G. (2013). Detection and Prevention of Selective Forwarding-Based Denial-of-Service Attacks on WSNs. Maryland, USA. *International Journal of*

Distributed Sensor Networks. Hindawi Publishing Cooperation. https://DOI:org/10.1155/2013/205920

Chatfield, A.T., and Reddick, C.G. (2018). A Framework for Internet for Internet of Things-enabled smart government: A Case of IoT cybersecurity policies and use cases in U.S. federal government. *Government Information Quarterly*. Wollongong, Australia, Elsevier Inc. https://DOI.org/10. 1016/jiq2016.09.007

Churchman, C.W. (1987). Systems profile: discoveries in exploration into systems thinking. Systems Research 4(22): 139-14 DOI: 10.13140/RG.2.2.17773.51681 .

Cooper, T. L. (2012). The responsible administrator: An approach to ethics for the administrative role (6th ed.). New York, NY: Jossey-Bass.

Craig, J. (2018). Cybersecurity Research—Essential to a Successful Digital Future. Australia: Elsevier B.V. DOI.org/10.1016/j.eng.2018.02.006

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining cybersecurity. *Technology Innovation Management Review, 4*(10), 13-21. doi:10.22215/timreview/835

Creswell, J.W. (2013). Qualitative Inquiry and Research Design: Choosing among five approaches (3rd Ed). Thousand Oaks CA: SAGE Publications

Dooley, L.M. (2002). Case Study Research and Theory Building. *Advances in Developing Human Resources.* https://DOI: 10.1177/1523422302043007

Drack, M., & Schwarz, G. (2010). Recent developments in general system theory. *Systems Research & Behavioral Science, 27(6), 601–610*. doi:10.1002/sres.1013

Dor, D. and Elovici, Y. (2016). A model of the information security investment decision-

making process. *Israel*: Elsevier B.V. https://DOI.org/10.1016/j.cose.2016.09.006

Deloitte, NASCIO Cybersecurity Study (2014) http://www.nascio.org/publications/documents

Edwards-Jones, A. (2014). Qualitative data analysis with NVIVO. *Journal of Education for Teaching, 40*(2), 193–195. doi:10.1080/02607476.2013.866724Elo, S., Kaariainen, M., Kanste, O., Polkki, T., Utriainen, K., & Kyngas, H. (2014). Qualitative content analysis: A focus on trustworthiness. *SAGE Open, 4*(1), 1–10. https://DOI:10.1177/2158244014522633

Eling, M., Schnell, W. (2016). What do we know about cyber risk and cyber risk insurance? The Journal of Risk Finance, Vol.17 No.5. Switzerland: Emerald Group. https://DOI.10.1108/JRF-09-2016-0122

Eriksson, K., & McConnell, A. (2011). Contingency planning for crisis management: Recipe for success or political fantasy? *Policy and Society*, 30(2), 89-99.

Eriksson, D.M. (2003). Identification of Normative Soruces for Systems Thinking: An Inquiry into Religious Ground-Motives for Systems Thinking Paradigms. *Systems Research and Behavioral Science.* Stockholm: John Wiley & Sons. https://DOI: 10.1002/sres.579

Fielder, A., Konig, S. Panaousis, D., Schauer, S., & Rass, S. (2018). Risk Assessment Uncertainties in Cybersecurity Investments. MDPI: *The Games. Vol (9) 34.* https://DOI:10.3390/g9020034

Fielder, A., Panaousis, D., Malacaria, P., Hankin, C., & Smeraldi, F. (2016). Decision support approaches for cyber security investment. UK: Elsevier B.V.

https://DOI.org/10.1016/j.dss.2016.02.012

Fischer, T. & Richards, L.D. (2017). From Goal-Oriented to Constraint-Oriented Design. *The Cybernetic Intersection of Design Theoryand Systems Theory. Leonardo, Volume 50, Number 1, 2017, pp. 36-41 (Article).* The MIT Press. https://DOI: 10.1162/LEON_a_00862

Flood, R.L (2010). "The Relationship of 'systems thinking' to Action Research", *Systemic Practice and Action Research, Vol 23, pp. 263-84*

Forero, R., Nahidi, S., De Costa, J., Mohsin, M., Fitzgerald, G., Gibson, N., & Aboagye-Sarfo, P. (2018). Application of four-dimension criteria to assess rigour of qualitative research in emergency medicine. *BMC Health Services Research, 18*(1), 120. https://doi.org/10.1186/s12913-018-2915-2

Freedom House. (2017). Freedom on the Net, 2017: *Manipulating Social Media to Undermine to Undermine Democracy*. Washington, DC: Freedom House.

Garavito-Bermúdez, D., Lundholm, C., and Crona, B (2016). *Environmental Education Research, v22 n1 p89-110 2016. (EJ1090164),* Stockolm, Sweden, Routledge. https://DOI. Org/10.1080/13504622.2014.936307

Gelo, O., Braakmann, D., & Benetka, G. (2008). Quantitative and qualitative research: Beyond the debate. Integrative Psychological & Behavioral Science, 42(3), 266–290. doi:10.1007/s12124-008-9078-3

Gibbs, G. R., Friese, S., & Mangabeira, W. C. (2002). The use of new technology in qualitative research. Qualitative Social Research, 3(2), 8. Retrieved fromhttp://www.qualitative research.net/index.php/fqs/article/view/847/1840

Glenn, J., Kamara, K., Umar, Z. A., Chahine, T., Daulaire, N., and Bossert, T. (2020). Applied systems thinking: a viable approach to identify leverage points for accelerating progress towards ending neglected tropical diseases. *Health Research Policy and Systems.* USA: Open Access. https://DOI.org/10.1186/s12961-020-00570-4

Golembiewski, R.T. and Rabin, J. (1997). Public Budgeting and Finance (4th Ed.). New York: Marcel Dekker Inc.

Goncharov, Max. 2012. "Russian Underground 101." Trend Micro Incorporated. Assessed June 27, 2019. https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-paper/wp-russian-underground-101.pdf.

Grant, C., & Osanloo, A. (2014). Understanding, selecting, and integrating a theoretical framework in dissertation research: Creating the blueprint for your "house." Administrative Issues Journal: Connecting Education, Practice, and Research, 4(2), 12–26.

Grossoehme, D. H. (2014). Overview of qualitative research. *Journal of Health Care Chaplaincy*, *20*(3), 109–122. https://DOI10.1080/08854726.2014.925660

Greene, M. (2014). On the inside looking in: Methodological insights and challenges in conducting qualitative insider research. *The Qualitative Report, 19*(15), 1-13.

Guerard, G., Amor, S.B., & Buti, A. (2012). A complex system approach for smart grid and modelling. Versailles, France: ResearchGate. https://DOI. 10.3233/978-1-61499-105-2-788

Islam, S., Farh, N., & Stafford, T.F. (2018). Factors associated with security/cybersecurity audit by internal audit function. Managerial Auditing Journal. Vol. 33 No. 4, 2018, pp. 377-409. USA: Emerald Publishing Ltd. https://DOI: 10.1108/MAJ-07-2017-1595

Jackson, M.C. (2003), Systems Thinking – Creative Holism for Managers, Wiley, Chichester.

Jonas, A. and Burrell, J. (2019). Friction, Snake oil, and weird countries: Cybersecurity systems could deepen global inequality through regional blocking. Big Data & Society. USA, CA: SAGE. https://DOI. 10. 1177/2053951719835238

Juniper Research (2015), "Cybercrime will cost business over $2trillion by 2019", available at: www.juniperresearch.com/press/press-release/cybercrime-cost - business-over-2trillion

Lagazio, M., Sherif, N., & Cushman, M. (2014). A multi-level approach to understanding the impact of cyber crime on the financial sector. *Computers & Security*, *45*(2014), 58–74. doi:10.1016/j.cose.2014.05.006

Lane, D.C. (2000). Should System Dynamics be Described as a 'Hard' or 'Deterministic' Systems Approach. *Systems Research and Behavioral Science,17, 3-22*. UK. John Wiley & Sons

Leedy, P.D. & Ormrod, J.E. (2015). Practical Research Planning and Design. (11th Ed.). New York, NY:Pearson

Lees, M.J., Crawford, M., Jansen C. (2018). Towards Industrial Cybersecurity Resilience of Multinational Corporations. Australia: Elsevier B.V.

https://DOI.10.1016/j.ifacol.2018.11.201

Lia, L., Hea, W., Xua, L., Asha, I., Anwarb, M., and Yuanb, X. (2018). Investigating the Impact of Cybersecurity Policy Awareness on Employee's Cybersecurity Behaviour. *International Journal of Information Management.* USA:Elsevier. https://DOI.org/10.1016/j.ijinformgt.2018.10.017

Lincoln, Y.S., & Guba, E.G. (1985). Naturalistic inquiry. Sage. https://doi. org/10.1016/0147-1767(85)90062-8

Lodico, M. G., Spaulding, D. T., & Voegtle, K. H. (2010). Methods in educational research: From theory to practice (Laureate Education, Inc., custom ed.). SanFrancisco, CA: John Wiley & Sons.

Lutscher, M.P., Weidmann, N.B., Roberts, M.E., Jonker, M., King, A., and Dainotti, A. (2019). At Home and Abroad: The Use of Dinial-of-service Attacks during Elections and Nondemocratic Regimes. Journal of Conflict Resolution, Vol 64(2-3) 373-401. Konstanz, Germany, Sage. https://DOI: 10.1177/0022002719861676

Kazemi, M., Khajouei, H., & Nasrabadi, H. (2012). Evaluation of information security management system success factors: Case study of municipal organization. African Journal of Business Management, 6(14), 4982-4989. doi:10.5897/AJBM11.2323

Khan, S.N. (2014). Qualitative research method: Grounded Theory. *International Journal of Business & Management, 9(11), 224-324.* https://DOI. 10.5539.ijbm.v9nll

Kensler, L.A.W., Reames, E., Murray, J., & Patrick, L. (2011). Systems Thinking Tools for Improving Evidence-based Practice: A Cross-Case Analysis of Two High

School Leadership Teams. USA, North Carolina Press. https://DOI.org/10.1353/hsj.2012.0002

Kissel, K. (Ed.). (2013). Glossary of key information security terms (NIST Interagency or Internal Report 7298, Revision 2). Gaithersburg, MD: National Institute of Standards and Technology.doi:10.6028/NIST.IR.7298r2

Kissoon, K. (2020). Optimum spending on cyberscuirty measures. UK, Oxfordshire, Emerald Publishers. DOI: 10.1108/TG-11-2019-0112.

Kogetsidis, H. (2011). Systems Approaches for Organizational Analysis. *International Journal for Organizational Analysis, Vol. 19, No. 4, pp. 276-287 Nicosia, Cyprus, Emerald Group Publishing.* https://DOI. 10.1108/19348831111173414

Korstjens, I., & Moser, A. (2018). Series: Practical guidance to qualitative research. Part 4: Trustworthiness and publishing. *European Journal of General Practice, 24*(1), 120-124. https://doi.org/10.1080/13814788.2017.1375092

Kumar, R. (2014). Research Methodology. A step-by-step guide for beginners. Fourth Edition. Sage: London

Margulies, P. (2017). Global Cybersecurity, Surveillance, and Privacy: The Obama Administration's Conflicted Legacy. *Indiana Journal of Global Legal Studies, Volume 24, Issue 2, 2017, pp. 459-495.* Indiana: Project Muse

McMahona, M. & Patton, W. (2018). Systemic thinking in career development theory: contributions of the Systems Theory Framework. B*ritish journal of guidance & counselling, Vol.* 46, No. 2, 229–240 https://DOI.org/10.1080/03069885.2018.1428941

McFee (2014), “Net losses: estimating the global cost of cybercrime”, available at www.mcafee.com/mx/resources/reports/rp-economic-impact-cybercrime2.pdf (accessed 16 March 2015).

Mingers, J. & White, L (2010). A review of the recent contribution of systems thinking to operational research and management science. *European Journal of Operational Research 207 (2010) 1147–1161*. UK. Elsevier, https://DOI:10.1016/j.ejor.2009.12.019

Meadows, D. (2008). Thinking in Systems – A Primer, Chelsea Green Publishing Company, White River Junction, VT (edited by Diana Wright).

Mesjasz, C. (2006). Complex systems studies and the concepts of security. *Complex systems studies*. Vol.35 No. 3/4, pp. 471-488. Cracow, Poland: Emerald Group Publishing. https://DOI. 10. 1108/08634920610653755

Mikesell, J. L. (2014). Fiscal administration: Analysis and applications for the public sector (9th ed.). Boston, MA: Wadsworth.

Mulej, M., et al (2004). How to restore Bertalanffian systems thinking. NY.Emerald Group Publishing Limited. https://DOI: 10.1108/03684920410514346

Mueller, M. (2017). Is Cybersecurity eating Internet governance? Causes and consequences of alternative framings. *Digital Policy, Regulation and Governance.* Vol. 19 No. 6 2017, pp. 415-428, Emerald Publishing Limited. https://DOI 10.1108/DPRG-05-2017-0025

National Association of Insurance Commissioners (NAIC) (2013), “Cyber risk”, available at: www.naic.org/cipr_topics/topic_cyber_risk.htm (accessed 4 May

2016).

Njilla, L. et al (2017). Cyber Security Resource Allocation: A Markov Decision Process Approach. International Symposium on High Assurance Systems Engineering. https://DOI. 10.1109? HASE. 2017.30

Ogilvy, J.A. (2011). Facing The Fold. Essays on Scenario Planning. UK: Triarchy Press

Ogut, H. et al (2011). Cyber Security Risk Management: Public Policy Implications of Correlated Risk, Imperfect Ability to Prove Loss, and Observability of Self-Protection. *Society for Risk Analysis*. Vol. 31, No3. 3. https://DOI: 10.1111/j.1539-6924.2010.01478.x

O'Sullivan, E., Rassel, G. R., Berner, M., & Taliaferro, J. D. (2017). Research methods for public administrators (6th ed.). New York, NY: Routledge.

Pandey, S. and Singh, R. K. (2019). Cyber security risks in globalized supply chains: conceptual framework. *Journal of Global Operations and Strategic Sourcing.* India: Emerald Publishing. https://DOI:10.1108/JGOSS-06-2019-0042

Pătrașcu, P. (2018). The 14th International Scientific Conference: *eLearning and Software for Education Bucharest.* Romania, "Carol I" National Defence University. https://DOI:10.12753/2066-026X-18-222

Patton, M. Q. (2015). *Qualitative research & evaluation methods: Integrating theory and practice* (4th ed.). Thousand Oaks, CA: SAGE.

Paul, J.A., and Wang, X. (2019). Socially optimal IT investment for cybersecurity. *Decision Support System*. USA, Georgia. Elsavier B.V. https://DOl.org/10.1016/j.dss.2019.05.009

Plack, M.M., Goldman, E.F., Cott, A.R., Pintz, C., Herrmann, D., Kline, K., Thompson, T., and Brundage, S.B. (2018). Systems Thinking and Systems-Based Practice Across the Health Professions: An Inquiry Into Definitions, Teaching Practices, and Assessment

Pour, M.S., Bou-Harb, E., Varma, K., Nesheko, N., Pados, D.A., Choo, K.R. (2019). Comprehending the IoT cyber threat landscape: A data dimensionality reduction technique to infer and characterize Internet-scale IoT probing campaigns. USA: Elsevier B.V. https://DOI.10.1016/j.diin.2019.01.014

Quinn, R.E. (2011). Becoming A Master Manager. A competing Values Approach. Fith Ed. USA: Wiley & Sons Inc.

Ravitch, S. M., & Carl, N. M. (2016). Qualitative research: Bridging the conceptual, theoretical, and methodological. Thousand Oaks, CA: Sage Publications.

Raban, Y., Hauptman, A. (2018). Foresight of cyber security threat drivers and affecting technologies. Foresight. Tel Aviv. Emerald Publishing Ltd. https://DOI.10.1108/FS-02-2018-0020

Reybold, R.E., Lammert, J.D., & Stribling, S.M. (2013). Participant selection as a conscious research method: Thinking forward and the deliberation of "emergent" findings. *Qualitative research, 13 (6), 699-716.* https://DOI. 10.1177/1468794112465624

Ross D. Arnold, R.D., & Wade, J.P. (2015). A Definition of Systems Thinking: A Systems Approach *Procedia Computer Science* 44 (2015) 669 – 678. USA, NJ: Elsevier B.V. https://DOI: 10.1016/j.procs. 2015.03.050

Rubin J.H., & Rubin I.S. (2012). Qualitative Interviewing. The Art Hearing Data. Sage Publications: London. Third Edition

Rudasill, L. and Moyer, F. (2004). Cyber-security, Cyber-attack, and development of government response: the librarian view's view. New library world, Vol 105, pp. 248-255. Illinois, USA: Emerald Group Publishing. https://DOI. 10.1108/03074804100550995

Rudestam, K. E., & Newton, R. R. (2015). Surviving your dissertation: A comprehensive guide to content and process (4th ed.). Thousand Oaks, CA: Sage. ISBN: 978-1-4522-6097-6

Ryan, C.W., & Tomlin, J.H. (2010). Infusing systems thinking into career counselling. *Journal of Employment Counselling, 47, 79-85*

Saldaña, J. (2016). *The coding manual for qualitative researchers* (3rd ed). Thousand Oaks, CA: SAGE.

Saghar, K., Farid, H., Kandall, D., Bouridane, A. (2016). Formal Specifications of Dial of Service Attacks in Wireless Sensor Networks. Kingdom of Saudi Arabia, Islamabad

Sanfilippo, D. & Valle, A. (2013). Feedback Systems: An Analytical Framework. *Computer Music Journal, Volume 37, Number 2, Summer 2013, pp. 12-27.* USA:The MIT Press. https://org/DOI:10.1162/COMJ a 00176

Sargeant, J. (2012). Qualitative research part II: Participants, analysis, and quality 205 assurance. *Journal of Graduate Medical Education*, *4*(1), 1–3. https://doi.org/10.4300/JGME-D-11-00307.1

Sauter, M. (2014). The Coming Swarm: DDOS, Actions, Hacktivism, Civil Disobedience on the Internet on the Internet. New York: Bloomsbury Publishing

Schneider, F., B. (2018).Viewpoint. Impediments with Policy Interventions to Foster Cybersecurity. *A call for discussion of governmental investment and intervention in support of cybersecurity.* Communications of the ACM. 61 (3). https://DOI.org/101145/3180493

Shaked, H., & Schechter, C. (2013). Seeing Wholes: The concept of systems thinking and its implementation in school leadership. *Educational Management Administration & Leadership*. Israel: Springer Science+Business. https://DOI.org/10. 1007/s11159-013-9387-8

Shaked, H., & Schechter, C. (2017). Systems thinking among school middle leaders. *Educational Management Administration & Leadership*, Vol, 45(4) 699-718. Israel: Sage. https://DOI.org/10.1177/1741143215617949

Senge, P. (1990). *The Fifth Discipline, the Art and Practice of the Learning Organization*. New York, NY: Doubleday/Currency.

Siponen, M., Mahmood, A., and Pahnila, S. (2013). Employees' adherence to information security policies: An exploratory field study. *Information & Management 51 (2014) 217–224*. Finland, Jyvaskyla:Elsevier B.V. https://DOI.org/ 10.1016/j.im.2013.08.006

Smith, B. A., & Hesse-Biber, S. (1996). Users' experiences with qualitative data analysis software: Neither Frankenstein's monster nor muse. *Social Science Computer Review, 14*(4), 423-432. http://doi:10.1177/089443939601400404

Srinidhi, B., et al (2015). Allocation of Resources to cyber-security: The effect of misalignment of interest between managers and investors. NY: https://DOI:10.1016/j.ssd.2015.04.011

Srinivas, J., Das, A.K., and Kumar, N. (2018). Government Regulations in Cybersecurity: Framework, standards and recommendations. *Future Generations Computer Systems.* India,Hydradad, Elsevier B.V. DOI.org.10.1016/j.future.2018.09.063

Sutton, J., & Austin, Z. (2015). Qualitative research: Data collection, analysis, and management. *CJHP, 68*(3), 226-231. https://doi.org/10.4212/cjhp.v68i3.1456

Sweeney, L. B., & Sterman, J. D. (2000). Bathtub dynamics: initial results of a systems thinking inventory. *System Dynamics Review*, *16*(4), 249–286. https://DOI:10.1002/sdr.198

Swiatkowska, J. (2017). Global Governance. Cybersecurity Statecraft in Europe: A Case Study of Poland

Swiss Re (2014), "Working together with clients to find cyber risk solutions", available at: www.swissre.com/reinsurance/insurers/casualty/smarter_together/working_smarter_together_for_cyberrisk_solutions_in_EME.html (accessed 18 March 2015).

Taewoo, N. (2019). Understanding the gap between perceived threats to and preparedness for cybersecurity. South Korea:Seoul. Sevier Ltd. https://IDO. Org/10.1016/j.techsoc.2010.03.005

Quigley, K., Calvin Burns, C. and Stallard, K (2015). Cyber Gurus': A rhetorical analysis of the language of cybersecurity specialists and the implications for security

policy and critical infrastructure protection. *Government Information Quarterly 32 (2015) 108–117.* Elsevier, *Glasgow, UK G1 1XU.* http://dx.doi.org/10.1016/j.giq.2015.02.001

UNIDIR Report, (2017): United Nations Institute for Disarmament Research

Wang, H., Lau, N., Gerdes, R.M. (2018). Examining Cybersecurity of Cyberphysical Systems for Critical Infrastructures Through Work Domain Analysis. *Human Factors, Vol. 60, No. 5, pp. 699-718.* USA,Virginia: Human Factors & Ergonomics Society

Williams, C. (2014). Security in the cyber supply chain: Is it achievable in a complex, interconnected world? *Technovation*, *34*(7), 382–384.

Wilner, A.S. (2018). Cybersecurity and its discontents: Artificial intelligence, the Internet of Things, and digital misinformation. *International Journal* Vol. 73(2) 308–316. Canada, Ottawa: Sage. https://DOI: 10.1177/0020702018782496

Wolgemuth, J.R., Erdil-Moody, Z., Opsal, T., Cross, J.E., Kaanta, T., Dickmann, E.M., & Colomer, S. (2015). Participants experience of the qualitative interview: Considering the importance of the research paradigms. *Qualitative Research, 15(3), 351-372.* https://DOI. 10.1177/1468794114524222

Woo, T. H. (2013). Systems Thinking Safety Analysis: Nuclear Security Assessment of Physical Protection System in Nuclear Power Plants. Seoul: Hindawi Publishing Corporation. https://DOI.org/10.1155/2013/473687

World Economic Forum (2015), Global Risks Report 2015, 10th ed. Available at: www3.weforum.org/docs/WEF_Global_Risks_2015_Report15.pdf (accessed 9

October 2015).

Yawson, R. M. (2012). Systems Theory and Thinking as a foundational Theory in Human Resources Development – A Myth or Reality? Human Resources Development Review. 13 (1) 53-85. USA. MN. Sage. https://DOI. 10.1177/1534484312461634

Yin, R.K. (2003). Research Design and Methods. 3rd Edition. USA:Sage Publications, Inc

Vance, A., Siponen, M., and Pahnila, S. (2012). Motivating IS security compliance: Insights of Habit and Protection Motivation Theory. *Information & Management, pp.190-198.* USA, Elsevier B.V. https://DOI. Org/ 10. 1016/j.im.2012.04.002

Von Bertalanffy, L. (1972). The history and status of general systems theory. *Academy of Management Journal,* 15(4), 407–426. https://DOI: 10.2307/255139

Vitel, P., and Bliddal, P. (2015). French Cyber Security and Defence: An Overview. *Information & Security: An International Journal*. (32). http://dx.doi.org/10.11610/isij.3209

Zexian, Y. & Xuhui, Y. (2010). A Revolution in the Field of Systems Thinking – A Review of Checkland's System Thinking. *Systems Research and Behavioral Sciences.* China: John Wiley & Sons. https://DOI: 10.1002/sren.102.

Zoto, E., Kianpour, M., Kowalski, S.J., and Lopez-Rojas, E.A. (2019). A Socio-Technical Systems Approach to Design and Support Systems Thinking in Cybersecurity and Risk Management Education. *Complex Systems Informatics and Modeling Quarterly*. Gjøvik, Norway: RTU Press https://DOI.org/10.7250/csimq.2019-18.04

Appendix A: Interview Protocol

Cybersecurity Fiscal Statecraft Conundrums in South Africa

Date: ----------
Location of interview: ----------
Face-to-face or virtual/online ----------
Interviewer: ----------
Recording mechanism: ----------
Interviewee: The identity of the participant will be confidential.
Two or more years of experience related to cybersecurity operations and policy implementation

Project Purpose

The purpose of this qualitative case study was to explore and describe cyber-threats conditions caused by the Denial-of-Service (DoS) cyber-attack which compromises cyber resilience of computerized systems by creating network instability, interruption and vulnerability to the digital data and information assets. Drawing from the case of the South African, Cyber Security Operations and National Cybersecurity Hub, a subunit charged with the responsibility for national cybersecurity coordination, the study explored the phenomenon of DoS and budgetary implications.

Your availability for the interview is highly appreciated. In this regard your insight and genuine responses to the interview questions will be critical to assist full exploration of the research problem. It is estimated that this interview should last about 40 to 45minutes. The questions are outlined below, however there might be follow-on questions as deemed necessary. The interview will be audio recorded, and I will also be taking notes throughout the interview so that I may accurately document your important insights.

As appropriate, you will receive the interview transcript for your quick review and approval. Please feel free to state any questions or concerns before we begin? Then with your permission, we will begin the interview.

RQ1. . What are the various Denial-of-service cyber threat events and response coordinated by the National Cybersecurity Hub unit in South African national

#	Question	Notes
1.	How can you describe typical activities of Cybersecurity operational activities in your organization?	
2.	How do the services provided by Department of Communication and Digital Technology through the National Cybersecurity Hub assist government and private sector to strengthen cybersecurity?	
3.	What are the strategies of National Cybersecurity Hub to respond to cyber-threats?	
4.	*Denial-of-service cyber-threat* manifest in two forms, those that cause flooding and crashing of network services. What type of cyber-threat measures does the National Cybersecurity Hub unit have to respond to attacks of various *Denial-of-service?*	
5.	What protective measures has the Department of Communication and Digital Technology put in place to mitigate impact of network flooding or crashing caused by *Denial-of-service?*	

RQ2. How do the rapid emergence of Denial-of-service cyber-threats conditions cause challenges for optimal budgeting and financing for cybersecurity operations managed by the Department of Communication and Digital Technology in South Africa?

#	Question	Notes
1.	What are your views concerning the importance of cybersecurity strategies/measures to protect computer network systems to ensure uninterrupted Government operations?	
2.	What are cybersecurity budgetary consideration Cybersecurity Hub have to prevent, mitigate and protect systems from cyber-threat incident when they occur?	
3.	How difficult is it to prevent cyber-threats such as *Denial-of-service*	
4.	What type of cyber-threat conditions make it difficult to mitigate *Denial-of-service*	
5	How difficult is to mobilize financial resources to recover interrupted computer network	
6.	What are your views about the costs related to prevention of *Denial-of-service* and implications to operations?	
6.	What are your views about the costs implications related to mitigation of *Denial-of-service?*	
7.	What are your views about the costs implications related to recovery operation after the *Denial-of-service a*ttack on government computer network system?	

Thank you for participating and sharing your insight in this important research.