An Assessment of Cyber Attacks Preparedness Strategy for Public and Private Sectors in Zambia

By

Kingstone Ali Mwila

A Dissertation Submitted to the University of Zambia in Partial Fulfillment of the Requirements for the Degree of Master of Engineering in Information and Communication Technology Security

THE UNIVERSITY OF ZAMBIA

LUSAKA

2020

Copyright Declaration

Declaration

I, Kingstone Ali Mwila, do hereby declare that the content of this document is my own and all other works by other people have been duly referenced, and that this work has not been previously presented to another university for the same purpose.

…….. ……

Kingstone Ali Mwila Date

Certificate of Approval

This dissertation of Kingstone Ali Mwila has been approved as fulfilling the requirement for the award of Master of Engineering in Information and Communication Technology Security by The University of Zambia.

Examiner 1	Signature	Date
Examiner 2	Signature	Date
Examiner 3	Signature	Date
Chairperson Board of Examiner	Signature	Date
Supervisor	Signature	Date

Abstract

Cyber-attacks are the use of network and computer-based attacks to critical infrastructures and services that compromises the confidentiality, integrity, and availability to further the persona, political, economic, and military goals of the attackers.

The nature and forms of cyber-attacks includes infrastructure sabotage, financial fraud, denial-of-service, data modification or deletion, theft of trade secrets and propaganda. Cyber-attacks can cause harm directly or indirectly to connected systems using botnet command control operators, organised criminal groups, hackers, insiders, and state-sponsored hackers using distributed denial-of-service attacks, Malware attacks, viruses and many more.

This paper reports the results from the private and public sectors in Zambia that comprises the Health; Consumer Products; and Services; Manufacturing, Mining, Construction and Engineering; public sectors; Energy (Power, utility); ICT and Telecoms; and Banking and Finance.

The study aimed at identifying whether Zambia utilises cyber-attacks preparedness strategy resources in an optimal manner to protect various assets.

The study shows that Zambian private and public sectors have low level compliance and have experienced cyber-attacks which indicated only 10% could recover from the attacks within a day and the rest it will require days, weeks and months to recover. That calls for considered efforts in developing measures for mitigation of these challenges in order to ensure national cyber-attacks preparedness defence strategy.

The study showed that the majority of organizations have understaffed cybersecurity personnel. The study shows less than 50% of the staff have cybersecurity training and 48.2% have the right skills. The study shows IT personnel manage cybersecurity instead of cybersecurity experts as a resulting weakness the security postures. The study indicated 70% availability of formal policies, documents, rules, and controls aimed at strengthening the security against cyber-attack is likely to yield more results if only the issues covered in the policies are implemented fully. The study shows 63% of the Organisations adopted cybersecurity frameworks or standards but the implementation is not in affect.

However, this is likely to be weakened by the lack of reporting procedures of any suspicious or real cybersecurity breach, and the lack of a cyber-security emergency response team, as revealed

by results of this study. This, therefore, calls for the need to develop a framework, based on the findings of this study that would specifically be tailored with other best frameworks and best practices towards addressing the problems of cybersecurity in Zambia.

Keywords: Cybersecurity, Cyberwarfare, framework, Critical infrastructure and services, cyber-attacks, model, hacker

Dedication

This document is dedicated to my nephew Mwila Kaboneka and I fondly call him my son.

Acknowledgement

I wish to express my thanks to Dr. Charles S. Lubobya for supervising my research. I wish to thank the respondents and the institutions for having provided the much needed data that greatly contributed to the findings of this research.

I am also grateful to Nachinga Ng'ambi, Masialeti, Musonda Kapaya, Mr. Justine Kangwa, Dr. Musonda Simwayi and everyone for their encouragement during my studies.

Table of Contents

List of Figures

List of Tables

List of Acronyms and Abbreviations

AIPAC	American Israel Public Affairs Committee
AT&T	American Telephone and Telegraph
ARPANET	Advanced Research Projects Agency Network
APT	Advanced Persistent Threat
BBC	British Broadcasting Corporation
BCMS	business continuity management systems
BMW	Bavarian Motor Works
CAN	Computer Network Attack
CAPF	Cyber Attacks Preparedness Framework
CERT	Computer Emergency Response Team
CI	Critical Infrastructure
CII	Critical Information Infrastructure
CIA	Central Intelligence Agency
CIRT	Computer Incident Response Team
COBIT	Control Objectives for Information and related Technology
CND	Computer Network Defence
CSF	Cybersecurity Framework
CSOC	Cyber Security Operation Centre
CSIRC	Computer Security Incident Response Capability
CSIRT	Computer Security Incident Response Team
CW	Cyber Warfare
C2	Command and Control

DoS	Denial of Service
DDoS	Distributed Denial of Service
FBI	Federal Bureau of Investigation
HTTP	Hyper Text Transmission Protocol
IEC	International Electrotechnical Commission
ISMS	Information Security Management Systems
ISO	International Standard Organisations and International
ISP	Internet Service Provider
ITU	International Telecommunications Union
ITU-D	International Telecommunications Union Document
PHP	Hypertext Preprocessor
PII	Personally Identifiable Information
PwC	Price Waterhouse Coppers
IoT	Internet of Things
FNDP	Fifth National Development Plan
FW	Firewall
IPS	Intrusion Prevention Systems
IDS	Intrusion Detection Systems
MoD	Ministry of Defense
NATO	North Atlantic Treaty Organization
ICT	Information and Communication Technology
ISO	International Standard Organisation
IEC	International Electrotechnical Commission,

GCA	Global Cybersecurity Agenda
HUC	Honker Union of China
HTML	Hyper Text Markup Language
ICMP	Internet Control Messaging Protocol
ICS	Intercommunications System
IDSes	Intrusion Detection System
IP	Internet Protocol
ISAE	International Standard on Assurance Engagements
IT	Information Technology
ITU	International Telecommunications Union
ITIL	Information Technology Infrastructure Library
KPMG	Klynveld Peat Marwick Goerdeler
MD	Message Digest
MitM	Man-in-the-Middle
NDP	National Development Plan
NSA	National Security Agency
NIPC	National Infrastructure Protection Center
PCI DSS	Payment Card Industrial Data Security Standard
PII	Personally Identifiable Information
R&D	Research and Development
R-SNDP	Revised version the Sixth National Development Plan
UK	United Kingdom
UN	United Nations

SMS	Short Messaging Solution
US	United States
USB	Universal Serial Bus
UPS	Uninterrupted Power Supply
USA	United States of America
SADC	Southern African Development Community
SANS	SysAdmin, Audit, Network, and Security
SOC	Security Operation Centre
SNDP	Sixth National Development Plan
SQL	Structured Query Language
SYN	Synchronisation
NIST	National Institute of Standards and Technology
NOSC	Network Operations and Security Center
PWC	Price Waterhouse Coopers
TCP	Transmission Control Protocol
VB	Visual Basic
VPN	Virtual Private Network
XSS	Cross-site scripting
ZAF	Zambia Air Force
ZICTA	Zambia Information and Communications Technology Authority
ZP	Zambia Police Service
ZNS	Zambia National Service
7NDP	Seventh National Development Plan

CHAPTER ONE

1.0 INTRODUCTION

Cyber-attacks are one of the most devastating threats to the nations. Any connected device is a potential target. Its impact affects critical infrastructures and services [1]. Estonia, Georgia, and Iran are some of the very good examples of cyber-attacks [2], [3]. The most common critical information infrastructures are power plants, telecommunications systems, health systems, banking and financial systems, and others which depend on connectivity [4].

Cyber-attacks preparedness involves the capabilities of proactive and reactive operations. It helps and recommended practice to identify the weapons used to attack the targets [5], [6]. The weapons range from denial of service, malware, ransomware, worms, and others [7]. The weapons used in the attacks only require to achieve the intended goals. In cyber-attack or breach, an attacker can be a professional or a novice. Defensive operations employ defence-in-depth mechanisms and techniques. It may include encryption, data loss prevention techniques, cryptography, firewalls, intrusion detection and prevention, and many others [8]. This can be fully implemented by having the policies and procedures in place. Compliance and implementation of best practices, standards and frameworks may lead to having a sense assurance. In the end the private and public sectors achieve confidentiality, integrity and availability of computer systems and its resources.

Cyber-attacks preparedness involves the development of processes, methodology, standards, techniques, and mechanism that forms a framework to provides a sense of alertness, to plan, to identify, and defend critical cyberspace infrastructures and services. Potential threats will be analysed and forces to be stopped. The strategy includes a credible defence, and ability to for resilient [9]. The study focuses on the immediate approach to explore and outline forms of cyber-attacks capabilities that would possibly threaten networks in the public and private sectors in Zambia and what potential effects they may have. The cyberspace requires coordinated efforts to manage because it is borderless in its nature. The ongoing efforts must be accompanied by cyber-attacks defence capabilities. Therefore, there is need to apply deliberate standards and best practices to achieve security objectives.

The arrangement of the research paper is as follows: background, related works, and the problem of the statement, objectives, research questions, and purpose of the study, methodology, data analysis, discussions, recommendations, and conclusion.

1.1 Background

The Seventh National Development Plan (7NDP), the master plan for development strategy in Zambia, establishes the strategy to deliver development to all Sectors [10]. The National ICT Plan implements access to ICTs. ICTs are key enablers to the growth of the economy [11]. The recent report published by the Zambia Information and Communications Technology (ZICTA) stated that there is an increased number of internet users from 7.9 million to 12 million [12]. The increased access to the internet via broadband reflections the growth of cyberspace with more connected devices, transmitting, processing and storing critical information [13]. The critical infrastructures and services are not limited to electronic payments, internet banking, and mobile banking, online shopping, online medical records, eLearning, online news and many more electronic or online platforms. These can also be refer to as digital services. The infrastructures and quality services play a key role in economic development. [14] It is observed that the public and private sectors are key for efficiency and improved critical service and infrastructure delivery.

As part of achieving the National development plan, Zambia is currently undergoing computerization of some of the key infrastructures (data centers, servers, and computers) such as power, health, judiciary, road tolling, defense and security, financial institutions, education, utility services and more. [12], [14], [15], [16], [11], [10]. The above are connected within and outside the borders of Zambia [8]. Therefore, different infrastructures and services face different potential threats of cyber-attack that can be devastating if the nation is not prepared to deploy a proactive cybersecurity strategy. Modern warfare is fought in the cyberspace without even non-military weapons [3].

The growing dependence on digital and electronic services has resulted in the growth of cyberspace locally and globally. However, cyberspace has also continued to introduce security threats to the citizens, business and to the state. Different cybercrimes and attacks are also committed there [7]. As of 2017, Price Waterhouse Coopers (PwC) reported that Cybercrimes increased by 23% in Zambia [18]. This is an evident need to make thorough preparations to protect the cyberspace. The increased threats to critical infrastructures can lead to a more devastating socioeconomic challenge if there is no adequate cyber-attacks preparedness strategy in place. The growing number of

connected devices, (Internet of Things (IoT) remains to be the growing targets. Security must be extended to networking and computer systems by applying different processes, techniques and mechanisms as part of the plan for defense-in-depth [20].

According to [21] The Defense Act Chapter 106 of the Laws of Zambia, The Ministry of Defense (MoD) is charged with the responsibility of preserving, protecting and defending the sovereignty and boundary integrity of Zambia for the primary purpose of the state, its citizens and residents are safeguarded from both internal and external aggression. The Ministry of Defense draws its mandate from the Government Gazette Notice No.836 of 2016 [71]. The defense force of Zambia comprises The Zambia Army, Zambia Air Force (ZAF), Zambia National Service (ZNS) and The Chaplaincy. The Zambia Army protects the nation from land-based enemies [22]. The Cyber Security and Cybercrime Bills of 2017 draft proposed the establishment of Zambia National Cybersecurity Agency comprising of the security wings and including the Zambia Police Service (ZP). The act which gives any institutions to be the ones managing cyberspace is not known but there is a proposed National Cyber Security Emergency Response Team (CERT) which is not enacted as well [23]. What we are yet to see, is another organ or agency (or at-least a Cyber Command and Control Division) that is fashioned to complement the four existing services and assist in protecting the Zambian Cyberspace (and critical information infrastructure) from internal and external aggression [22].

1.2 Statement of the Problem

The internet is changing the landscape over which business, political, and social interactions are taking place [24]. As such, the public and private are investing in new technologies. There are on-going efforts of the development of the networked or connected devices and application into cyberspace, hence the new term Internet of Things (IoT) [14], [15], [17], and [27]. This is in the quest to cope with the demand for digitization and digitalization. The cyberspace is a valuable environment with its resources and activities have become susceptible to attacks [27]. Nations might be rich in military personnel, technology, and equipment, but they remain susceptible to attacks through the internet [25].

Therefore, cyber-attacks techniques have changed and warfare is fought in cyberspace [27] [26], and policymakers are now waking up to the challenges of cyberspace shifts. The dynamic of cyber-attacks are asymmetric, evolving just like terrorism and the weapons of mass destruction [28].

In Zambia, there has been pronunciations of the Nation ICT Policy, Seven National Development Plan and many other key developmental plans in Zambia, as a way of recognizing the importance of ICTs as the enabler to the economic sectors. However, in spite of this recognition on the importance of ICTs, there are no specific defense plans and strategies for the cyber-attacks preparedness for Zambia in these documents. Therefore, this a gap that needs to be explored. There is no much-published research or existing research on a similar subject for Zambia. This study will, therefore, endeavor to assess the cyber-attacks preparedness strategy for public and private sectors in Zambia.

1.3 Aim or Purpose of the Study

The purpose of the study is to assess a cyber-attacks preparedness strategy for Public and Private Sectors in Zambia as the country continues to expand its critical infrastructure and services. The intention is to identify whether Zambia utilizes cyber-attacks readiness resources in an optimal manner.

1.4 Study Objectives

The general objective of the study is to assess cyber-attacks preparedness for the public and private organisations in Zambia.

This study will be guided by the following specific objectives;

1) To identify the nature and the forms of cyber-attacks.
2) To evaluate the existing preparedness strategies against cyber-attacks.
3) To develop framework that can be used to curb cyber-attacks.

1.5 Research Questions

1) What is the nature and the forms of cyber-attacks? What are the weapons and sources of cyber-attacks?
2) What are the critical infrastructures which might be targeted for cyber-attacks? What are the existing strategies against cyber-attacks preparedness in Zambia?
3) What are the appropriate frameworks and strategies that can be used to curb cyber-attacks in Zambia?

1.6 Significance of the Study

Findings of this study will help in the following:

1) To the best knowledge of the researcher, not much has been done in this area. Therefore this study will help cover the knowledge gap in cyber-attacks in Zambia. The findings of

this study can be used for reference by future scholars for further research work on the same or similar research topics.

2) By identifying the weaknesses of the current strategies, this study will help policymakers both in the private and public institutions formulate policies that will protect further attack of information and systems within the organizations. This will further prevent the loss of valuable information and ultimately revenues within these organisations.
3) The development of a framework resulting from this study can be used by various policymakers dealing with the challenges of cyber-attacks.

1.7 Scope of the Study

This study focused on attacks committed within the context and landscape of Zambia. Further, the study endeavored to address all forms of cyber-attacks.

1.8 Operational Definitions

Cyber warfare – The use of network and computer-based attacks to further the political, economic, and military goals of nation-states.

Defense-in-depth – the application of cybersecurity techniques and mechanisms at multiple levels.

Cyber security – the practice of defending computers, networks and data from malicious attacks.

Cyberspace – the notional environment in which communication over computer networks occurs.

Critical Infrastructure – refers to processes, systems, facilities, technologies, networks, assets and services essential to the health, safety, security or economic well-being of citizens and the effective functioning of state.

Cyber-attack – gaining unauthorized access into the network or computer system to conduct an illegal intend task.

Cyber Weapons – material, instrument, mechanism, equipment, or software used, designed, or intended to be used to conduct a cyber-attack.

1.9 Ethical Considerations

The corresponding author hereby confirms that ethics were considered for this research. And that the article is original and its contents are unpublished. The co-authors has read and approved the manuscript for submission.

1.10 Theoretical Framework

This study will also be guided by the [29] International Standard Organisation and International

Electrotechnical Commission (ISO/IEC) 27000 series, (ISO/IEC) 20000, (ISO/IEC) 38500, Control Objectives for Information and related Technology (COBIT), IT Baseline Protection Catalogs, Information Security Management Model, and Information Technology Infrastructure Library (ITIL) and other theoretical best practices. The ISO/IEC 27000 series are widely recognised standardisation for information security (also known as the ISO 27000 series) is developed and published by ISO and IEC to provide globally recognised standards and frameworks for best-practice in information security management.

The guidelines are used when they are implemented effectively within the scope and the needs of the business. Cybersecurity standards are generally applicable to all organisations regardless of their size or the industry and sector in which they operate. The standards, frameworks and best practices are usually recognised as essential component of any cybersecurity and governance strategies for the business [29]. ITIL supports the alignment of IT services the business, facilitate business change, transformation, and growth [30]. COBIT is the framework for the governance and management of enterprise IT [31].

1.12 Organization of Thesis

This thesis has been organized into five major parts. The introduction discusses the problem background, problem statement, research questions, study objectives, the theoretical and significance of the study. Chapter two goes on to review the literature from books, journals, articles and web pages that have been recorded on the subject matter and Chapter three looks at methodology while chapter four discusses the results obtained from the collected and processed data. Chapter five highlights the discussion, recommendations and conclusions that have been drawn from the entire study.

1.13 Chapter Summary

Cyber-attacks remain one of the threats to the development of the social and economic growth of the nation. Despite the pronunciation of the Seventh National Development Plan and the Nation ICT Policy, we do not know about the plans for the cyber-attacks preparedness framework for Zambia. The nation has recorded the increasing construction of key infrastructure and delivery of services via the Cyberspace. These critical infrastructures and services are connected to the internet and to the rest of the world. Attackers either internally or externally might exploit the weakness which might lead to an attack. Any attack on these will paralyses key sectors. There leaves a gap

that needs to be explored. This study will, therefore, endeavor to develop a cyber-attack defense preparedness framework for Zambia.

In this study, the key critical sectors and services in the Lusaka province were identified as a representation of the sectors in Zambia.

CHAPTER TWO

2.0 LITERATURE REVIEW

The Internet has become a target for strategic cyber-attacks among countries that are figuring prominently in the security and safety strategies, and companies are investing billions [32], [33], [170]. On all of them are driven by the increased dependence on the Internet, from controlling the armed forces to trade, e-commerce, social communication. Everything relies on the Internet. We are in some ways dependent on the Internet today [34], [35]. Attackers exploit the Internet to achieve their well-prepared agenda. The most-reported cyber-attacks the motives behinds are different some are regarded a political, activism, sabotage, state-sponsored, and more [36], [37]. Cyber warfare-attacks are not only associated and initiated by military operations, but the civilians who know what they are doing are also launching cyber-attacks [38]. With the increase of easy to use the tool on the internet, anyone with an attacking motive can launch an cyber-attack. Some researchers use the terms ‘cyber-attack’ and ‘cyberwarfare’ interchangeably [27].

2.1 Definitions

2.1.1 Cyber-Attack

The cyber-attacks that have occurred in the past years have shown the vulnerabilities of using the internet and the weaknesses of cyber defenses [32]. One can view a cyber-attack as any action taken to harm a computer network for a political, sabotage, protect against something, for financial gain and others. It is also a security breach in the cyberspace [37]. [39] Computer network vulnerabilities, if are found, are usually exploited to undermine the function of the system. Some of the vulnerabilities used are known as ‘zero-day’ as they had not been uncovered or made known to the developers. Stuxnet, for example, was found to use a total of four zero-day vulnerabilities [40].

2.1.2 Cyber Warfare

Clausewitz defines war as an act of violence to compel our opponent to fulfil our will [41]. The United States Department of Defence defines the cyberspace as the notional environment in which digitised information is communicated over computer networks. The National Military Strategy for computer network Operations refers to the computer network of the domain characterised by the utilisation of natural philosophy and also the spectrum to store, modify, and exchange

knowledge via networked systems and associated physical infrastructures. Cyberwarfare as: 'an armed conflict conducted in whole or in part by cyber means' [42].

Stiennon, on the other hand, defines cyber warfare as the use of network and computer-based attacks to further the political, economic, and military goals of nation-states [41].

The fourth industrial revolution continues to grow but, the big data, internet of things, artificial intelligence systems, cloud computing are becoming targets for cyber-attacks. Larger economies have invested to establish the command and control systems, to manage and control everything by employing intelligence cyber capabilities [27]. The increased targets to critical infrastructure connected to the cyberspace results in cyber-attacks (cyberwarfare) continues to become borderless. As a result they are different from traditional physical internal and external aggressions which is plotted by using military techniques on the land, sea, and water [43].

Cyberwar generally is associated with the military but it is broader than that. It can be referred to as war waged against those entities that endanger or disrupt the wellbeing of the cyberspace. It is waged to protect the well-functioning of the cyberspace. It reassures the assurance of normal operations achieving the objectives of confidentiality, integrity, and availability of the computer systems and resources [44].

2.2 Related Works

Military terminology has migrated into non-military contexts in the same fashion that military technology has migrated into civilian enterprises (example the Advanced Research Projects Agency Network (ARPANET) becoming the Internet). Other terms, such as Advanced Persistent Threat (APT), (originally a synonym for network attacks supported by the government of the People's Republic of China) have endured similar transitions [45]. In many cases, migration of terminology is beneficial, as it develops better specificity in discussions of technology operations. However, the utility of a term is reduced when its distinctive meaning is eroded or destroyed as part of the migration to a new context [46].

In the publication 'The birth of cyberwar. Political Geography". There are many historical events attributed to the birth of cyber warfare, but the Iranian and Estonian attacks are regarded the birth. In particular, it traces the ways in which the site and situation of the birth cyberwar have affected the emerging techniques of cybersecurity. Cybersecurity professionals, politicians, and military

elites are often agents of cyberwar. For example, Tallinn became elevated as a cybersecurity centre of calculation, and finally how the events of 2007 have served as a precautionary baseline for the anticipatory actions through which future cyberwars are made present [47].

The birth of cyberwar. Political Geography" only shares some detailed related research about cyberwar and foretell the future weaponisation but it does not suggest the awareness and preparation for future attacks. It does not suggest the defense mechanism. Therefore, this research is proposing to explorer the gap.

Another publication "Cyberwarfare: Issues and challenges". The paper identified challenges in cyber warfare and analyses contemporary work carried out. It concluded by making suggestions on how the field may best be progressed by future efforts [48]. This research looked at the specific cyber warfare challenges and does not look at any frameworks with respect to any specific area hence no proposed enhancements as suggested in this research paper.

One of the published material titled "Cyber resilience preparedness of Africa's top-12 emerging economies", the author of this book proposes the Cyber Resilience Preparedness Index for monitoring and comparing the cyber resilience of Africa's top-12 emerging economies. The index covers five critical areas that incorporate a total of 24 indicators derived or adapted from the International Telecommunication Union of 2014 Cybersecurity posture profile, a Depository Trust and Clearing Corporation white paper on global cyber risk and the well-known Cyber Readiness Index [49]. It looks at Cyber Resilience Preparedness Index for monitoring and comparing the cyber resilience of Africa's top-12 emerging economies and does not look at the framework with respect to any specific area hence no proposed enhancements as suggested in this research paper.

J. A. Bullock. Etal in the book "Cybersecurity and Critical Infrastructure" established that the infrastructures are extensive and include all of the basic physical and organizational structures, systems, services, and facilities that are required for society to operate. The security of computer—or "cyber"—systems, is a matter of national security. We are faced with the fact that a nation, group, or even an individual armed with nothing more than a complex computer virus or knowledge of a weakness in a software package or hardware system can quietly and from a great distance cause significant social or economic disruption or worse, physical destruction, injuries, and deaths [50]. This book looks at the general overview of critical infrastructures and, however,

does not look at with specific preparedness frameworks against cyber-attacks with respect to any specific area hence no proposed enhancements.

Introduction to Cyber-Warfare: A Multidisciplinary Approach: Introduction to Cyber-Warfare: A Multidisciplinary Approach, written by consultants on the front lines, provides you associate insiders cross-check the globe of cyber-warfare through the use of recent case studies. The book examines the problems associated with cyber warfare not solely from an engineering perspective however from military, social science, and scientific views similarly. The research provides a multi-disciplinary approach to cyber-warfare, analyzing the data technology, military, policy, social, and scientific problems that area unit live. There are some elaborated case studies of cyber-attack together with inter-state cyber-conflict (Russia-Estonia), cyber-attack as a component of associate data operations strategy (Israel-Hezbollah,) and cyber-attack as a tool against dissidents among a state (Russia, Iran). Explores cyber-attack conducted by giant, powerful, non-state hacking organizations like Anonymous and LulzSec.

The author covers cyber-attacks directed against infrastructures, such as water treatment plants and power-grids, with a detailed account of Stuxnet [51]. The research provides detailed case studies and critical infrastructures but does not discuss the need for the state to be prepared by adopting any framework or model. This research was built from that and explored ways to develop a framework that might add to the past research works.

Cyber Warfare Awareness in Lebanon: Exploratory Research: Countries are ready for the aforesaid challenges and threats, whereas Lebanon is not. It investigates the current standing of cyber warfare awareness and clarifies what changes could also be incorporated into the Lebanese sectors, as well as the tutorial one.

This study focused on students. The outcomes were that in Lebanon, the educated community not only lacks awareness but also knowledge of what is happening in the arenas of cyber warfare, cyber weapons and cybersecurity [53]. The study focused on awareness and on the population of students. Therefore, the proposed research will build up and develop a preparedness framework defense against cyber-attacks.

Cyberwarfare - An analysis of the means and motivations of selected nation-states. The purpose of this report was to supply a practical assessment of the capabilities, means, and motivations of

designated nation-states to conduct a far off, computer-to-computer attack either against the United States or against regional adversaries. The consequences of an attack "through the wires," and therefore the degree of potential disruption, can usually depend upon the generality (and so importance) of the network impaired by the attack: national versus regional, local, or municipal in scope [7]. The study offers a very detailed practical assessment which can also be applied in this research but the research will go farther to develop the framework or model which was not considered in this related work.

2.3 Cyber-Attacks Preparedness

The modern world is highly interconnected, the cyberspace and the wide array of risks and threats associated with it have become more and more preoccupying for citizens, businesses and the states. The increasing range and sophistication of threats in the cyber realm – from malware to distributed denial of service (DDoS) attacks to advanced persistent threats (APT) – have prompted means to eliminate risks threatening the private and public sectors. This includes economic and military espionage, theft of intellectual property, interference with critical infrastructure, and destruction of data. In this context, states are developing cyber-defence and cyber-offense capabilities to prepare for the advent of 'cyberwar' [42]. Internet attack reports have increased making headlines in the news across the globe. Therefore, it is important for individuals, business and governments to be alert by employing security and safety measures against cyber-attack surprises. It is imperative to state that how Nations prepare themselves against cyber-attacks will determine the impact of a cyberattack on their infrastructure [7]. The preparation is always with intent prevent a tactical defeat during conflict when a cyberattack targeting command and control and communications infrastructure is blocked [156].

2.4 Cybersecurity Frameworks

The widespread and usage of connected electronic devices influence the social-economic status of the state [24], [53]. Cyber-attacks, the use of network and computer-based attacks to further the, individual, political, economic, and military goals of nation-states [54], [55], [51], [56]. Therefore, the dependence on the internet creates threats as well [57], [58], [59], [24]. Cyber-attacks finds its origin not because of connected devices but in hacking. The United States (U.S) Commerce Department of the National Institute of Standards and Technology (NIST) developed a Framework used for Infrastructure Cybersecurity [60], called the Cybersecurity Framework [55]. The

Cybersecurity Framework needs to be prioritized, flexible, and economical to support the protection and resilience of its essential infrastructure and totally [61], [62]. See Figure 2.1

The Framework Core is structured into five Functions that identify the key cybersecurity outcomes identified to manage cybersecurity risk [63], [61]:

1) ***Identify*** – develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.
2) ***Protect*** – develop and implement the appropriate safeguards to ensure the delivery of critical infrastructure services.
3) ***Detect*** – develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.
4) ***Respond*** – develop and implement the appropriate activities to take action regarding a detected cybersecurity event.
5) ***Recover*** – develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event [64].

Figure 2.1: NIST Cybersecurity Framework Version 1.1 [60]

Table 2.1: NIST Cybersecurity Framework Version 1.1(Credit NIST) [60]

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

2.5 The United Nations Agenda to Cybersecurity

Since the 1865 International Telecommunications Union (ITU), a wing of the United Nations (UN) has significantly contributed to set global telecommunications, information security and standards in different capacities for its members. In 1946 ITU became formally the specialised agency of the United Nations in the field of telecommunications, information and communication technologies (ICTs). The Agency the global focal point for member states, governments and the private sector in developing policies and standards for networks, services, and mechanisms against threats and

vulnerabilities. The Agency coordinates UN Resolutions aimed at spreading the benefits of the new technologies to all nations [27], [160].

The ITU, Global Cybersecurity Agenda (GCA) has released a framework or model which is generic for international multi-stakeholder and its member state on cybersecurity. The aim is to build synergies with current and future initiatives and members with the sense of security assurance in the cyberspace and information society. Below are Work Areas of the GCA:

1) *Legal Measures:* This Pillar seeks to elaborate methods for the event of model globally applicable and practical crime legislation.
2) *Technical and Procedural Measures:* This Pillar focuses on measures for addressing vulnerabilities in software system merchandise acceptable enfranchisement schemes, protocols and standards.
3) *Organizational Structures:* The Pillar aims to form organisational structures and techniques to assist forestall, discover and reply to attacks against essential info infrastructures.
4) *Capacity Building:* This Pillar seeks to elaborate methods for enhancing information and experience to spice up cybersecurity on the national policy agenda.
5) *International Cooperation:* The Pillar focuses on methods for international cooperation, dialogue and coordination.

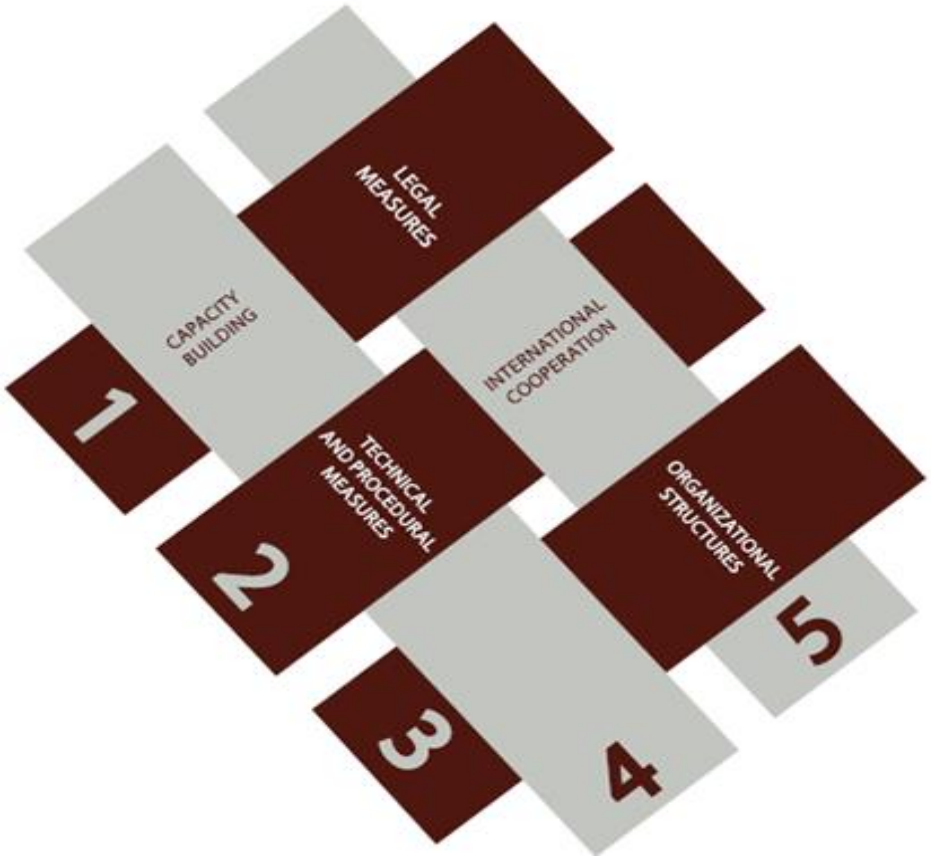

Figure 2.2: ITU CGA Model [27]

2.6 Why Cyber-attacks are On the Rise

The continuous advancement in technology has shifted the way humans live and behave. Most human activities depend on the usage of technology [65], [66]. The world is connected like never before. Everything is connected. Humans are connected to humans, humans are connected to machines, [64] machines are connected to humans, and machines are connected to machines [4, 67]. As with all technological advances in history, the cyber world has also been turned into weaponisation. It began with people pushing the limit of the net or going for private gain, but now governments have begun to realize that the potential of cyber-attacks are very real, and therefore the cyber breaches may well be disastrous. The Internet is vulnerable to attacks especially if appropriate defense parameters are not applied [74]. The attacks are on the rise because a lot of critical infrastructures and services are implemented without proper defense strategies [24], [25]. There are on-going demands for the digital services but the call to respond to it with up-to-date

regulations are slow [68]. Where there is no strategy on standards, policy and mechanism attackers find it easy to penetrate.

The borderless of the Cyberspace allows participation from all types of hackers, keeps increasing with limitless involvement [25]. An attacker can easily connect to other computers in the network to remain anonymous. These computers will be used to create processing power to the attacker [58]. The attacker can pull the processing power from different computer networks from different geographical locations without being noticed. Countries do not use the same laws. What is illegal in one country might not be also into another. The increase in technologies in comparison with the laws, technological development is ever ahead of laws. [4].

The actors in cyber-attacks are not only military personnel. They do not necessarily need to be experts to cause malicious actions [20]. The ignorance of the users which is taken by lack of awareness is another form that causes attackers to gain easily into the targeted systems and cause harm or fulfill the intentions [9]. There is also a shortage skilled and experienced of cyber-warriors globally, more especially in developing nations [69].

2.7 Offensive Weapons and Tactics

Cyber-attacks activities are very broad in nature and are categorized according to motives of actors and the impact it creates [70].

2.7.1 Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) Attacks

A denial-of-service attack overwhelms a system's resources so it cannot answer service requests [71]. This happens by disabling or destroying an online resource through overwhelming it via too many requests.

2.7.2 TCP SYN Flood Attack

In this attack, an attacker exploits the use of the buffer space during a Transmission Control Protocol (TCP) session initialization handshake. The attacker's device floods the target system's small in-process queue with connection requests, but it does not respond when the target system replies to those requests. However, it causes the target system to time out while waiting for the response from the attacker's device, which makes the system crash or becomes unusable when the connection queue fills up [71].

2.7.3 Teardrop Attack

This attack causes the length and fragmentation offset fields in sequential Internet Protocol (IP) packets to overlap one another on the attacked host; the attacked system attempts to reconstruct packets during the process but fails. The target system then becomes overwhelmed and crashes.

2.7.4 Smurf Attack

This attack involves using IP spoofing and the Internet Control Messaging Protocol (ICMP) to saturate a target network with traffic. This attack method uses ICMP echo requests targeted at broadcast IP addresses. These ICMP requests originate from a spoofed "victim" address.

2.7.5 Ping of Death Attack

This type of attack uses IP packets to 'ping a target system with an IP size over the maximum of 65,535 bytes. IP packets of this size are not allowed, so attacker fragments the IP packet. Once the target system reassembles the packet, it can experience buffer overflows and other crashes.

2.7.6 Botnets

Botnets are a network of systems infected with malware under hacker control in order to carry out DDoS attacks. These bots or zombie systems are used to carry out attacks against the target systems, often overwhelming the target system's bandwidth and processing capabilities. These DDoS attacks are difficult to trace because botnets are located in differing geographic locations [72].

2.7.7 Man-in-the-Middle (MitM) Attack

A MitM attack occurs when a hacker inserts itself between the communications of a client and a server. Here are some common types of man-in-the-middle attacks:

2.7.8 Session Hijacking

In this type of MitM attack, an attacker hijacks a session between a trusted client and a network server. The attacking computer substitutes its IP address for the trusted client while the server continues the session, believing it is communicating with the client [73]. See Figure 2.3: Man in the Middle Attack (Session Hijacking) and Figure 2.4: Man in the Middle Attack (Session Hijacking).

2.7.9 IP Spoofing

Internet Protocol (IP) spoofing is used by an attacker to convince a system that it is communicating with a known, trusted entity and provide the attacker with access to the system [74]. The attacker sends a packet with the IP source address of a known, trusted host instead of its own IP source address to a target host. The target host might accept the packet and act upon it.

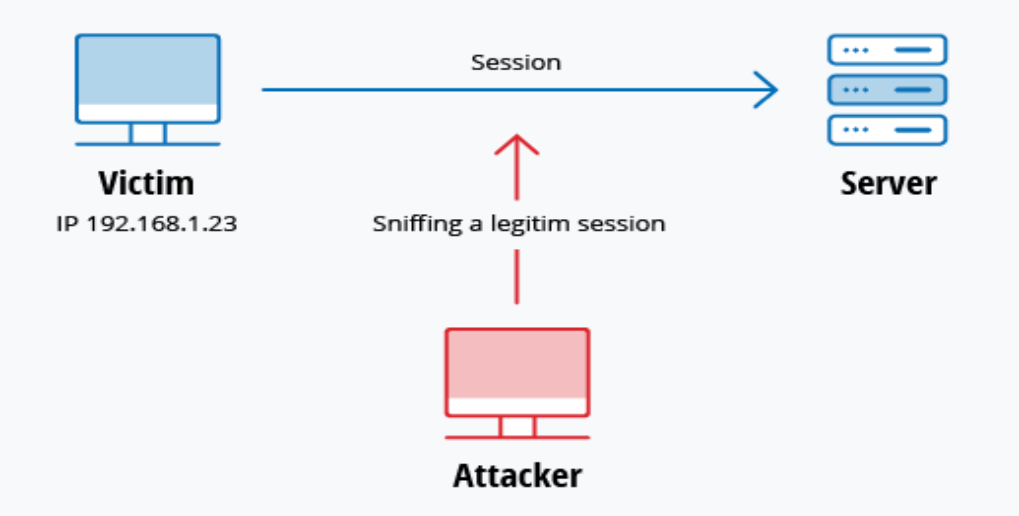

Figure 2.3: Man in the Middle Attack (Session Hijacking) [80]

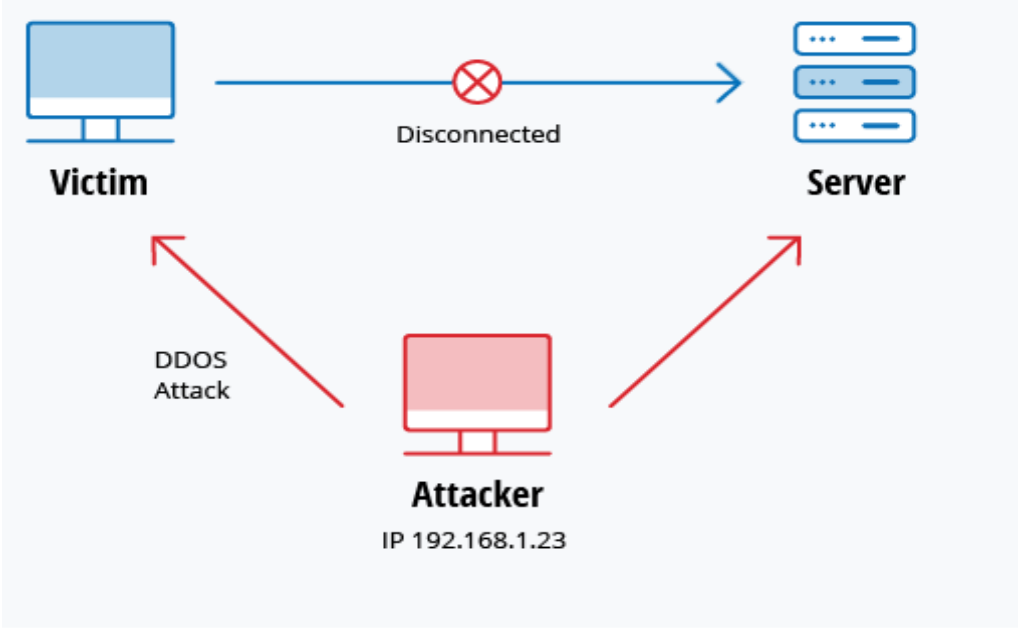

Figure 2.4: Man in the Middle Attack (Session Hijacking) [80]

2.7.10 Phishing and Spear-Phishing Attacks

A phishing attack is a practice of sending emails that appear to be from trusted sources with the goal of gaining personal information or influencing users to do something. It combines social engineering and technical trickery.

Spear phishing is a much-targeted type of phishing activity. Attackers take the time to conduct research into targets and create messages that are personal and relevant. Because of this, spear phishing can be very hard to identify and even harder to defend against [75]. One of the simplest ways that a hacker can conduct a spear-phishing attack is email spoofing, which is when the information in the "From" section of the email is falsified, making it appear as if it is coming from someone you know, such as your management or your partner company. Another technique that scammers use to add credibility to their story is website cloning — they copy legitimate websites to fool you into entering personally identifiable information (PII) or login credentials.

2.7.11 Drive-by Download Attack

Drive-by download attacks are a common method of spreading malware. Hackers look for insecure websites and plant a malicious script into HTTP or PHP code on one of the pages. This script might install malware directly onto the computer of someone who visits the site, or it might re-direct the victim to a site controlled by the hackers [76]. Drive-by downloads can happen when visiting a website or viewing an email message or a pop-up window. Unlike many other types of cybersecurity attacks, a drive-by doesn't rely on a user to do anything to actively enable the attack — you don't have to click a download button or open a malicious email attachment to become infected. A drive-by download can take advantage of an app, operating system or web browser that contains security flaws due to unsuccessful updates or lack updates [73].

2.7.12 Password Attack

Because passwords are the most commonly used mechanism to authenticate users to an information system, obtaining passwords is a common and effective attack approach. Access to a person's password can be obtained by looking around the person's desk, ''sniffing'' the connection to the network to acquire unencrypted passwords, using social engineering, gaining access to a password database or outright guessing. The last approach can be done in either a random or systematic manner brute-force and dictionary attacks [76].

2.7.13 SQL Injection Attack

Structured Query Language (SQL) injection has become a common issue with database-driven websites. It occurs when a malefactor executes a SQL query to the database via the input data from the client to server. SQL commands are inserted into data-plane input (for example, instead of the login or password) in order to run predefined SQL commands. A successful SQL injection exploit can read sensitive data from the database, modify (insert, update or delete) database data, execute administration operations (such as shutdown) on the database, recover the content of a given file, and, in some cases, issue commands to the operating system [76].

2.7.14 Cross-Site Scripting (XSS) Attack

Cross-site scripting (XSS) attacks use third-party web resources to run scripts in the victim's web browser or scriptable application. Specifically, the attacker injects a payload with malicious JavaScript into a website's database. When the victim requests a page from the website, the website transmits the page, with the attacker's payload as part of the HTML body, to the victim's browser, which executes the malicious script. For example, it might send the victim's cookie to the attacker's server, and the attacker can extract it and use it for session hijacking. The most dangerous consequences occur when XSS is used to exploit additional vulnerabilities. [77] These vulnerabilities can enable an attacker to not only steal cookies, but also log key strokes, capture screenshots, discover and collect network information, and remotely access and control the victim's machine.

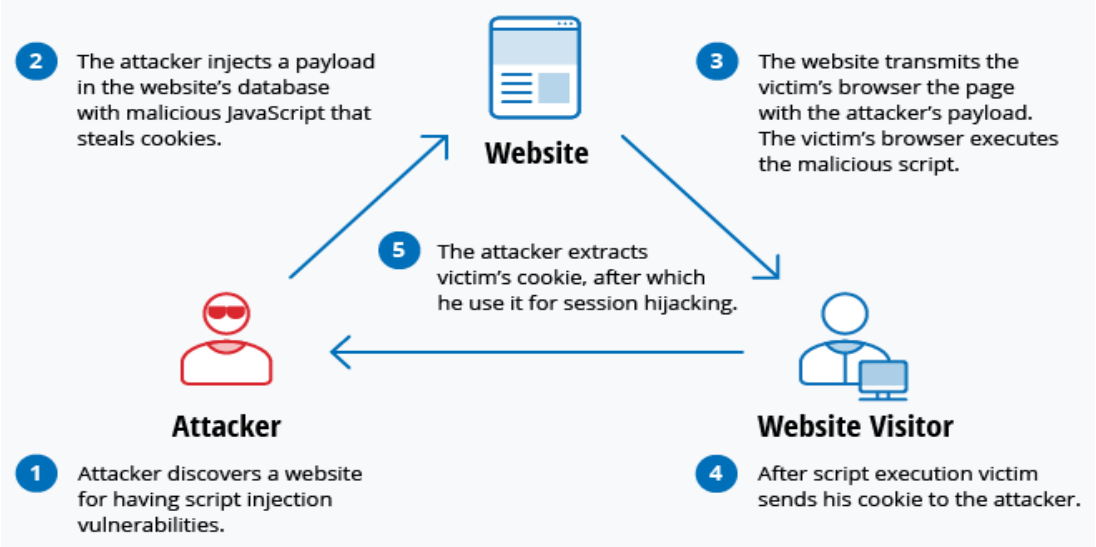

Figure 2.5: Cross-site scripting (XSS) attack (Source Coursera) [80]

While XSS can be taken advantage of within Visual Basic (VB) Script, ActiveX and Flash, the most widely abused is JavaScript — primarily because JavaScript is supported widely on the web.

2.7.15 Eavesdropping Attack

Eavesdropping attacks occur through the interception of network traffic. By eavesdropping, an attacker can obtain passwords, credit card numbers and other confidential information that a user might be sending over the network [78].

2.7.16 Birthday Attack

Birthday attacks are made against hash algorithms that are used to verify the integrity of a message, software or digital signature. A uniquely characterized message processed by a hash function produces a Message Digest (MD) of fixed length, independent of the length of the input message [79]. The birthday attack refers to the probability of finding two random messages that generate the same MD when processed by a hash function. If an attacker calculates same MD for his message as the user has, he can safely replace the user's message with his, and the receiver will not be able to detect the replacement even if he compares MDs.

2.7.17 Malware Attack

It can be described as unwanted software that is installed in your system without your consent. It can attach itself to legitimate code and propagate; it can lurk in useful applications or replicate itself across the Internet. Here are some of the most common types of malware: Macro viruses, File infectors, System or boot-record infectors, Polymorphic viruses, Stealth viruses Trojans, Logic bombs, Worms, Droppers, Ransomware, Adware and others.

2.8 Sources of Cyber-Attack Weapons

Actors who consciously decide to conduct cyber-attacks can potentially cause harm for any system which directly or indirectly is connected to the Internet [27]. See Figure 2.6. The diagram below shows source of cyber-attacks.

1) *Botnet Command Control Operators:* Botnet central command uses a network, or zombies, of compromised, remotely controlled systems to connected attacks and to spread phishing schemes, spam, and malware attacks. [55].

2) *Organised Criminal Groups:* Organised criminal teams get to attack systems for gain. They use sophisticated and advanced spam, phishing, and spyware or malware to commit identity theft and online fraud.
3) *Hackers:* Hackers break into networks for the thrill of the challenge, bragging rights in the hacker community, protest, and revenge, stalking others, and monetary gain, as well as other reasons [58].
4) *Insiders:* Insiders might access data either by curiosity or intention as a result of their knowledge of the target system typically permits them to realize unrestricted access, thereby causing damage to the system or stealing system data. [58].
5) *Nations Sponsored:* Nations use cyber tools as a part of their information-gathering and undercover work activities. [59].

2.9 Motives for Cyber Attacks

The actors of cyber-attacks also refer to as 'hackers' (whether for financial gain or as a challenge), cause-based groups, proxies for governments, and governments (including their military and intelligence agencies) [27]. The motives for the attacks range from financial gain to the advancement of national security interests [80], to the satisfaction of peer recognition, and to the advancement of various causes [60], [73]. To understand to motives it is important to ask a question: Is a Cyber War taking place right now or about to begin? Who is attacking? [81]. What is the target? What kind of attack methods is being used? [82], [83].

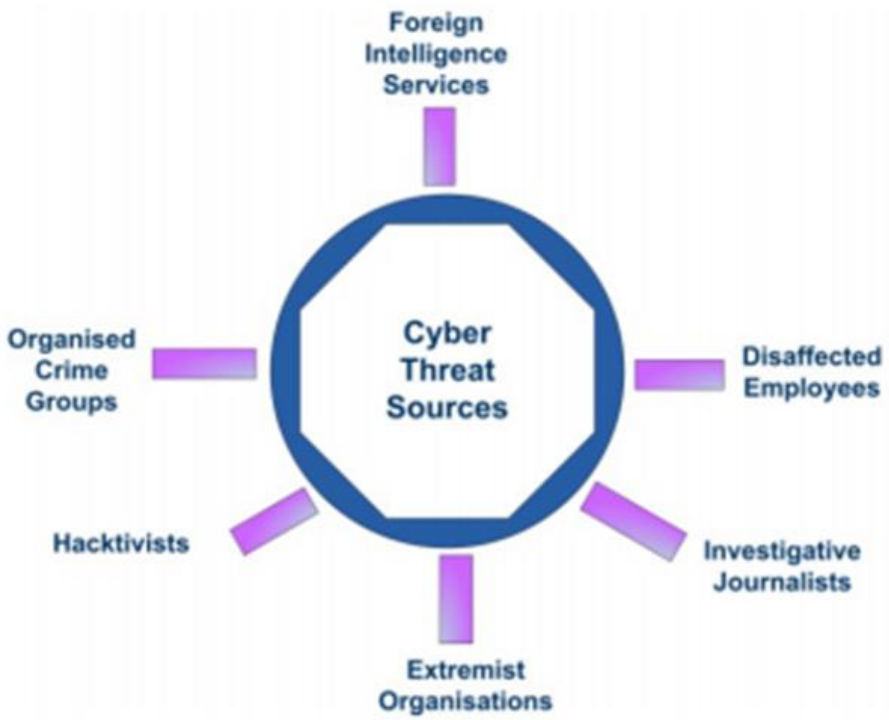

Figure 2.6: Sources of Cyber-Attacks (Source ITU) [37]

1) **Disaffected Employees:** These are the most dangerous to an enterprise as they are "insiders". Since many companies subcontract their network services a disgruntled vendor could be very dangerous to the host enterprise.
2) **Hacktivists:** Hack as a mechanism to promote some political or ideological purpose. Usually coincide with political events
3) **Organised Criminal Groups:** Real criminals, are in it for whatever they can get no matter who it hurts.

2.10 Forms and Nature of Cyber Attacks

The Forms and Nature of Cyber Attacks are Offensive in nature to destroy, disrupt or neutralise adversary cyberspace capabilities both before and after their use against friendly forces, but as close to their source as possible [84]. It is claimed that the attackers always have an advantage when successfully exploited the vulnerabilities, gains access and clear the marks [85]. They only need to find one hole to penetrate a system, while those who defend the system must locate and seal all holes [86], [87]. The techniques for cyber offensive operations, including network intrusions, malware, botnets, and denial-of-service (DoS) attacks [88], [89]. The method of attack

is determined by the objectives and the type of vulnerabilities exploited [90], [91]. An attacker can spend weeks [89], months or even years to study the targeted network and come up with the method that can help to break into the system [92]. The author reviewed the forms and nature of cyber-attacks in section 2.7. They can be formed as offensive weapons as well as the forms and nature of cyber-attacks [93], [94]. These include the espionage, propaganda, denial-of-service (DoS) [95], data modification and infrastructure manipulation [70], [80].

2.10.1 Espionage

Governments around the world complain publicly of cyber espionage but no state or group will easily accept being the sponsor of the attack [96]. Cyber espionages are making headlines in the daily international news. Computer hackers are anonymously secretly and illegally access unauthorized computer data and network communications. The implication of these attacks are that they lead to undermining intelligence-gathering on highly sensitive corporate, political and military communications [76].

2.10.2 Propaganda

Internet Propaganda is cheap and effective, easiest and the most powerful cyber-attack [96]. With the proliferation of the internet, social media, and online news sites, it is very easy to form propaganda news. Therefore, propaganda spreads very quickly is usually very provocative in its nature [70].

2.10.3 Denial-of-Service (DoS)

The simple strategy behind a DoS attack is to deny the use of a computer resource to legitimate users [76]. The most common tactic is to overwhelm the target system with too many requests for services or information causing it to run out of memory. Physical damage or vandalism of physical computer systems and any form of interference can also be a form of DoS [88].

2.10.4 Data Modification

Data modification is very dangerous as a result of a successful attack which will mean that legitimate users (human or machine) can build a crucial decision(s) supported maliciously altered info. Such attacks vary from web site defacement (often spoken as “electronic graffiti”, however which may still carry information or disinformation) to information attacks meant to corrupt weapons or Command and Control (C2) systems [76].

2.10.5 Infrastructure Manipulation

National critical infrastructures are increasingly connected to the Internet [76]. For example, the management of the electricity grid may be crucial to the nation because it is important for national security planners to monitor because electricity has no substitute, and all other infrastructures depend on it. Major critical infrastructures are developed and managed by the public and private sectors [97]. In the proposed cybersecurity and crimes bill 2017 [13], it is proposed that the critical information infrastructures shall be registered to the government so that the state can provide security [98].

2.11 Challenges Affecting Cyber Defense

Cyberspace actors conceal or disguise their identities in a way that is not possible in the real world. Anonymity is an obvious advantage of an offender, and digital technology facilitates this in a number of ways [165]. Offenders may deliberately conceal their identity and remove digital evidence by using available encryption software, proxy servers, VPNs, tor browsers and so on [99]. The dark and deep webs have continued to remain as one of the major challenges in cyber defense. The management of risk to info systems is taken into account elementary to effective cybersecurity [71], [90].

Most cyberattacks have different impacts, but a successful attack on critical infrastructure (CI) could have significant effects such as compromises national security, economic sabotage, disruption of basic services, communication infrastructure sabotage and many more. Reducing such risks usually involves removing threat sources, addressing vulnerabilities, and lessening impacts [82].

Cybercrime is regarded as cheap, profitable, and comparatively safe for the criminals. In contrast, cybersecurity can be expensive, is by its nature imperfect, and the economic returns on investments are often unsure [99].

Traditional approaches to security may be insufficient and challenging in the highly interconnected environment, but consensus on alternatives has proven elusive. The dependence and growth of social media, mobile computing, online applications, big data, cloud computing, and the Internet of Things introduce new threats [155]. These require constant innovation in defense intelligence.

2.12 Regulatory and Legal Jurisdictions

With the growing interconnectedness of the world, the risks associated with online communication have become increasingly pressing. Due to the global nature of such communication unhindered by physical boundaries, network technologies challenge the existing international legal structure based on such notions as jurisdiction and sovereignty, where each sovereign jurisdiction regulates communication that takes place in its territory [157]. Online communication, that bypasses geographical and jurisdictional restraints, is a serious concern for the national and international legal orders in their current form [73]. The challenge is that the current legal frameworks are traditionally regarded as local in nature, being restricted to the territorial jurisdiction in which an event occurs [99].

With all these challenges in hand, the effective legal regulation of the internet presumes creation of the viable policy that can adequately address the substance of the problem and its technical complexity on various levels, including legislative interventions in the form of criminalization and harmonization; international cooperation; collaboration with the private sector; professional educational and capacity building in terms of technical support and assistance, especially in the developing countries [99], [100].

2.13 Involvement of Non State and Sate Actors in Cyber-attacks

Cyberspace is a networked operational environment connecting the state and non-state actors and much like in the physical space, the tactics, targets, information, and general operation by each in cyberspace are different [101]. The presence of non-state actors on the international stage has grown steadily in recent years. The unique features of cyberspace, including its borderless character, its inherent interconnectedness, the anonymity it affords and its accessibility, has provided a thriving environment for non-state actors and cyberspace has thus further empowered non-state actors to act independently from states in the international arena. Indeed, it is likely that malicious transboundary cyber conduct committed by non-state actors now exceeds that committed by states [102].

Launching a massive cyber-attack does not require a large number of people. An individual with access to the internet is capable of such an attack due to the possibilities of the network and other resources. Consequently, a one-to-one scale of commission is not a viable default assumption [74], [99]. That states are subject to an obligation to prevent their critical infrastructure from being used

in a manner injurious to the international legal rights of other states is well established in regular international law. There are some obligations to the state as implementing the laws and institutions necessary to prevent and criminalize the contacts in their territory, although international law helps in formulating the design and content of such measures. Every institution must develop a posture that a threat emanates from its critical infrastructure and states have (actual or constructive) knowledge of that threat they must act reasonably in utilizing their capacity and resources to suppress it. The institutions especially the state is obligated to develop International Corporation to extradite non-state actors [71].

A state is responsible for the actions of a non-state actor where those actions constitute internationally wrongful conduct and can be attributed to the state [103]. The obligation upon states to prevent their territory from being used to cause harm to other states has deep roots in international law. The most famous articulation of this customary obligation can be found in the Corfu case in 1949 [100]. One of the primary reasons for why the cyberspace is such a difficult environment to regulate is because actors can easily obfuscate their identity. Another reason is that actors can easily conceal malware within ostensibly legitimate computer operations. Technologically advanced states will possess sophisticated cyber tracing techniques that enable authorities to accurately identify those responsible for committing malicious cyber operations and thus take enforcement action against them and will also be able to better decipher computer codes in order to ascertain whether they contain malware. International law requires these states to do more to counter cyber threats emanating from their territory than those possessing less technical capacity. Note however that the standard of due diligence owed in any particular case can become more demanding if a state capacity changes [101].

2.14 Defense Strategies

All defensive countermeasures designed to detect, identify, intercept, and destroy or negate harmful activities attempting to penetrate or attack through cyberspace' [84]. Mounting a good defense requires understanding the offense outlook broadly. The researcher has reviewed the most common forms and nature of cyber-attacks that hackers use to disrupt and compromise information systems. An attacker can launch DDoS assaults, malware infection, man-in-the-middle interception, and brute-force password guessing, to trying to gain unauthorized access to critical infrastructures and sensitive data [24].

It is important to apply basic measures to mitigate threats. Keep your systems and anti-virus databases up to date, train the employees, configure firewall to whitelist only the specific ports and hosts you need, keep passwords strong, use a least-privilege model in the IT environment, make regular backups, and continuously audit theIT systems for suspicious activity [104].

The literature has pointed out that there are so many methods of conducting cyber-attacks, a huge market for technology that protects the network from unauthorized access has grown. The strategy of developing a Defense-in-depth with objectives to achieve, Prevention, Detection, Identification and Mitigation the deployment of security techniques and mechanisms at all layers such as Cryptography, Encryptions, and Access Control: Identification and Authentication, Intrusion and Malware Detection and Prevention Systems [88]. It also gives an overview of technologies and methods of defense, including cryptography, access controls, and intrusion or malware detection or prevention [93]. When all these are achieved, a sense of security assurance is realized, confidentiality, integrity and availability of the infrastructure and services.

2.15 Cyber Command and Intelligence

An effective cyber defense framework requires a wide range of offensive and defensive measures as well as a central authority for command and control [105].

The integration of ICTs into human activities has increased in usage and in number. Cyberspace is vulnerable to attacks which can cause destruction to critical systems and services. Defense intelligence help identify the risks and apply techniques for defense [158]. Spies are used to gathering information about the targets. They will study the technology better and use it to gather as much information about the target [76].

2.16 Disruptive Attacks on Critical Infrastructure

ITU-D Study cluster 126 defines Critical Infrastructure (CI) as *"the key systems, services and functions whose disruption or destruction would have an enervating impact on public health and safety, commerce, and national security, or any combination of those* [106]." while what constitutes critical infrastructure varies across States, during this Study, we tend to regard typical infrastructure sectors as well as health, water, transport, communications, government, energy, finance and emergency services sectors [27].

2.17 Historic Case Reviews

The Example of Sony Pictures cyber-attack was not only left to Sony alone but the US government took interest to protect the assets. The Sony Pictures attack have been described as an act of cyber warfare which can be categorized as espionage. There was a loss of revenue and disruption of services. The US government intervened to protect private property assets.

Nations have not openly come to accept being responsible for any cyber-attacks. What is commonly known is just cold war and propaganda? History has shown that great nations have fought cyber way [107]. The United States, China, and Russia have always been at war. The United States is the hacking power grid of Russia and, Russia is hacking the United State. The hacking is more aggressive than in the past according to the New York Times [108].

The growth of the internet of things in the twenty-first century is a growing cyber-attacks nightmare [109]. The historical events have proved that cyberattacks (warfare) activities with the involvement of military and non-military weaponisation [110].

All the major cyber powers; the United States, Russia, China, Israel, France, Britain, and perhaps to some extent, Iran, Syria, and a few others have been able to hack into one another's "critical infrastructure" (power grids, financial systems, transportation lines, and many more.), which have been connected up to computer networks for the past 25 years. From time to time, these countries have actually hacked into computer systems [108].

2.17.1 Chechnya Propaganda of 1994

The cyberspace has becomes the most popular source of news in real-time. Online news sites and internet users have found the internet as the easiest way to share news which has contributed to conflicts around the globe [24].

During the 1990s when the World Wide Web was just gaining its popularity, pro-Chechen and pro-Russian forces fought the war on the Internet, as well as on the ground [29]. The Chechen separatist movement used the internet as a tool for delivering powerful public relations messages, propaganda [76]. The intention of using propaganda and other information, was used in the creation of a number of fund war bank account in Sacramento, California, helped to bring Chechen living in foreign countries [111].

The most common propaganda was not pro-Chechen, but the information was anti-Russian. Digital images of bloody corpses served to turn public opinion against perceived Russian military excesses. In 1999, the internet was flooded with images that depicted Kremlin officials an incident they denied in which a Chechen bus was attacked and many passengers killed [112]. As technology progressed, Internet surfers watched streaming videos of favorable Chechen military activity, such as ambushes on Russian military convoys [111].

Thereafter, the Russians vowed to improve their cyberspace. In 1999, Vladimir Putin, then Prime Minister of Russia, stated that they had surrendered their terrain some time ago ... but now they were entering the game again. That was how Moscow realized to request for support from the West with the motive to shut down the important pro-Chechen kavkaz.org web site, which resulted in the introduction of centralized military censoring concerning. The war within the North Caucasus was then declared [112].

During the second Chechen war (1999-2000), Russian officers were defendant of escalating the cyber conflict, by hacking into Chechen websites. The arrangement and coordination pointed out that the nation-state was involved in the attack. The website, kavkaz.org which was hosted in the United State was reportedly brought down by Russian Special Forces of a national capital theater underneath encirclement by Chechen terrorists [113].

2.17.2 Military Hacking in Kosovo War of 1999

The increasing number of connected devices and users have created an atmosphere in the cyberspace a computer system can be a subject or object of attack. A computer system can become a combatant. When the internet started to gain its popularity. North Atlantic Treaty Organization (NATO) got engaged on the internet. [76] It is believed that Kosovo was its first state to be engaged in what was known by then as an Internet war.

NATO engaged aerial attack to pro-Serbian (or anti-Western) hacker groups, “Black Hand”, which attacked NATO Internet infrastructure. It is unknown who sponsored the group. Other claim that it was a Yugoslav military. This group wanted to stop NATO’s military operations [114].

The Black Hand (Pan-Slavic secret society) that helped to start World War I, hacked and mimicked NATO’s “critical” computers, with intent to “delete all the data”. It is believed that at least one U.S. Navy computer was brought off-line [76].

Denial of Service attack and virus-infected NATO, U.S., and United Kingdom (UK) computers [115]. In the meantime, the U.S., the White House website was defaced. But the U.S. denied and made claims never to suffer any impact. The UK admitted to having an attack on its database and lost some information [115]. Elsewhere in Belgium at NATO's Headquarters, these attackers created a propaganda victory. This was because NATO's official website for information for the war in Kosovo was "not responding for several days." The emails and other servers become nonresponsive around the world [116].

2.17.3 Cyber-Attacks in the Middle East in 2000

In October 2000, the Middle East Cold was which provides military weapons and tactics that can be likened to Cyberwarfare. It was evident when the Israelis nation anthem was planted on the Hizballah website. The pro-Israeli attacks also went farther targeting websites and political organizations; which were enemies to Israel, such as Palestinian National Authority, Hamas, and Iran [117].

The Pro-Palestinian hackers had a combatant against Israeli political, military, telecommunications, media, and universities. The Bank of Israel, e-commerce sites, and the Tel Aviv Stock Exchange sites were targeted sites on which was regards as pure economic sabotage. This kind of warlike many others revealed new tools and tactics. DoS program was used by both sides for the "Defend" [76].

The Middle East cyber-attack was a sign that the cyberspace conflicts can quickly attract the attention of the international community. It was observed that the Pakistan Hackerz Club attacked the U.S.-based pro-Israel lobby American Israel Public Affairs Committee (AIPAC), and published sensitive emails, credit card numbers, and contact information for some of its members [20] and the telecommunications firm American Telephone & Telegraph (AT&T) became a victim for providing technical support to the Israeli government during the crisis [49].

In 2006, as tensions extend between Israel and Gaza, pro-Palestinian hackers attacked what believed to be 700 Israeli Internet domains, including those of Bank Hapoalim, Bank Otsar Ha-Hayal, BMW Israel, Subaru Israel, and McDonalds Israel [76].

2.17.4 Tension between US and China in 2001

On April 26, 2001, the Federal Bureau of Investigation's (FBI) National Infrastructure Protection Center (NIPC) released advisory 01-009:

"Citing recent events between the United States and the People's Republic of China (PRC), malicious hackers have escalated web page defacements over the Internet. This communication is to advise network administrators of the potential for increased hacker activity directed at U.S. systems. Chinese hackers have publicly discussed increasing their activity during this period, which coincides with dates of historic significance in the PRC…" [118].

The hackers who were known as China Eagle Alliance and PoizonB0x, on the Pacific, defaced the US websites with titles such as "USA Kill" and "China Killer". The cyberattacks characterized by defacements and DoSs from both sides [119], [120].

On April 25, 2001, The FBI investigated the California electric power grid test network a Honker Union of China (HUC) [121]. This case was widely dismissed as propaganda, but the Central Intelligence Agency (CIA) informed the power company in 2007 that not only is a tangible hacker threat to such critical infrastructure possible, it, in fact, but has also already happened. [122], [123].

Combatant against Israeli political, military, telecommunications, media, and universities. The Bank of Israel, e-commerce sites, and the Tel Aviv Stock Exchange sites were targeted sites on which was regards as pure economic sabotage. This kind of warlike many others revealed new tools and tactics. DoS program was used by both sides for the "Defend" [76].

2.17.5 Estonia Hacking On Government and Private Institutions in 2007

Beginning on April 27, 2007, the Estonian government, law enforcement, banking, media, and Internet infrastructure endured three weeks of cyber-attacks. The impact raised concerns from governments around the world [124].

Estonians conduct over 98% of their banking transactions online, the impact of multiple distributed denial-of-service (DDoS) attacks, the two largest banks and all forms of internet communication were interrupted for a prolonged period causing international services disrupted too. The Communication infrastructure attacks on one of the Estonian government's Internet Service Providers (ISPs) disrupted government communications [120].

On the propaganda front, a hacker defaced the Estonian Prime Minister's political party website on April 27, changing the homepage text to a fabricated government apology for having moved the statue, at the side of a promise to restore it back to its original location. The attack has been attributed to Russia though Russia has denied it [76].

2.17.6 Ukraine Christmas Power Outage

Mark Ward, Technology correspondent, BBC News reported that just before Christmas, more than 225,000 Ukrainians who were plunged into darkness when the power company was hacked. On 23 December 2015, in the late afternoon, the attackers remotely gained access to computers in the control centre of power firm Prykarpattyaoblenergo to flip circuit breakers and shut down substations [125].

Security experts investigated a power outage that affected parts of the Ukrainian capital, Kiev, and the surrounding region which has been attributed to cyberattack. Ukraine has suffered two cyber-attacks which caused blackouts [120], [128].

[127] SANS Institute published the following list of the technical components used by the attackers, graphically depicted in Figure 2.7:

1) *"Spear phishing to gain access to the business networks of the Oblenergos.*
2) *Identification of BlackEnergy 3 at each of the impacted oblenergos.*
3) *Theft of credentials from the business networks.*
4) *The use of virtual private networks (VPNs) to enter the ICS network.*
5) *The use of existing remote access tools within the environment or issuing commands directly from a remote station similar to an operator HMI.*
6) *Serial-to-Ethernet communications devices impacted at a firmware level 15*
7) *The use of a modified KillDisk to erase the master boot record of impacted organization systems as well as the targeted deletion of some logs [127]"*
8) *Utilizing Uninterrupted Power Supply (UPS) systems to impact connected load with a scheduled service outage.*
9) *Telephone denial-of-service attack on the call center." [127]*

Figure 2.7: Ukraine Attack Consolidated Technical Components (Credit SANS) [127]

2.17.7 Iranian Stuxnet Worn Attack

Stuxnet is a computer worm that exploits unknown Windows zero-day vulnerabilities to infect computers and spread in the network. Its purpose was not just to infect PCs but to cause real-world physical effects [120]. Specifically, it targets centrifuges used to produce the enriched uranium that powers nuclear weapons and reactors [126]. Stuxnet is a weaponized cyber-attack against an industrial control system [129]. The Stuxnet Worm first emerged during the summer of 2010 [130]. Others claim that it started as far as 2005 [126].

Stuxnet worm was stored on a Universal Serial Bus (USB) drive designed specifically routing out the workings of a nuclear power plant and a virus that slowly multiplied to destroy the nuclear centrifuges by surreptitiously manipulating the rate of spin, while ensuring feedback to operators monitoring the centrifuges reflected nothing amiss [131]. It is reported to have been created as a part of a joint US and Israel project with the aim of disrupting Iran's ability to develop its nuclear capability [132].

Stuxnet was primarily intended to attack only Iranian nuclear facility at Natanz. The facility was not connected to the outside world. That worm was launched using a USB sticks inside by what was believed to be intelligence agents. However, the malware has spread to other systems outside Iran though the internet but the damage has been as it was in Iran [126].

The developers of the worm are up to date unknown [126], but there are other claims that many experts suggest that the Stuxnet worm attack on the Iranian nuclear facilities was a joint secrete operation between the United States and Israel. Edward Snowden, the United States National Security Agency (NSA) whistleblower, said that this was the case in 2013. [132] Despite this speculation, there is still no concrete evidence as to who designed the original cyber weapon.

2.17.8 First Cyber- Attack in Georgia 2008

In August 2008, the Russian Army invaded Georgia. Many, coordinated cyber-attacks accompanied the military campaign. This represents the primary instance of a large-scale Computer Network Attack (CNA) conducted in the wheel with major ground combat operations [123].

The Russian cyber campaign against Georgia started on the seventh August, Russian hackers targeted Georgian news and government websites. Russian Military Forecasting Center official Colonel Anatoly Tsyganok said these first actions were a response to Georgians hacking South Ossetian media sites earlier in the week. The fact that the alleged counterattacks occurred only one day prior to the ground campaign has led many security experts to suggest that the hackers knew about the date of the invasion beforehand. [51].

The DDoS attacks were launched out by botnets. A botnet is a network of computers on the Internet (termed "bots" or "zombies") that have been infected with a piece of software known as malware [169]. The malware allows a computer "command and control" server to issue commands to these bots. Often, botnets launch spam emails [133].

2.17.9 Liberian Cell Phone Network Operator was Shut Down in 2015

Liberian internet access was brought down using the notorious Mirai botnet in 2016. The attacker disrupted internet access through the use of botnets or armies of computers that have been planted with a piece of malware [137]. The attacker who was identified as Kaye was selling access to his botnets so that his buyers could launch a DDoS attack, which can overwhelm a website or internet

provider with too much traffic, forcing it offline. The attacker used the same botnet to attack Deutsche Telekom in Germany [142]. The botnet overwhelmed the internet which resulted in an outage that affected close to a million customers. Germany has offensive and defensive technologies. Though he managed to bring down the services, in February 2017, authorities tracked down and arrested Kaye, in Cyprus where he lived at the time [138].

2.18 Standards and Best Practices

It is important to identify, establish and implement the useful best-practices, standards and guidance for effective cybersecurity. Those should be able interacting with other standards and guidance [139, 140]. Most of the standards are can be customised to any organization regardless of the size or the industry and sector in which they operate [141], [142].

2.18.1 The National Institute of Standards and Framework's Cybersecurity Framework

The Cybersecurity Framework (CSF) is a voluntary framework primarily intended for critical infrastructure organizations to manage and mitigate cybersecurity risks based on existing standards, guidelines, and practices. However, the CSF has proven to be flexible enough to also be implemented by non-US and non-critical infrastructure organizations. The CSF is a living document – it recognizes that continual improvement is necessary to adapt to changing industry needs [141]. As such, version 1.1 was recently released. See Figure 2.1.

2.18.2 ISO/IEC 27001

ISO/IEC 27001 is the international Standard for best-practice information security management systems (ISMSs). It is a rigorous and comprehensive specification for protecting and preserving your information under the principles of confidentiality, integrity, and availability. The Standard offers a set of best-practice controls that can be applied to any organization based on the risks faced and implemented in a structured manner in order to achieve externally assessed and certified compliance.

2.18.3 ISO/IEC 27032

ISO/IEC 27032 standard focuses explicitly on cybersecurity but does not as precise or prescriptive recommend as those supplied in ISO/IEC 27001. This Standard recognizes the vectors that cyber-attacks rely upon, including those that originate outside cyberspace itself. It provides guidelines for protecting your information from external environments. ISO/IEC 27032 matches well with

ISMS simply by updating and expanding the policies, processes and training your organization needs.

2.18.4 ISO/IEC 27035

ISO/IEC 27035 is the standard for incident management and forms the crucial stage of cyber resilience. While cybersecurity management systems are designed to protect your organization, it is essential to be prepared to respond quickly and effectively when something does go wrong. This Standard also includes guidance for updating policies and processes to strengthen existing controls following analysis of the event and minimize the risk of recurrence.

2.18.5 ISO/IEC 27031

ISO/IEC 27031 is the Standard for organizational preparedness for business continuity and a logical step to proceed from incident management, as an uncontrolled incident can transform into a threat to ICT continuity. As part of the profile of a cyber-attack, it is essential that your organization is prepared for a cyber-attack beating your first line of defense and threatening your information systems as a whole.

2.18.6 ISO/IEC 22301

ISO/IEC 22301 is the Standard for business Continuity Management Systems (BCMSs), and forms the final part of cyber resilience. This Standard not only focuses on the recovery from disasters, but also on maintaining access to, and security of, information, which is crucial when attempting to return to full and secure functionality.

2.19 African Union Convention on Cyber Security and Personal Data Protection

The African Union Convention designed the National Cybersecurity Frame Work [143] with focus on the national policy and strategy.

1) **National Policy:** Each state shall undertake to develop, in collaboration with stakeholders, a national cybersecurity policy which recognises the importance of Critical Information Infrastructure (CII) for the nation identifies the risks facing the nation using the all hazard approach and outlines how the objectives of such policy are to be achieved [144], [164].

2) **National Strategy:** State parties shall adopt the strategies they deem appreciate and adequate to implement the national cyber security policy, particularly in the area of legislative reform and development, sensitization and capacity building, public-private

partnership, and international cooperation, among other things. Such strategies shall define organizational structures, set objectives and timeframes for successful implementation of the cybersecurity policy and lay the foundation for active management of cyber security incidents and international cooperation [145], [146].

2.20 SADC Cybersecurity

The Southern African Development Community (SADC) Secretariat to continue promoting capacity building initiatives relating to cyber security [165]; The SADC Secretariat urged to develop a list of harmonized indicators to measure progress in cyber security commitment of all SADC Member States and to include these indicators under the SADC ICT Observatory; The SADC Secretariat urged to develop a SADC Model Cyber Security Strategy that would be utilized by SADC Member States in developing their own National Cyber Security Strategy [143].

2.21 National Laws, Regulations and Policy

Information and communication technologies (ICTs) are increasingly important in achieving development goals and promoting citizen participation [154]. Zambia is one of a member of countries in the Southern African region that have sought to include ICTs in their national development plans [149]. The Government of the Republic of Zambia since the re-emergency of development planning in 2003, has implemented three National Development Plans (NDPs) namely Fifth National Development Plan (FNDP), Sixth National Development Plan (SNDP) and its revised version the Sixth National Development Plan (R-SNDP). These Plans are all building blocks to actualising the Vision 2030 of becoming a prosperous middle-income country. The Seventh National Development Plan (7NDP) covering the period 2017-2021 is the successor to the R-SNDP following its expiry in 2016. It builds on the achievements and lessons learnt during the implementation of the previous NDPs [10].

The architecture of the ICT Policy in Zambia is premised on three core thematic areas and thirteen pillars. The three core areas are 1) capacity building, 2) a competitive and efficient ICT sector, and 3) an effective legal and regulatory framework [148]. The thirteen pillars of the ICT policy are outlined in Table 2.2 below which summarises the roadmap for the policy.

The national ICT Policy is aligned to the following vision statement, *"A Zambia transformed into an information and knowledge-based society and economy supported by consistent development of, and pervasive access to ICTs by all citizens by 2030"* [10].

Table 2.2: The Roadmap for the Policy Source: Ministry of Transport and Communications [10], [11]

Pillar	Objectives
Human Resource Development	To attain sufficient and world-class human resource capacity in critical and relevant ICT skills required for developing and driving Zambia's Information and knowledge based society
Agriculture	To improve productivity as well as competitiveness of the agricultural sector through the use of ICTs.
Education	To integrate ICTs in the education systems and nations' research and development (R&D).
Health	To improve access to quality healthcare as close to the family as possible through the deployment and exploitation of ICTs.
Youth and Women	To leverage the use of ICTs to mainstream youth and women issues in all activities of the economy and society.
Tourism	To integrate ICTs in the development of the tourism industry and facilitate the conservation of Zambia's natural resources and heritage.
Telecommunication Infrastructure	To increase access and promote widespread deployment of ICT services through the expansion of the national telecommunication infrastructure
e-Government	To improve public sector management as well as efficient and effective delivery of public goods and services.
e-Commerce	To promote Zambia's full and effective participation in national, regional and global trade.
Legal and Regulatory Framework	To develop appropriate institutional, legal and regulatory systems in order to support the development of a competitive local ICT sector.
Security in Information Society	To safeguard national, institutional and individual security concerns.
Access Media, Content and Culture Heritage	To promote public access to information and promote the national cultural heritage.
ICT Services	To develop a competitive local ICT industry

2.22 Legal and Regulatory Framework

During the 20th century, technological advances brought about the convergence of telecommunications and computer technologies. This signified the beginning of an era known as

the information age. The information age is characterized by the rise of digitalization which basically implies a technological shift from analog and electro-mechanical technologies to digital technologies [156]. A very distinctive feature of the information age is the continuous integration of computer and digital communications technologies in virtually all aspects of life and critical services that support modern societies and the tendency towards "connecting everything to everything". This has given rise to the emergence of the information society. However, the emergence of the information society as a result of the integration of computer and digital communications technologies in all aspects of life has also redefined traditional notions of security. The security of digital data, computers, digital communications technologies and information networks now have an overwhelming influence on almost all aspects of life and society including the global economy [166]. Thus, with the emergence of the information society, malicious conducts against information systems such as computer systems and networks now have the potential of affecting individuals, countries and the global economy in ways previously unimagined. The most critical challenges of the information society have been the security of digital data and information systems and the prevention of the malicious misuse of information communications technologies by criminals, terrorist groups, or state actors [159], [160]. Measures to address these security challenges of the information society have given rise to a new concept known as "cybersecurity". Cybersecurity seeks to promote and ensure the overall security of digital information and information systems with a view to securing the information society. Thus, the concept is broadly concerned with social, legal, regulatory and technological measures that will ensure the integrity, confidentiality, availability and the overall security of digital information and information systems in order to achieve a high degree of trust and security necessary for the development of a sustainable information society [11].

The National Development plan has lead into the enactment of regulatory and legal frameworks which has evolved in the process. The need to develop the bills became inevitable for the nation to regulate and provide a safe cyberspace [162], [163].

2.22.1 Computer Misuse Act 2004

[111] Zambia acknowledged the need for legislation of the use of cyberspace and this was brought to the fore with heavy lobbying by the banking sector with help of Computer Society leading to a Cybersecurity law the computer misuse act that was passed in 2004. However, some critics were

concerned that the law, if adopted, could be used to curb access to the internet. The bill was passed quickly through parliament without much debate due to a suspected case of lack of understanding. [149]

2.22.2 Electronics and Communications Transaction Acts Act No. 21 of 2009

An Act to develop a safe, secure and effective environment for the consumer, business sector and the Government to conduct and use electronic communications; promote legal certainty and confidence, and encourage investment and innovation, in the electronic communications industry; facilitate the creation of secure communication systems and networks; establish the Central Monitoring and Coordination Centre and define its functions; repeal the Computer Misuse and Crimes Act, 2004; and provide for matters connected with or incidental to the foregoing.

The Act, does not offer strategic direction and does not provide a frame or which best practices to adopt. There has been a lot of advancement in technological innovations which to some extent render the current act not effective.

2.22.3 Information and Communications Technologies [No. 15 of 2009 199]

An act to continue the existence of the Communication Authority and renamed it as the Zambia Information and Communication Technology Authority; prove for the regulation of the information and communication technology; facilitates access to information and interests of services providers and consumers; repeal the Telecommunications Act, 1994 and to provide for matters connected with or incidental to forgoing [149].

2.22.4 Cyber security and cybercrimes Bills 2017

The parliament ministerial statement, with regard to the review of the excising legal framework, the Government is in the process of unbundling the Electronic Commutations and Transaction Act, No. 21 of 2009 into five distinct legislative Acts to be proposed to Parliament enactment, namely; the e-Government Bill; the Cyber Security Bill; the Data Protection Bill; the e-Transactions and e-Commerce Bill; and Cybercrime Bill which is a penal law that will be used to prosecute cybercrime offences.

The Government will further propose to Parliament to adjust and update the Information and Communications Technology Act No. 15 of 2009, in order to strengthen the regulatory mandate assigned to Zambia Information and Communications Technology Authority (ZICTA) and provide

the institution with clear enforcement capabilities for execution of statutory rules and procedures outlined in the Act [13].

An ACT to authorize the taking of measures to ensure cyber security in Zambia; establish the Zambia National Cyber Security Agency and provide for its functions; protect victims against cybercrime; provide for Child Online Protection; provide Information and Communication Technology user education on cybersecurity and develop local skills in cyber security; facilitate identification declaration and protection of critical information infrastructure; repeal certain provision in the Electronic and Communications Transactions Act No. 21 of 2009; provides powers to investigate and prevent cybersecurity incidents; criminalize offences against computers and network related crime; provide for investigation and collection of evidence for computer and network related crime; provide for the admission of electronic evidence for such offences; and provide for matters connected within or incidental ton the foregoing [13].

2.23 Chapter Summary

This chapter has analyzed some of the literature on cyber warfare and further studied Zambia's Information and Communications Act of 2009 and National ICT Policy. It also reviewed the United Nation Cybersecurity agenda. The chapter reviewed some of the cybersecurity frameworks or mode that are being used by many nations and business for information and network security. It further analyzed specific cases of developed and developing countries in relation to how they have fared protecting critical infrastructures and services.

CHAPTER THREE

3.0 METHODOLOGY

The methodology that was used through this research work was essentially an examination through literature searches and the analysis of the primary data collected from the field through questionnaires. The data source did contribute to the objectives resulting in conclusions and recommendations being drawn from the critical analysis of the collected data.

3.1 Research Design

An explanatory design was used in the study. The study aimed at collecting information to describe the existing situation and attempts to find solutions to the challenges and develop a cyber-attack preparedness framework for Zambia. The researcher used both primary and secondary data. The Primary data was obtained using questionnaires while secondary data was collected from the internet, journal, books, ministerial statements, and published books. The questionnaire was used to collect both qualitative and quantitative descriptive data.

3.2 Study Area or Site

The study was carried out in Lusaka, Zambia. Purposive sampling was used in the selected institutions within Lusaka District as the study site since it has the largest number of infrastructure and service providers in Zambia. In Lusaka, Lusaka District was purposively selected as the study location because it is the capital city and is the central administration of many organisations. This was because the district is the largest area in Lusaka Province with a covered with public and private industries, number of commercial service providers and key infrastructures connected to a larger population. Lusaka is known to have the largest population and headquarters of these operations.

The selected identified organisations included, Zambia National Data Centre, Smart Zambia, Zambia Information and Telecommunications Authority, Zambia Telecommunications Company, Bank of Zambia, Bankers Association, National water and sanitation council of Zambia, Zambia Air Force, Zambia Police, Lusaka Water and Sewerage Company, Energy Regulations Board, KPMG, PWC and others.

3.3 Study Population

Population in this case refers to the total number of respondents that were selected to participate in this study. The population comprised of specialists and employees of Zambia National Data Centre, Smart Zambia, Zambia Information and Telecommunications Authority, Zambia Telecommunications Company, Bank of Zambia, Bankers Association, National water and sanitation council of Zambia, Zambia Air Force, Zambia Police, Lusaka Water and Sewerage Company, Energy Regulations Board, KPMG, PWC and others.

3.4 Study Sample

The sample study included Chief Information Security officers, information security professionals, Cybersecurity professionals, Network Administrators, IT Auditors, Computer Engineers, End Users and other related professionals who are directly involved in administration and management cybersecurity. One hundred and fifty questionnaires were circulated to organisations and individual professionals.

3.5 Sampling Techniques

The researcher used a purposive sampling technique to selected targeted respondents believed to be reliable for the study.

3.6 Instruments for Data Collection

The instruments that were used in the collection of data included a self-administered questionnaire, internet, cell phone, pen and notebook. The researcher used a structured questionnaire in the study. The questionnaire was left with both open-ended and closed-ended questions.

3.7 Procedure for Data collection

Data Collection for the study were primary and secondary collections. Primary data was the information gathered directly from the respondents through questionnaires, and interviews from the questionnaire. Secondary information was found from the internet, journals, conferences, ministerial statements and books. Other sources were document reviewed such as essential material like weekly, monthly, quarterly and annual audit information systems audit reports.

3.8 Data Analysis

Microsoft Office package (Excel) was employed in the research in order to aid in the analysis and interpretation of data. This software did make it easier to analyze the various variables and also facilitated the presentation of information in the form of bar chart, and percentages. The program was preferred because:

1) It is user friendly.
2) The researcher has had some knowledge on how to use the package.
3) It has enough memory capacity for a long range of numbers.
4) Easy to process and quantify information

Questions on the questionnaire had to be coded in order to process the pieces of information and quantifying the data by using Excel package. This facilitated the analysis of data and for presentation purposes. Excel is also user friendly and useful for data analysis.

3.9 Research Methodology Chart

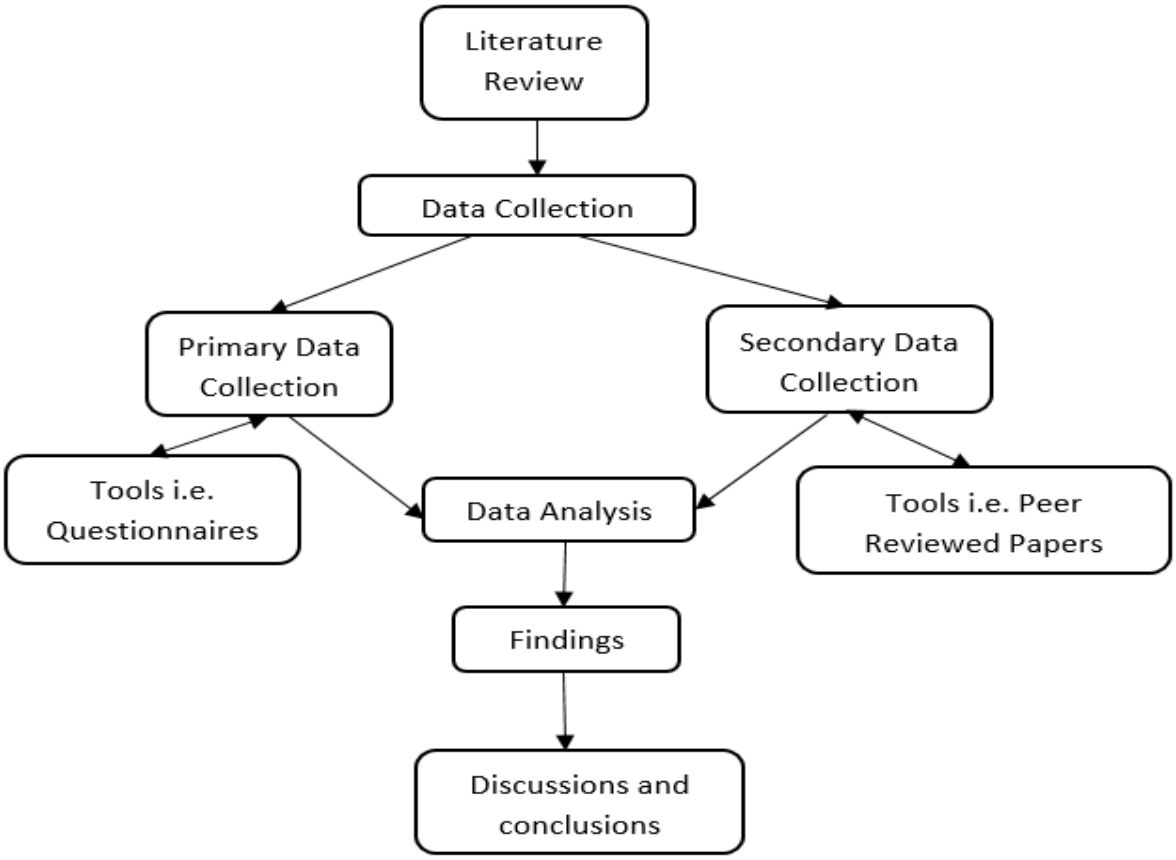

Figure 3.1: Research methodology chart [150]

3.10 Limitation of Study

1) Some institutions never responded and did not answer the questionnaire because their institution has a policy of nondisclosure for whatsoever purpose if it not for their benefit.
2) Some respondents unnecessarily took long in answering the questionnaire. This delayed the whole process of data collection and analysis.
3) Some institutions have restricted access to their premised and which very often was a challenge to meet respondents.
4) Bureaucracy was another issue, some authorities were not available hence there were no approvers to allow the researcher to conduct the survey.
5) Copies were not handled properly, some got lost and re-printing became a cost.

3.11 Chapter Summary

This Chapter dealt with the methods that were employed in the collection of data. The research used a mixed method approach in order to get the benefit of both the qualitative and quantitative design. It showed how the methodology used would address the issues raised in the research questions. It further highlighted the instruments that were used during the data collection and also reviewed some of the limitations that were encountered during process.

CHAPTER FOUR

4.0 RESULTS AND ANALYSIS OF FINDINGS

This chapter gives a systematic presentation of the data collected, the findings, analysis and interpretation of the research results. Data collection for this study was done using a structured questionnaire, which was distributed to different companies in Lusaka. Particularly, the study focussed on a sample population selected from the Health - 2%; Consumer Products and Services - 16%; Manufacturing, Mining, Construction and Engineering - 4%; Government (Regulator, Law enforcement, Defense) - 23%; Energy (Oil, gas, power, utility) - 4% ; Telecommunications (ICT, ISP, Software, Telecoms) - 34% industries as well as those in the banking and financial sector - 2%.

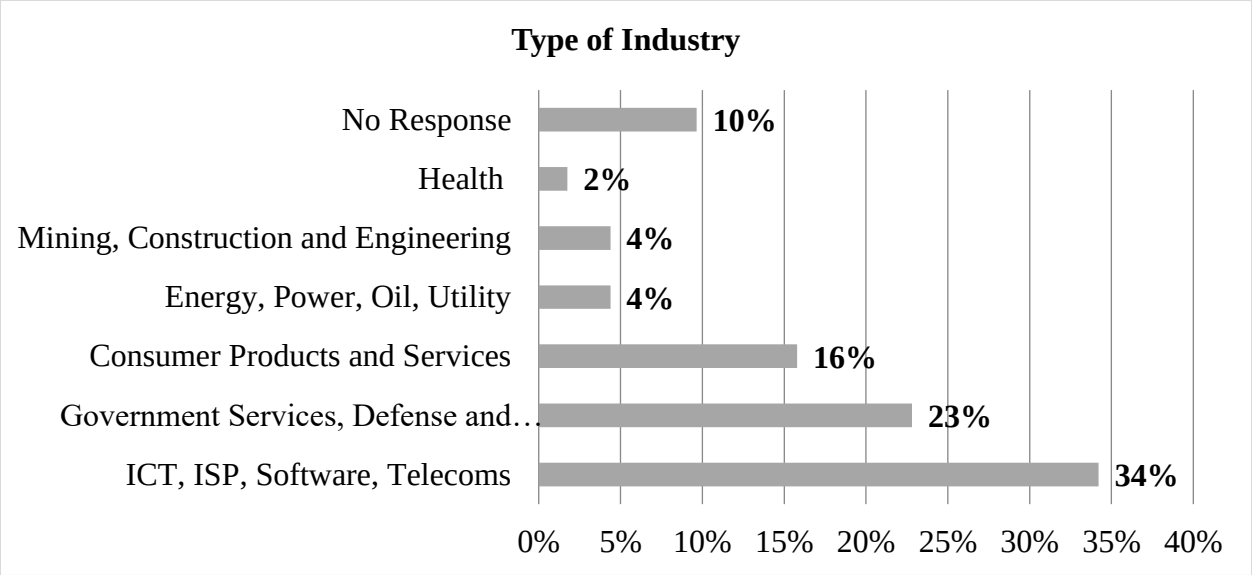

Figure 4.1: Type of industry

Analysis and presentation of findings for the study were done using Microsoft Excel. The presentation of findings of this study in this section were organized according to the following specific objectives:

1) To identify the nature and the forms of cyber-attacks.
2) To evaluate the existing strategies used in preventing cyber-attacks.
3) To develop a framework that can be used to curb cyber-attacks.

4.1 Descriptive Statistics

This analysis of demographic distribution for the respondents was done in order to have a general picture of the characteristics of specialists and experts whose views were put in this study.

4.1.1 Gender and Age Distribution

One hundred and fifty (150) questionnaires were distributed among the selected population sample. One hundred and fourteen questionnaires were successfully filled in translating to 76% response rate. Among the respondents interviewed were IT specialists, IT Auditor, Cybersecurity Professionals, Chief Information Security Officers, and among computer users among which 74.6% of the respondents were male while 25.4% were female respondents. See fig 4.2 below.

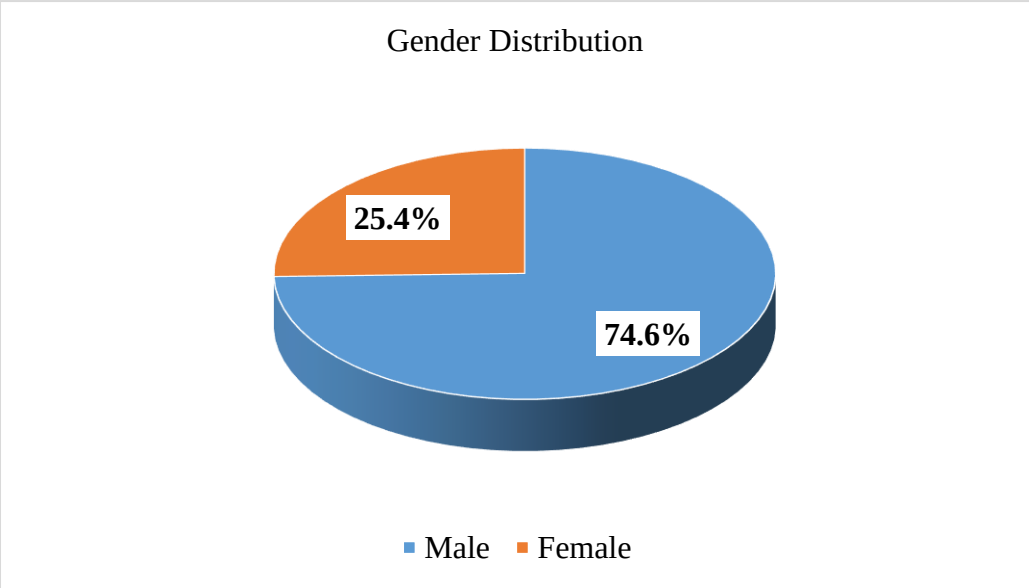

Figure 4.2: Gender Distribution

Further, respondents that were interviewed formed a normal distribution with majority of the respondents in excess of 41.2% falling in the age category of 26-35 years, followed by the 36-45 years age group that were in excess of 37.7%. The least of these age groups were the 15-25 years and the 46 years and above category with 9.6% and 11.4% respectively. See fig 4.3 below.

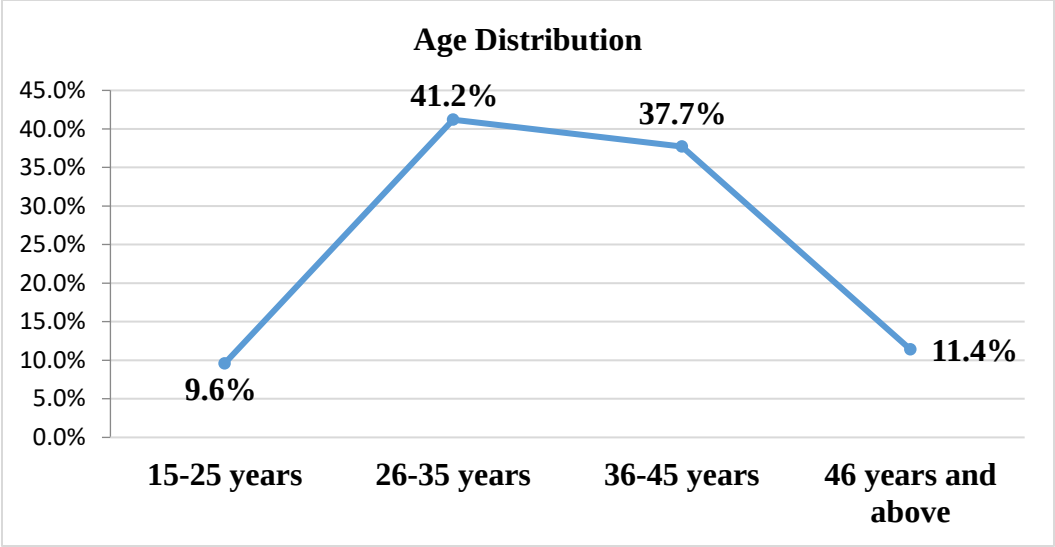

Figure 4.3: Age Distribution

4.1.2 Education Qualification, Position Level and Years of Service

Regarding the education qualification of the respondents that were interviewed in this study, 57% of the respondents had a degree qualification while 32.5% had masters. Further, 7.9% of the respondents had a diploma as their highest education qualification. Only 1.8% of the respondents had a mere certificate or other related qualifications as their highest qualification. See fig 4.4 below for a detailed illustration of the education qualifications, indicating that majority of the respondents had sufficient qualifications to be able to give reliable information on the subject under study.

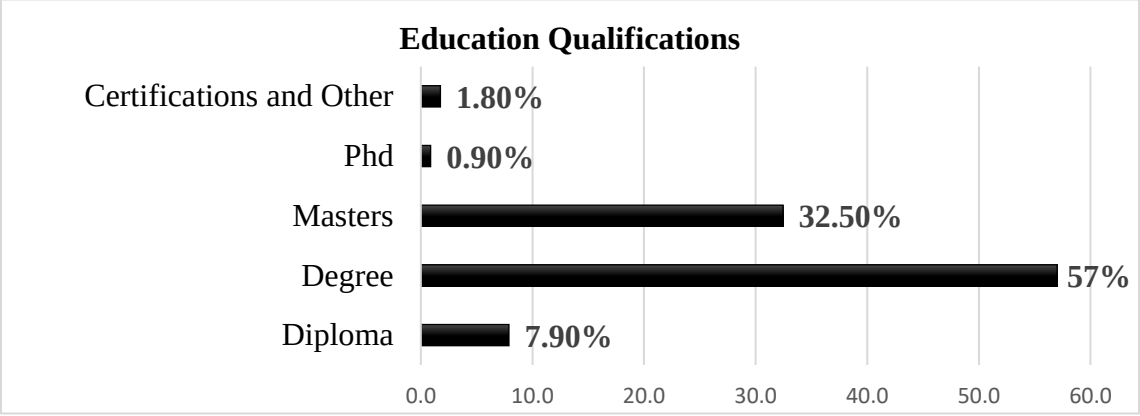

Figure 4.4 Education Qualification

Further, among these respondents, majority of them in excess of 62.3% were in management positions in their work places, while the rest in excess of 37.7% were in lower positions within their Organizations. In terms of years of service in their various institutions, 39.5% had only worked for three years or less in their Organizations while 37.9% of the people had worked for more than three years in these institutions. See fig 4.5 below for detailed statistics of the years of service for individual respondents that were interviewed.

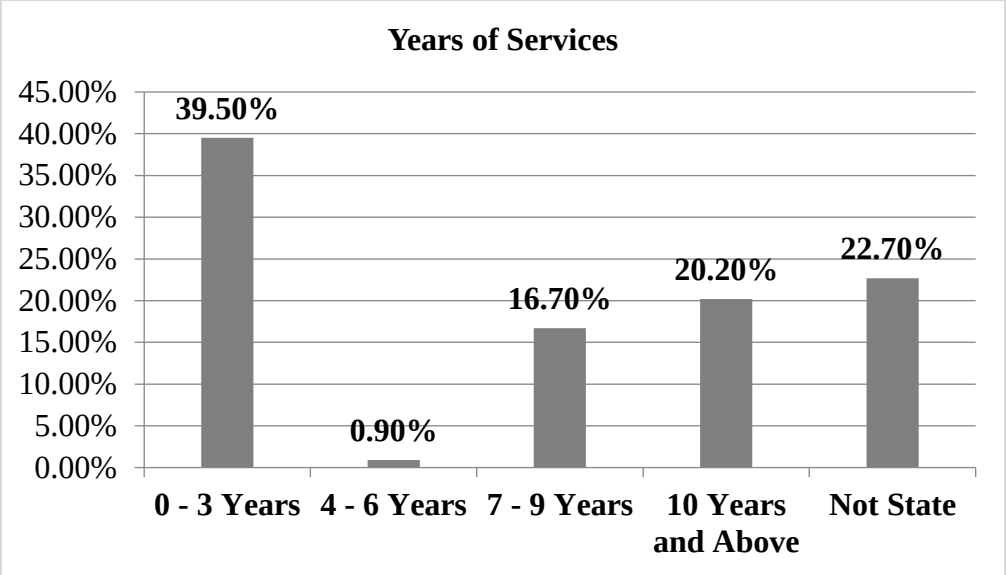

Figure 4.5: Years of Service in individual workplaces

From the above descriptive analysis of the demographic characteristics of the respondents, it is apparent that majority of the respondents had sufficient education, as well as work experience to be able to understand and explain the dynamics of cyber security in their respective workplaces.

4.2 Identifying Nature and Forms of Cyber-attacks

One of the specific objectives of this study was to identify the nature and forms of cyber-attacks that people had experienced in their organization. However, before delving into the actual nature and forms of cyber-attacks, the study sought to establish the level of awareness for such threats among the different Organizations under study.

4.2.1 Organizational Awareness of Cyber-attacks

Findings of this study revealed that all the institutions under study were aware of the cyber-attacks. Further, that majority of the respondents in excess of 77.2% had indicated that their managers had placed high priority on cyber security. However, in spite of this seemingly positive outlook, the authorities in the various Organizations had taken the vice lightly. This is demonstrated by the

levels of information-seeking behaviour of these organizations in as far as advice and guidance on cyber security is concerned.

4.2.2 Information, Advice or Guidance on Cyber Security

From the findings, only 50% of respondents that indicated that their Organization had sought information, advice or guidance on the cyber security threats in their Organization in the previous 12 months. The rest either had not sought for such information or were not so sure whether their Organizations had sought for such information or not. See Figure 4.6 below for detailed findings on Organizations seeking information on the cyber-attacks.

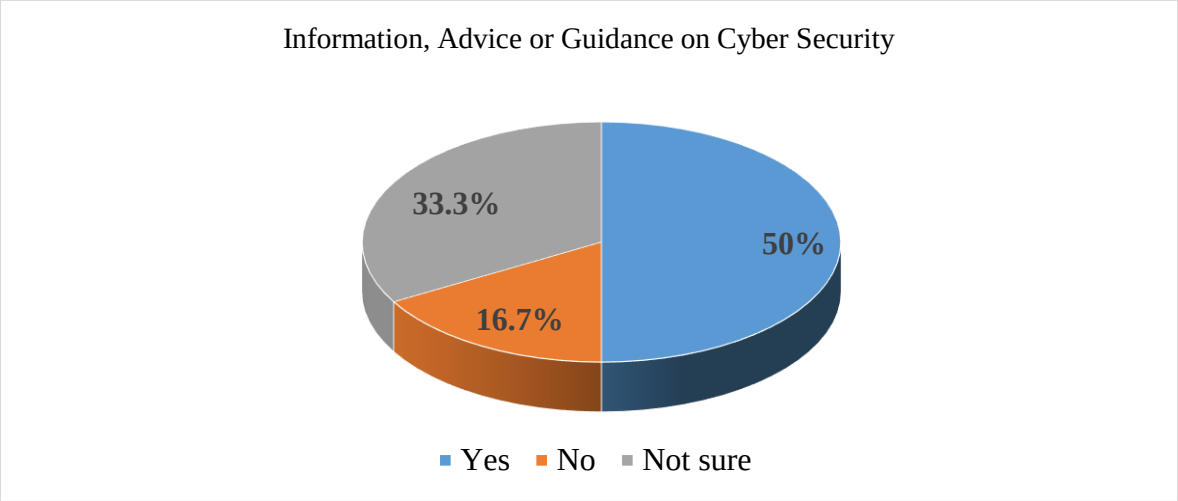

Figure 4.6: Information, Advice or Guidance on Cyber Security

4.2.3 Nature and Forms of Cyber Attacks

Findings of the study revealed a number of cyber-attacks forms had been experienced in a number of institutions with the most common forms of cyber-attacks being fraudulent emails or data being directed to fraudulent websites, with 55.3% of the respondents indicating that they had experienced it. Further, 48.2% of the respondents indicated that they had experienced attacks in form of Spyware, Malware or Ransomware.

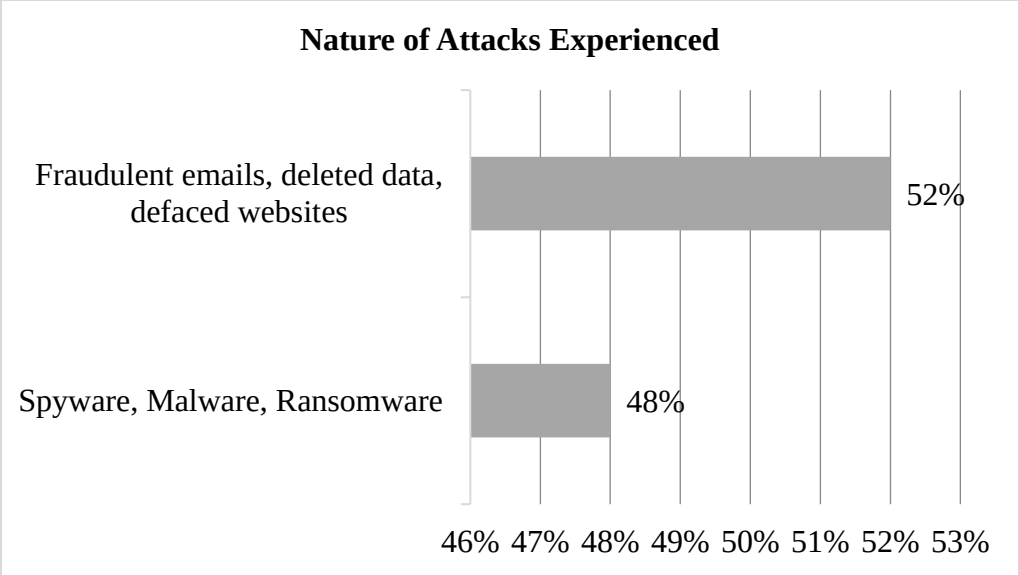

Figure 4.7: Nature and forms of cyber-attacks

Other common forms of cyber-attacks reported or experienced in the organizations from which the study was conducted include: Hacking of online bank accounts, denial-of-service attacks, impersonating organization in emails, viruses, unauthorised use of computer networks or servers by outsiders, unauthorised manipulation of customer records, and other breaches.

4.2.4 Frequency of Attacks

In terms of the frequency of such security breaches in the past 12 months, the study established that 0.9% indicated that such attacks happened every day, while 2.6% of the respondents indicated that such attacks took place once every week. However, majority of the respondents in excess of 16.7% indicated that such breaches happened at least once every year, followed by 12.3% who indicated that the breaches happened less than once a month in their Organizations. Furthermore, 62.3% of the respondents indicated that they were know of any cyber-attacks or breaches in their organisations.

How often in the last 12 months, did you experience cyber security breaches or attacks?

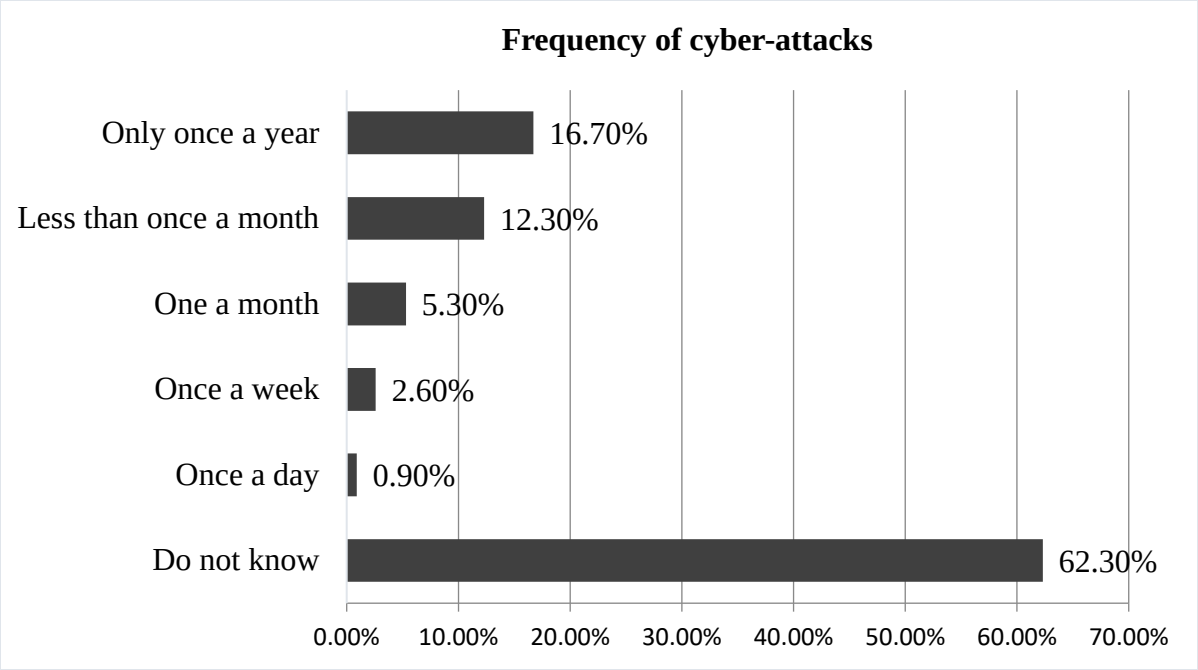

Figure 4.8: Cybersecurity breaches

4.2.5 Effects of Cyber Attacks

The study established that such security breaches and attacks had resulted in the following:

1) Fraudulent emails and data being directed to fraudulent websites.
2) Loss of revenue or money.
3) Lost or stolen assets, trade secrets as well as intellectual property.
4) Temporary loss of access to files or networks.
5) Permanent loss of files.
6) Software or systems corrupted or damaged.
7) Website or online services taken down or slowed.

Further, in terms of the Organization itself, the following were the impact of such cyber-attacks:

8) Staff members stopped carrying out daily work, thus preventing the efficient and effective provision of goods and services.
9) Complaints from customers increased in number. This required that the Organization to do goodwill compensation to its customers.
10) There were fines and legal costs that the institutions had to make.
11) There was loss of revenue and share value.

12) Lost man hours during the time of clearing the breaches and attacks.
13) The Organization needed to come up with new measures in order to deal with any possible future attacks.
14) There was communication breakdown both within and without the Institutions due to these cyber-attacks.
15) The effects on the operations of the Organization further resulted in reputational damage of institutions.

4.2.5 Recovery Period

Regarding the most disruptive breach, or cyber-attack, it took different periods for different Organizations to address the problem and restore their normal operations upon identifying the breach. Only 10.5% of the respondents indicated that it took no time at all to restore business back to normal operations upon identifying the attack. 23.7% of the respondents indicated that it took the whole day to restore operations to normalcy while the rest of the respondents in excess of 15.8% indicated that it took either a week or more to restore normal operations. However, 50% of the respondents did not even know how long it took the Organization to restore operations from the time the breach was identified. See fig 4.9 below for detailed illustration of this finding.

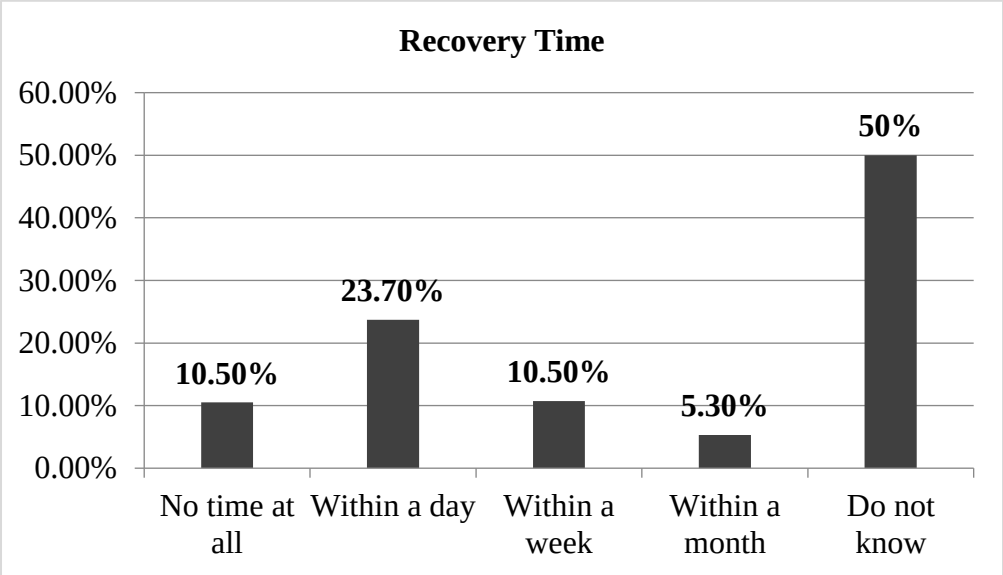

Figure 4.9: Time taken to restore business to normal operations upon identifying the breaches

4.3 Existing Strategies in Preventing Cyber attacks

In order to establish appropriate framework meant to curb cyber-attacks it was also important to outline and analyse the existing strategies that Organizations are currently using. One such strategy that was analysed was the existence of formal policies or documents for cyber security risks.

4.3.1 Availability of Formal Policies Dealing with Cyber Security

From the findings of the study, 63.2% of the respondents revealed that their organizations had formal polices and documents dealing with cyber security risks. 14% of the respondents stated that they had no formal policies or documents dealing with such, while 22.8% were not sure whether such policy documents were available in their Organizations or not. See Figure 4.10 below for detailed illustration of institutions with cyber security policy documents.

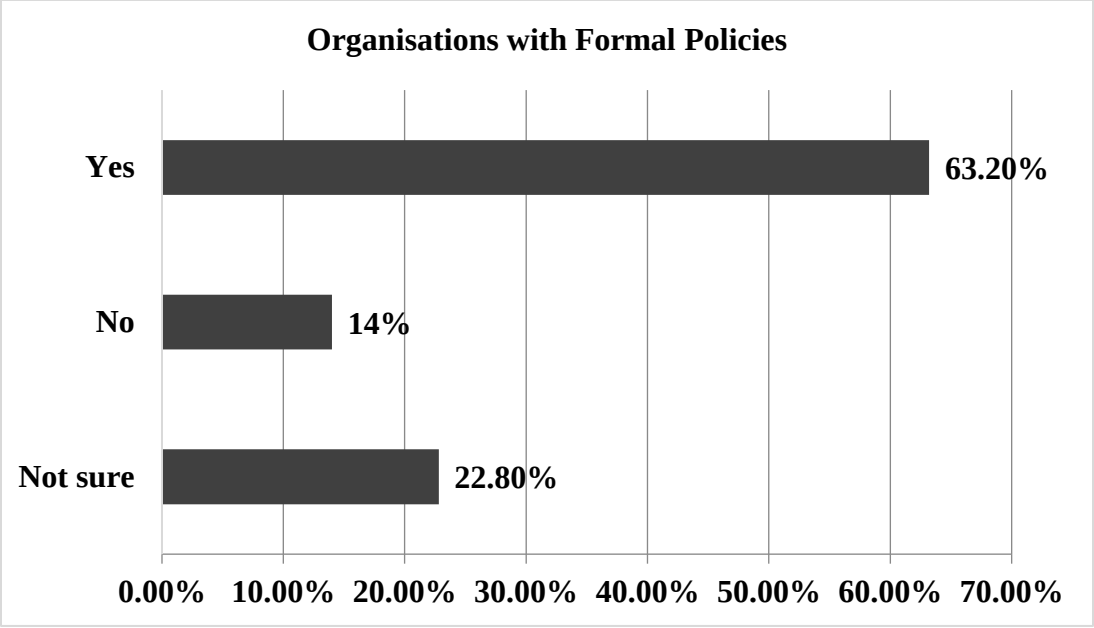

Figure 4.10: Organizations with formal policies or documents for cyber security risks in any way

4.3.2 Issues Covered in the Cyber Security Policies

In terms of those with policies on cyber security risks, the following are the major available policies that are being used in these institutions:

1) Devices Remote or mobile working.
2) Document management systems.
3) Use of new digital technologies such as cloud computing data classification.

4) Restrictions in the use of personally owned devices such as USB sticks.
5) Restrictions on what staff are permitted to do on the IT system of their organization
6) What can be stored on removable devices (example USB sticks).

4.3.3 Rules and Controls

The study revealed that in order to identify cyber security risks, the following activities have been undertaken within these Organizations:

1) Ad-hoc health checks or reviews beyond regular processes;
2) Internal and external audit;
3) Business-as-usual health checks that are undertaken;
4) Risk assessment covering cyber security risks;
5) Invested in threat intelligence to your organization;
6) SMS blasts to customers warning them against fraudsters

Further, the following rules and control systems were put in place in order to enhance the security systems against cyber-attacks.

7) Access/Role based rules where access was only allowed via company owned devices.
8) Applying software updates when they are available
9) Up-to-date malware protection;
10) Ensure the Firewalls available are with appropriate configuration;
11) Restricting IT admin and access rights to specific users;
12) Backing up data securely via other means;
13) Guidance on acceptably strong passwords;
14) Security controls on company owned devices (example laptops)

4.3.4 Establishment of Cyber Security Departments in the Institutions

Regarding established cyber security departments within the Organizations under study, findings revealed that 16.9% of the respondents indicated that they had cyber security departments in their Organizations, while only 25% indicated that they did not have such departments in their Organizations. Only 33% of the respondents were not sure about the existence of such departments in their Organizations. See Figure 4.11 below for detailed illustration of institutions with established Cybersecurity or information security department.

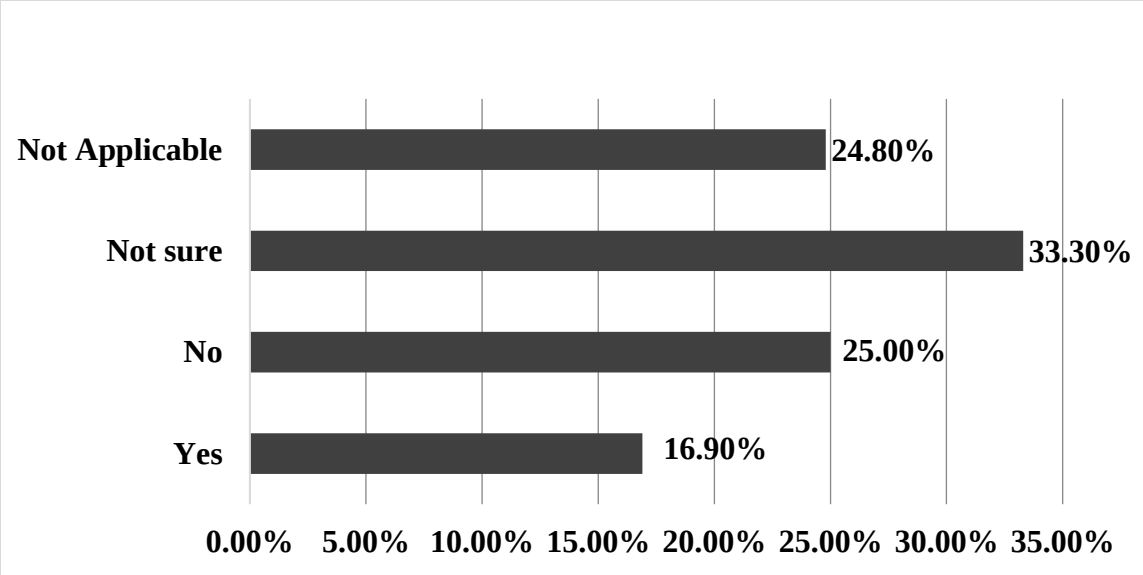

Figure 4.11: Do you have an Information/Cyber Security Department in your Organization?

Among those Organizations that had established the cyber security department, 17% of the respondents indicated that they had a total number of less than 5 members of staff in their cyber, 66% indicated that the number of the staff is 6-10, 5% indicated that staff head count is 11 and above, while the rest were not sure off the number of the staff in the security department. See Figure 4.12 below for detailed illustration of institutions.

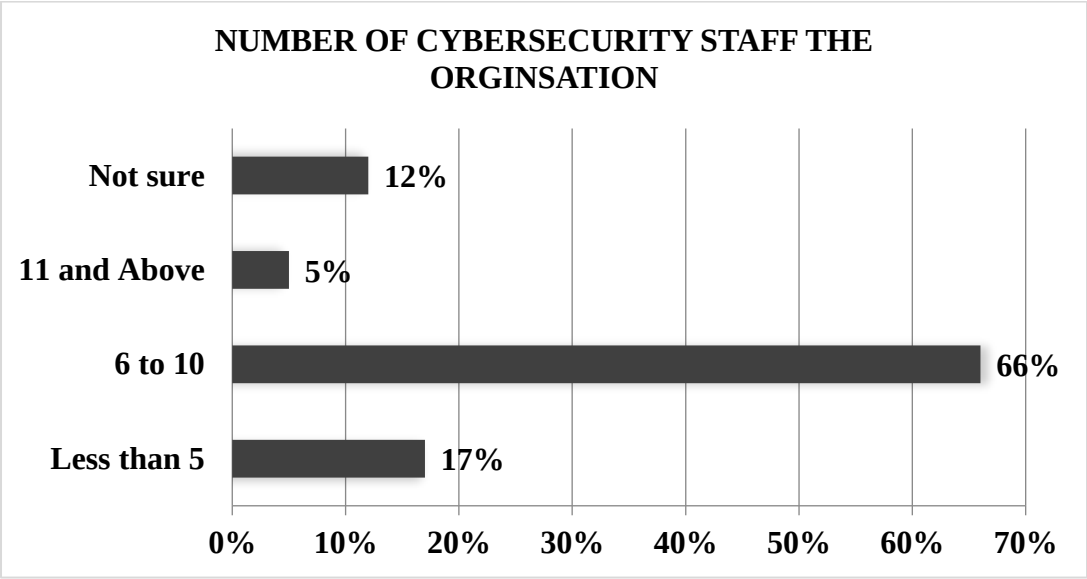

Figure 4.12: Number of Cyber security staff in your organization Information/Cyber Security Department in the Organization

4.3.5 Training on Cyber Security

When asked about the knowledge and skills of the people dealing with cyber security in these Organizations, 48.2% of the respondents agreed, or strongly so, that people dealing with such in their Organizations had the necessary skills and knowledge to effectively do the job. Only 21% indicated that the people dealing with cyber security matters in their organizations did not have the requisite skills to do this job effectively, while 15.8% of the respondents remained neutral regarding the knowledge and skills of the people dealing with issues of cyber security in their Organizations. See Figure 4.13 Right Skills and Knowledge on cyber security.

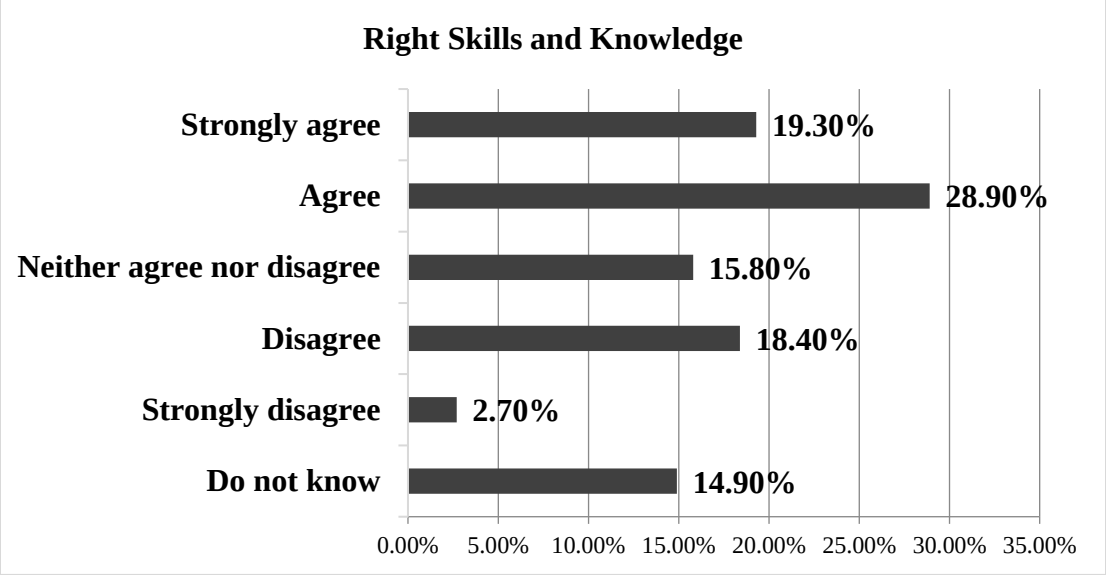

Figure 4.13: Whether people dealing with cyber security have the right skills and knowledge to do this job effectively.

When further asked whether any of their staff members had attended cyber security in the previous 12 months, only 43.9% indicated that staff from their institutions had attended any such training. 28.9% stated that there was no such training attended to by any of their staff members, while 27.2% of them were not so sure, whether any staff members had attended. See Figure 4.14 Training and skills on cyber security.

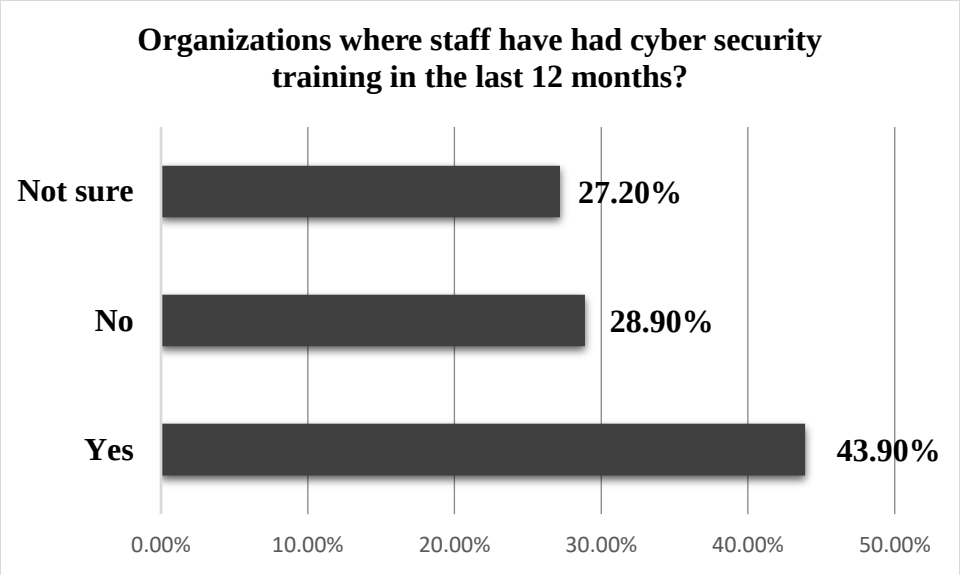

Figure 4.14: Organizations where staff have had cyber security training in the last 12 months.

This result about the people getting training on cyber security, combined with the one on skills and knowledge of the people dealing with cyber security in these organizations showed consistency, and reveals the fact that generally, Organizations were doing very little to ensure that there is qualified and skilled manpower to effectively handle the cyber security in their Organizations.

When asked if the organisation had enough and trained staff dealing with cyber security in the organisation to effectively manage the risks. 48.2% of the respondents agreed, 26% indicated organizations did not have enough and trained staff dealing with cyber security in the effectively manage the risks, while 15.8% of the respondents remained neutral regarding the knowledge and skills of the people dealing with issues of cyber security in their Organizations. See Figure 4.15 Training and Skills on cyber security.

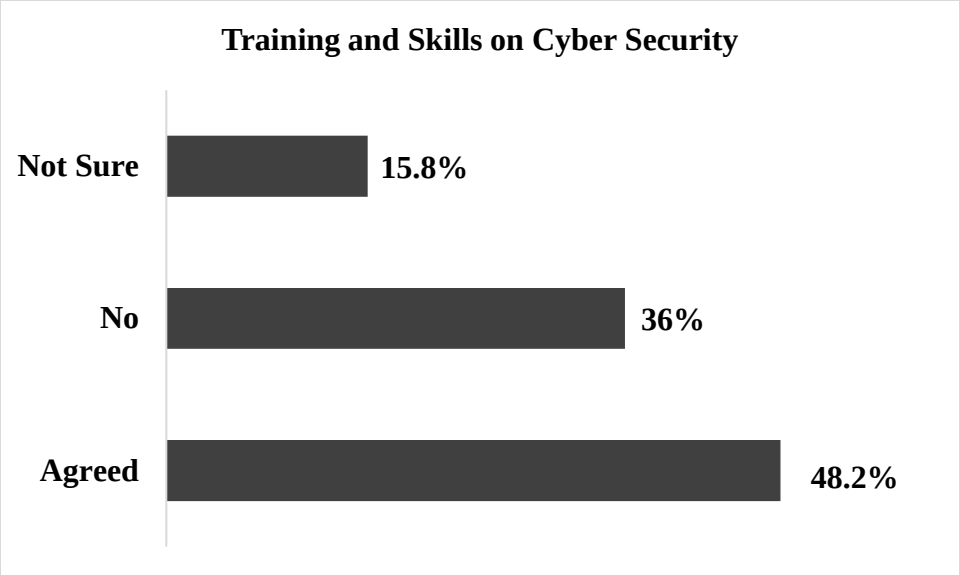

Figure 4.15: Training and skills on cyber security

4.3.6 Personnel Trained in Cyber Security

Of those that had had cyber security training, the study revealed that the highest number of staff trained in Cyber security were those from Information Technology Departments (IT staff) in excess of 39.5%, while the least number of cyber security trained staff were from other staff with 11.1%. Results further revealed that 16.1% of the Directors, and 33.3% of Cyber/information security staff in the institutions under study had received training in cyber security. See figure 4.16 below for detailed illustration of the findings.

Ideally, it would be expected that the highest number of people trained in cyber security are those in the cyber security department. However, contrary to this expectation, results reveal that this department has a lower number of people that received training in cyber security in as far as the institutions under study are concerned. Given that, results revealed that the majority of respondents in excess of 72.8% indicated that they have cyber security departments; this abnormally could be an indication that most Organizations have misplaced their training priorities in other departments that are not cardinal in ensuring cyber security in these institutions, while ignoring the critical department such as the Cyber Security department itself.

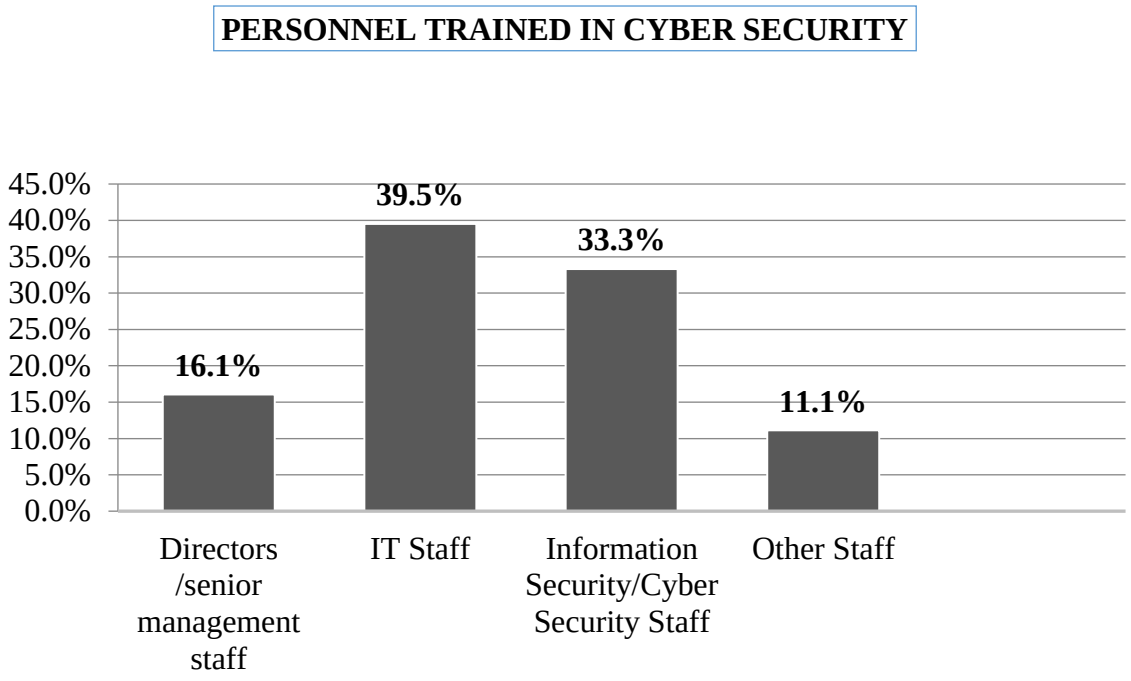

Figure 4.16: Personnel trained in Cyber Security

4.3.7 Reporting and Responses to Cyber Security Attacks

Asked whether respondents were aware of the presence of any reporting procedure in case of any suspicious, or cyber security breach in their organization, only 16.7% of the respondents indicated that they were aware of any such procedure, while 7% of the respondents were not aware of any such reporting procedure in their Organization. However, majority of respondents in excess of 76.3% were not even sure of the existence of such procedures in their Organizations. Figure 4.17: for detailed illustration of the results.

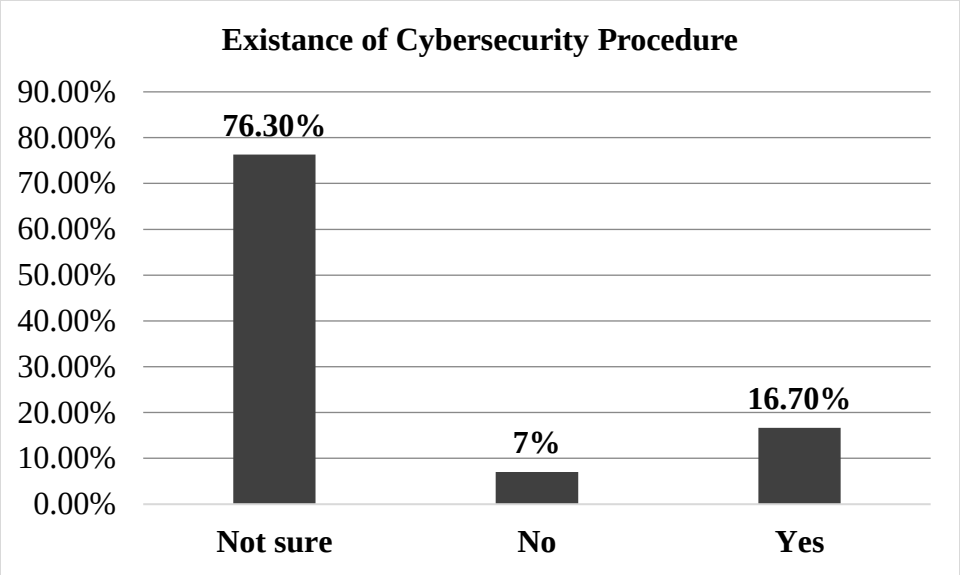

Figure 4.17: Do you have or aware of the reporting procedure of any suspicious or cybersecurity breach in your organization?

However, even though most of these Organizations lacked the reporting procedures largely, results revealed that 40.4% of the Organizations under study have a cyber-security emergency response team, which is responsible for any unforeseen emergency cyber-attacks within the Organizations. Further, that 30.7% did not have this cyber security emergency response team, while 28.9% were not sure whether such a team was available in their Organization. See Figure 4.18 below for detailed illustration.

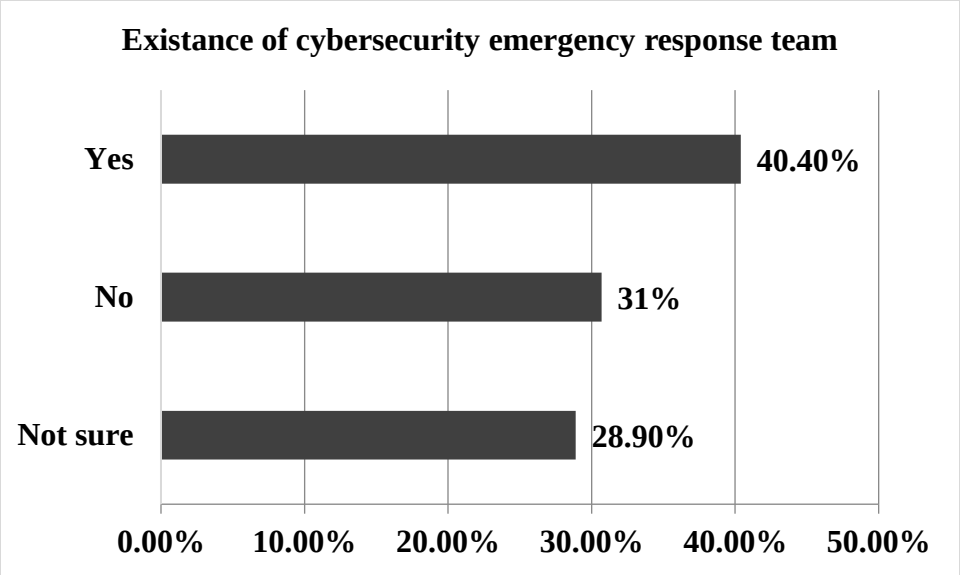

Figure 4.18: Does your organization have a cybersecurity emergency response team.

4.3 8 Adoption of Cybersecurity Frameworks, Standards and Best Practices

In terms of those with cybersecurity frameworks, standards and best practices, the following are some of the major available cybersecurity frame works, standards which institutions adopted within and that of their suppliers:

1) Payment Card Industry Data
2) Security Standard (PCI DSS)
3) Recognised standards such as ISO 27000 series
4) National Institute of Science and Technology Cyber Security Frame Work
5) Independent service auditor's report such as ISAE 3402
6) COBIT Framework
7) ITIL Frame Work

The findings revealed that 63% of the respondents indicated that they had cyber security framework in their Organizations, while only 19% did not indicate whether such frame works are used in their Organizations. Only 10 % of the respondents were not sure about the existence of such frame works in their Organizations. Further, 8% did not have any cyber security frameworks or best practices. See Figure 4.19 below for detailed illustration.

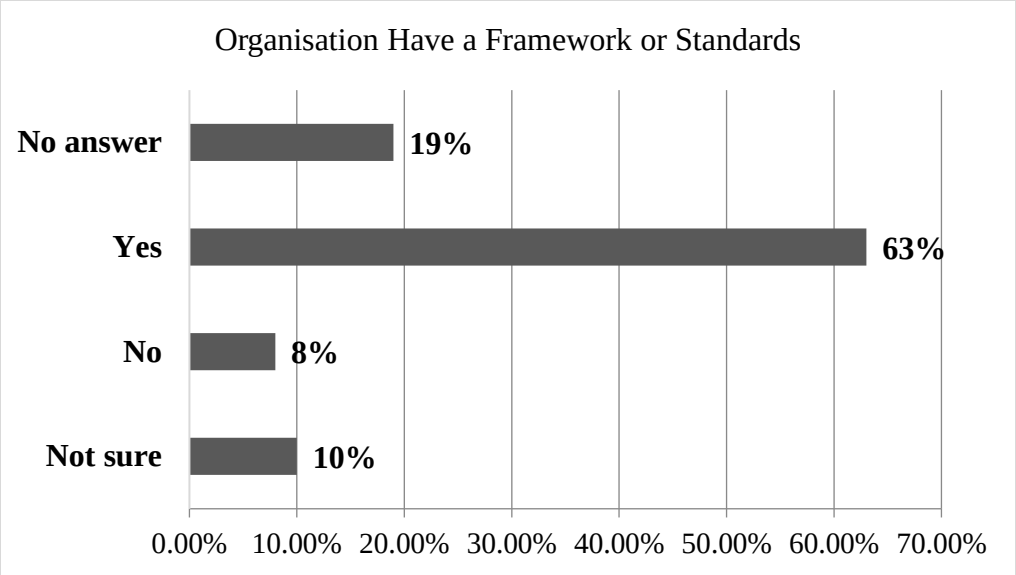

Figure 4.19: Does your organisation have a framework or standards? If any, do you require you organisation and suppliers to have or adhere to them?

This result about the adoption and implementation of cyber security frame works, standard and best practices in these organizations showed consistency, and reveals the fact that generally, Organizations were doing very little to ensure and to enforce effectively the cyber security frame works in their Organizations. The inefficient use of the frameworks is as a result the people handling cyber security are general IT specialists. It requires those with high level of understanding and competences, the cyber security specialists.

4.5 Chapter Summary

A total of 114 questionnaires were received out of a 150 that were distributed. From the received 114 copies and respondents which represented 74.6% and 25.4% respectively. It was noted from the study that respondents had sufficient understanding about the study. The study showed that the institutions have experienced cyber-attacks resulting into loss of revenue, loss of data, disrupt of services and many others in Lusaka. This could have been contributed by insufficient cyber security staff in these critical information infrastructures and services.

CHAPTER FIVE

5.0 DISCUSSION, RECOMMENDATIONS AND CONCLUSIONS

In this chapter, based on the empirical results and findings from this research project, the researcher presents a model to act as a framework to assist industries hosting critical infrastructures and services with the strategy cybersecurity implementation process. The researcher considered developing a framework in which is easily adaptable and practical application in any environment; commercial, non-commercial and in defence.

5.1 Discussion

The research study set out the objectives and to answer the five research questions outlined in chapter one.

The National Institute of Science and Technology (NIST) have developed a cybersecurity framework version 1.1 designed to detect, identify, intercept, and destroy or negate harmful activities attempting to penetrate or attack through cyberspace [84], [161]. This study, therefore, attempted to evaluate the extent to which organizations are keeping up to this challenge.

From the findings of the study, it was established high frequency into negative effects both on the operations as well as on the infrastructure and services of the Organization. These effects range from loss of data, financial loses, software systems damage, and websites slowed or brought down. This has further resulted in work derailment, as high operational costs as well as the loss of revenue and profits, among other things. Such findings resonate with observations made by various literature on the impact of cyber-attacks in affecting the critical infrastructures and services [3], [40].

However, findings revealed that though the majority of respondents indicated that managers in their institutions had placed a high priority on cybersecurity, the vice had been taken lightly as shown by the low levels of cybersecurity information-seeking behavior within these Organizations. Further, upon identifying the security breaches, only a few organizations, represented by 10.5% indicated that they can restore the operations instantly. The rest of them took either the whole day or more for them to recover from such an attack, an indication that in dealing with such cyber-attacks, most of these institutions could be using strategies that are not effective.

The United Nations ITU has advocated for the Cyber Security preparedness model, which outlines several requirements in ensuring cyber-warfare preparedness and these include

technology/operations awareness, intelligence gathering, preparation and strategy, operational response attack as well as discovery upon realization and identification of the attack. The model is a representation of the offensive and defensive methodology, processes, mechanisms, and techniques in cyberspace, and is meant to be used as a mechanism to examine in detail the factors that should indicate some cyber-attacks defense preparedness capabilities for the nation [151].

In conforming to the above-stated frameworks, one of the strategies currently being employed by the various Organizations includes the establishment of separate cybersecurity departments that specifically focus on addressing the challenges of cybersecurity. To this extent, the study established majority of the institutions interviewed had established such departments, with more than 70% of them indicating that they had at least six or more staff members in such departments. However, when it comes to training, the study revealed that from the total respondents, less than 50% of them indicated that they had received formal training on cybersecurity. Among those that had attended training, most of these Organizations have focused their attention on training personnel who are in the IT department as a way of empowering them to handle cybersecurity issues, compared to the Cyber Security personnel themselves. Further, the quality of training given to these personnel raises doubts given the results revealing that only 48.2% agreed to the assertion that people dealing with cybersecurity in these institutions have the right skills and knowledge to do this job.

Besides having the cybersecurity departments, the availability of formal policies, documents, rules, and controls aimed at strengthening the security against cyber-attack is likely to yield more results if only the issues covered in the policies are implemented fully. There is a lack of compliance with the frameworks or models, standards and policies which the organization has adopted. However, this is likely to be weakened by the lack of reporting procedures of any suspicious or real cybersecurity breach, and the lack of a cyber-security emergency response team, as revealed by the results of this study. This, therefore, calls for the need to develop a framework, based on the findings of this study that would specifically be tailored towards addressing the problems of cybersecurity in Zambia.

5.1.1 Enterprise Governance and Strategic Direction

The research study set out the objectives and to answer the five research questions outlined in chapter one.

The National Institute of Science and Technology (NIST) have developed a cybersecurity framework version 1.1 designed to detect, identify, intercept, and destroy or negate harmful activities attempting to penetrate or attack through cyberspace [84]. This study, therefore, attempted to evaluate the extent to which organizations are keeping up to this challenge.

From the findings of the study, it was established high frequency into negative effects both on the operations as well as on the infrastructure and services of the Organization. These effects range from loss of data, financial loses, software systems damage, and websites slowed or brought down. This has further resulted in work derailment, as high operational costs as well as the loss of revenue and profits, among other things. Such findings resonate with observations made by various literature on the impact of the cybersecurity mechanisms adopted in the organizations that are ineffective due to the high levels of non-compliance to cybersecurity frameworks and to best place implementation. Cybersecurity must be part of the budget agenda. Cybersecurity requires to have allocated budget planned to meet the demanding resources. When cybersecurity is regarded as a burden and not as an investment to the organisation its posture will be vulnerable to be exploited, which can be very grave and costly than expected. It is for this reason that we propose to develop the preparedness framework in Figure 5.1 which specifically be tailored towards addressing the problems of cybersecurity in Zambia. The framework contains the module to respond to the attacker, once this is established it can be reported to the authorities responsible to handle to diplomatic and boundary issue to a suspected nation-state. It remains a challenge as the nation has not yet established the agency responsible to handle the cyberspace, Zambia Police Service, Zambia Air Force, and others have different mandates cyber-attacks in affecting the critical infrastructures and services [63; 65].

However, findings revealed that though the majority of respondents indicated that managers in their institutions had placed a high priority on cybersecurity, the vice had been taken lightly as shown by the low levels of cybersecurity information-seeking behaviour within these Organizations. Further, upon identifying the security breaches, only a few organizations, represented by 10.5% indicated that they can restore the operations instantly. The rest of them took either the whole day or more for them to recover from such an attack, an indication that in dealing with such cyber-attacks, most of these institutions could be using strategies that are not effective.

The United Nations ITU has advocated for the Cyber Security preparedness model, which outlines several requirements in ensuring cyber-warfare preparedness and these include technology/operations awareness, intelligence gathering, preparation and strategy, operational response attack as well as discovery upon realization and identification of the attack. The model is a representation of the offensive and defensive methodology, processes, mechanisms, and techniques in cyberspace, and is meant to be used as a mechanism to examine in detail the factors that should indicate some cyber-warfare preparedness capabilities for the nation [151].

In conforming to the above-stated model or framework, one of the strategies currently being employed by the various Organizations includes the establishment of separate cybersecurity departments that specifically focus on addressing the challenges of cybersecurity. To this extent, the study established majority of the institutions interviewed had established such departments, with more than 70% of them indicating that they had at least six or more staff members in such departments.

However, when it comes to training, the study revealed that from the total respondents, less than 50% of them indicated that they had received formal training on cybersecurity. Among those that had attended training, most of these Organizations have focused their attention on training personnel who are in the IT department as a way of empowering them to handle cybersecurity issues, compared to the Cyber Security personnel themselves. Further, the quality of training given to these personnel raises doubts given the results revealing that only 48.2% agreed to the assertion that people dealing with cybersecurity in these institutions have the right skills and knowledge to do this job.

Besides having the cybersecurity departments, the availability of formal policies, documents, rules, and controls aimed at strengthening the security against cyber-attack is likely to yield more results if only the issues covered in the policies are implemented fully. There is a lack of compliance with the frameworks or models, standards and policies which the organization has adopted. However, this is likely to be weakened by the lack of reporting procedures of any suspicious or real cybersecurity breach, and the lack of a cyber-security emergency response team, as revealed by the results of this study. This, therefore, calls for the need to develop a framework, based on the findings of this study that would specifically be tailored towards addressing the problems of cybersecurity in Zambia.

5.1.2 Low Representation of Cybersecurity Experts

The current representation of the low number of cybersecurity skills and personnel levels in that most organizations contribute to a lack of compliance and understanding of the technologies. It was also observed that most organizations are understaffed or have no cybersecurity personnel. There is also unfamiliarity with tools such as software and hardware which is designed and imported from foreign countries. This unfamiliarity is also fuelled by the dependence on foreign expertise to manage the organization's infrastructures and services. In order to conclude on the general research objective of developing a cyber-attacks preparedness framework for Zambia and therefore recommend the possible solutions to overcome the challenges. Insufficient reporting procedures. Inadequate cooperation between the private sector and law enforcement, and between different countries. Lack of skills and knowledge to handle tools and other technologies.

5.2 Conclusions

In conclusion, Cyber-Attack Preparedness Framework is an important tool for the protection of critical infrastructures and services of the state and business communities. The cyberspace with all the connected devices and services have continued to be platforms that require sound and proper protection mechanisms to provide security assurance. The evolution of cyberspace has continued to positively impact our society and has greatly changed the way we live, learn and conduct our everyday business. This applies to the private and public sectors. Critical infrastructures have been identified as a valuable resource that would foster economic and social development in a nation and connect the nation to other parts of the words. From the literature that has been reviewed, it has been established that critical infrastructures and services have become targets for cyber-attacks. It would furthermore benefit if these critical infrastructures and services are given primary attention by applying appropriate cybersecurity defence mechanism.

However, despite the importance of having smart cities, the Internet of Things and implementing ICTs being well known to policymakers, its security has been threatened by a lot of cyber-attacks that need the intervention. The country needs to deliberately come up with measures that can bring about and promote a well-established security assurance to critical infrastructures and services that would result in the secure national cyberspace. In this fourth industrial revolution era, the Internet is used as a medium for the transmission, storage, and sharing of resources. Some of these resources are highly valued for the governance of the state, businesses and the individuals. There

are different groupings interested in such valuable sources including nations, companies, and individuals. The term cyber warfare may not only be applied to military spheres but civilians are waging this war just by applying their skills and knowing what they want.

5.3 Recommendations

We recommend that decision-makers and the enterprises consider strategically to exhibit commitment and support in directing cybersecurity by providing frameworks, appropriate budget, and tools which are approved. The research identified Banking and Finance, Power and Energy, Health, Utility, Telecoms, government agencies are critical in restructures.

A complete comprehensive framework must be implemented from end to end. ICT security needs to be aligned to all developments and procedures organizational-wide. User awareness programs need to be the top of the security agenda for all business associates in a quest to be prepared and have a resilient environment.

The researcher spent enough time and effort in producing a cyber-attacks defence preparedness framework for public and private sectors in Zambia. The Government through its regulating agencies plays a primary role in enabling the environment through its decision making.

The private sector produces and consumes 'actionable' cyber products and services. These are Non-military actors advancing in the exploration and usage of the cyberspace. The researcher created the proposed framework as a simple way to describe the function process and frame dialogue about ways to achieve cybersecurity goals. The framework is also meant to be adopted in a civilian environment and it was designed with the approach so that it can provide a high-security posture for the private and public critical infrastructures and services.

5.3.1 Proposed Framework

The framework captures the Function Strategy, Capacity Building, Technology, Intelligence, Operational Protection, Operational Detection, Operational Response, and Recovery. The Proposed framework can be used government agencies and private corporation in Security Operation Centre (SOC), which go by many names: Computer Security Incident Response Team (CSIRT), Computer Incident Response Team (CIRT), Computer Security Incident Response Capability (CSIRC), Network Operations and Security Center (NOSC), and, of course, Cyber Security Operation Centre (CSOC).

We have depicted the framework proposed from the International Telecommunications Union, Nation Institute of Standard Technology, combined with ISO 27000 Series, COBIT 5 Framework and many others. The mode shows that the key critical infrastructure and services either provided by the public or the private are protected. It expands its capabilities in line with two-way defence mechanisms (symmetric and asymmetric) in order to overcome internal and external threats.

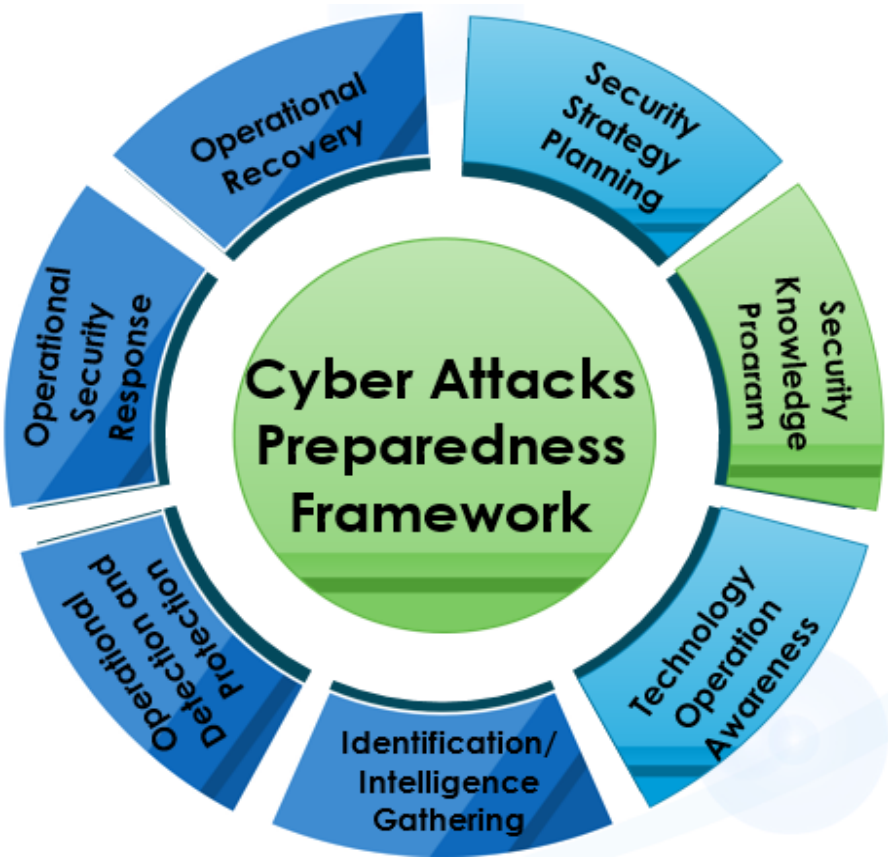

Figure 5.1: Proposed Cyber Attacks Preparedness Framework (CAPF)

Table 5.1: Proposed Cyber Attacks Preparedness Framework

Proposed Cyber Attacks Preparedness Framework (CAPF)	
Cybersecurity Strategy & Planning	Give the CSOC the authority to do its job through the effective organizational placement and appropriate policies and procedures.
Security Program Knowledge	Favour staff quality over quantity, employing professionals who are passionate about their jobs, provide a balance of soft and hard skills, and pursue opportunities for growth.
Cyber Security Technology and Operation Awareness	Consolidate functions of incident monitoring, detection, response, coordination, and computer network defence tool engineering, operation, and maintenance under one organization, Cyber Security Command Centre. Realize the full potential of each technology through careful investment and a keen awareness of—and compensation for—each tool's limitations.
Identification and Intelligence Gathering	Exercise great care in the placement of sensors and collection of data, maximizing signal and minimizing noise. Be a sophisticated consumer and producer of cyber threat intelligence, by creating and trading in cyber threat reporting, incident tips and signatures with other CSOCs
Cyber Security Operation and Protection	Carefully protect CSOC systems, infrastructure, and data while providing transparency and effective communication with constituents.
Operation Detection and Precautions	Achieve a balance between size and visibility/agility, so that the CSOC can execute its mission effectively. Carefully protect CSOC systems, infrastructure, and data while providing transparency and effective communication with constituents [120]
Operational Security Response and Attack	Respond to incidents in a calm, calculated, and professional manner.
Operational Recovery	It is a recovery of specific parts of the IT infrastructure in the case of an IT failure or a relatively a cyber-attack. The recovered data can have various forms: a file, an email message, a database entry, and other critical systems.

5.3.2 How to use the Framework

The framework is not developed to tell the public and private sectors what to do or how to do it. The intention is not to give you the course of action. The framework is meant to offer the course of action to cybersecurity.

The CWPF with an associated ITU, NIST, ISO 27000 series and other frameworks can be used to describe cyber activity in a consistent and repeatable fashion. The framework can:

1) Establish a shared ontology and enhance information-sharing. It is far easier to map the translation of multiple frameworks to a common reference than directly to each other.
2) Can support missions ranging from strategic decision-making to analysis and cybersecurity measures and users from generalist to technical experts.
3) Support common situational awareness across organizations.
4) Accommodate a wide variety of data sources, threat actors and activity
5) Provide a foundation for analysis and decision-making
6) Provide a starting point for organizations that have not yet adopted a Security Framework.
7) Built around the simple framework and value-neutral concepts, the CSPF can be customized for an organization's needs and these modifications from the original CSPF are readily apparent, facilitating mapping and data exchange.

5.3.3 Implementation of Effective Cyber Attack Preparedness Framework

1) Welcome the cyber-attack defence preparedness by the Executive officials in the business strategy.
2) Align the framework with other known standards and best practices.
3) Alight the framework in increase Return on Investments and increased asset security.

5.3.4 How the Framework was developed?

The idea of creating a cyber-attack preparedness framework came from observations among the National ICT Master Plan, National Seventh Development Plan that cybersecurity was not being described fully by different agencies in a variety of ways that made inconsistent understanding and addition suggestions of the framework. There are over different standards and frameworks being

used across government, academia, and the private sector. Each model reflects the priorities and interests of its developer, but the wide disparities across frameworks made it difficult to facilitate efficient situational to the industry.

A typical operation includes the following elements:

1) Prevention of cybersecurity incidents through proactive: Continuous threat analysis; Network and host scanning for vulnerabilities; Countermeasure deployment coordination; Security policy and architecture consulting.

2) Monitoring, detection, and analysis of potential intrusions in period and thru historical trending on security-relevant knowledge sources.

3) Response to confirmed incidents, by coordinating resources and directing the use of timely and appropriate countermeasures.

4) Providing situational awareness and reporting on cybersecurity status, incidents, and trends in adversary behaviour to appropriate organizations

5) Engineering and operating Computer Network Defense (CND) technologies such as intrusion detection system (IDSes) and data collection/ analysis systems [152].

5.3.5 The Relationship between CSPF and Other Cyber Security Frameworks

While NIST and other frameworks have not promulgated or endorsed a specific cyber-attacks defence preparedness framework, it advocates the use of a cybersecurity framework in addition to a cybersecurity framework to inform risk decisions and evaluate safeguards and actions taken. NIST and other models offers the documentation that describes threat frameworks that offers depth understanding into that safeguards are additional necessary at a given purpose in time and specific threat circumstances.

5.3.6 CAPF and CSIRTs or CERTs

Garry Mukelabai [153] suggested that there is a need to recognize that improving Cybersecurity is a national and global problem and that each country in the region must improve its national efforts and undertake actions to hitch and support regional and international efforts to boost Cybersecurity. Below are the pointers that will help achieve the efforts:

1) Develop a national Cybersecurity strategy;

2) Review and, if necessary, revise current cyber legislation and draft new legislation, to criminalize the misuse of ICTs, taking into account the rapidly evolving Cybersecurity threats and;

3) Develop incident management capabilities with national responsibility and use current samples of (Computer Security Incident Response Team/Computer Emergency Response Team) CSIRTs/CERTs once developing these. There is a need to raise awareness about the existence of these national response teams. See Figure 5.2.

5.3.6.1 Cyber Attacks Incident Management Capability

Sector Specific CERTS report to National CERT to use the CAPF

Figure 5.2: Computer Emergency Response Team [153]

5.3.6.2 Duties of a CERT

A central, trusted organisation that co-ordinates the response to Cybersecurity incidents. Also assists in proactive measures to reduce risk.

1) Watch, Warning, Information Alert

2) Investigation & incident Response

3) Information Sharing and Analysis Centre

5.4 Further Works

While conducting this research, the researcher made some observations of gaps that may need further research. These gaps were beyond the scope of this work. Areas of further research includes but not limited to the following:

1) Similar research needs to be carried out in the defence force so as to get a more representative picture of Cyber-attacks Preparedness from the security or defence force of Zambia.

2) A more detailed investigation of how the continent and others are managing critical services and infrastructures in this fourth industrial revolution.

5.5 Chapter Summary

Critical infrastructures and services have to experience cyber-attacks resulting in compromising confidentiality, integrity, and availability by lack of infrastructure, unskilled cybersecurity professionals, failure to adopt and force frames and low level in training personnel. There is very increase in infrastructure investment but few technical expertise. The low level of applying complete defence-in-depth is one of the major causes of cyber-attacks.

There is a need for the adoption and implementation of the cyber warfare preparedness frame which can be applied and tailored to any cyberspace in Zambia.

6.0 REFERENCES

[1] D. J. Bodeau. Improving cyber security and mission assurance via cyber preparedness (cyber prep) levels," Proceedings - SocialCom 2010: 2nd IEEE International Conference on Social Computing, PASSAT 2010: 2nd IEEE International Conference on Privacy, Security, Risk and Trust, pp. 1147-1152, 2010.

[2] K. David. IEEE Spectrum, "*The Real Story of Stuxnet."* December 26, 2013. [Online] http://spectrum.ieee.org/telecom/ security/the-real-story-of-stuxnet/. [Accessed on 05/02/2019]

[3] I. Traynor. "*Russia accused of unleashing cyberwar to disable Estonia."* The Guardian, May 17, 2007. [Online] http://www.theguardian.com/ world/2007/may/17/ topstories3.russia [Accessed on 05/02/2019]

[4] C. Nelson. Cyber Warfare: The Newest Battlefield. P. 3 - 4. 2017. [Online] http://www.cse.wustl.edu/~jain/cse571-11/ftp/cyberwar/index.html [Accessed on 06/06/2019]

[5] S. Cheang, "Conceptual model for cybersecurity readiness assessment for public institutions in developing country: Cambodia," ICCIT 2009 - 4th International Conference on Computer Sciences and Convergence Information Technology, pp. 1411-1418, 2009.

[6] B. Von Solms, "Critical Information Infrastructure Protection (CIIP) and Cyber Security in Africa - Has the CIIP and Cyber Security Rubicon been crossed?" in Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, 2012.

[7] C. Billo, W. Chang. “Cyber warfare an analysis of the means and motivations of selected Nation states”. M. A. Thesis. Institute for Security Technology studies at Dartmouth College. 45 Lyme road Hanover, NH 03755, 2004, 603-646-0700 [eBook] http://www.ists.dartmouth.edu/library/212.pdf [Accessed on 7/03/2019]

[8] R. Daley, "Operationalizing the coordinated incident handling model," 2011 IEEE International Conference on Technologies for Homeland Security, HST 2011, pp. 287-294, 2011.

[9] S. Hoffman. CRN, "*Russian Cyber Attacks Shut Down Georgian Websites*." August 12, 2008. [Online] http://www.crn.com/news/security/ 210003057/Russian-cyberattacks-Shut-down-georgian-websites.htm. [Accessed on 05/02/2019]

[10] Seventh National Development Plan. Ministry of National Development Planning. Lusaka. Vol. 1, p. 80, [Online] http://www.mndp.gov.zm/download/7NDP.pdf [Accessed On 12/07/2017]

[11] National Information and Communication Technology Policy. 2006. Ministry of Communications and Transport, Lusaka

[12] ZICTA Statistics Portal [Online] http://onlinesystems.zicta.zm:8585/statsfinal/ICT%20Indicators.html [Accessed on 15/12/2018]

[13] Ministry of Transport and Communications. The-Cyber-Security-and-the-Cyber-Crimes-DRAFT-Bill-2017. [Online] http://www.parliament.gov.zm/node/6419 [Accessed on 22/06/2019]

[14] R. Chitotela. The National Assembly of Zambia. The Vice-President's Question Time. [Online] http://www.parliament.gov.zm/node/6212 [Accessed on 22/07/18]

[15] U. J. Orji. *"Cybersecurity Law and Regulation"* Wolf Legal Publishers. Netherlands. 2012.

[16] Electronic Communications and Transactions | No. 21 of 2009 219. Ministry of Transport and Communications. Lusaka

[17] National Assembly of Zambia ICT Master Plan. June 2010. [Online] https://www.uneca.org/sites/default/files/PublicationFiles/sro-sanationalassemblyofzambiaictmasterplan.pdf [Accessed on 23/07/18]

[19] M. Malakata. *"Cybercrime up by 23% in Zambia".* Published on 21 April 2017 [Online] http://www.itwebafrica.com/security/512-zambia/237744-cybercrime-up-by-23-in-Zambia. [Accessed on 21/07/2018]

[20] J. Andres, and S. Winterfeld. "*Cyber Warfare".* Elsevier, Amsterdam. 2011

[21] Ministry of Legal Affairs, Government of the Republic of Zambia. The Laws of Zambia. [Online] http://www.parliament.gov.zm/sites/default/files/documents/acts/Defence%20Act.pdf [Accessed on 06/10/2019]

[22] Ministry of Defence [Online] http://www.mod.gov.zm/?page_id=5215 [Accessed on 12/03/2019]

[23] Ministry of Transport and Communications. Information and Communications Technologies [No.15 of 2009 129] Government Printers Lusaka Zambia [Online] https://www.zicta.zm/Downloads/The%20Acts%20and%20SIs/ICT%20Acts/ict_act_2009.pdf [Accessed on 22/06/2019]

[24] N. Kshetri. Pattern of global cyber war and crime: A conceptual framework. Journal of International Management, 2005.11(4), 541-562.

[25] E. T. Jensen. Cyber warfare and precautions against the effects of attacks. Tex. L. 2009, Rev., 88, 1533.

[26] D. M. Drew, and D. M. Snow. Making Twenty-First-Century Strategy: An Introduction To Modern National Security Processes and Problems, Air University Press, Maxwell AFB, Alabama. (2006)

[27] ITU National Cybersecurity Strategy Guide. [Online] www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf [Accessed On 2019-01-15]

[28] N. Kshetri. Pattern of global cyber war and crime: A conceptual framework. Journal of International Management, 2005.11(4), 541-562.

[29] J. Carr. Inside Cyber Warfare. O'Reilly Media, Inc. USA. 2010

[30] M. Wimmer, R. Traunmuller, and K. Lenk. Electronic business invading the public Sector: considerations on change and design. In Proceedings of the 34th Annual Hawaii International Conference on System Sciences, 2001 (p. 10 pp.–). [Online] http://doi.org/10.1109/HICSS.2001.926520 [Accessed on 11/01/2019]

[31] What is Cobit 5? http://www.isaca.org/COBIT/Pages/COBIT-5.aspx [Accessed on 11/01/2019]

[32] W. C. Ashmore. *"Impact of Alleged Russian Cyber Attacks".* [Abstract]. School of Advanced Military Studies United States Army Command and General Staff College. Fort. Leavenworth, Kansas. 2008 – 2009.

[33] M. Dion, "Intelligence and Cyber Threat Management," in Cybersecurity Best Practices, Springer Fachmedien Wiesbaden, 2018, pp. 363-392.

[34] S. Goel and K. Williams International Cyber Conflicts. [Online] https://www.coursera.org/learn/cyber-conflicts/lecture/xndSq/introduction-to-cybercrime-and-fundamental-issues [Accessed on 14/062019]

[35] J. Walker, "Cyber security for emergency management," in 2010 IEEE International Conference on Technologies for Homeland Security, HST 2010, 2010.

[36] M. P. Efthymiopoulos, "A cyber-security framework for development, defense and Innovation at NATO," Journal of Innovation and Entrepreneurship, vol. 8, no. 1, 2019.

[37] G. B. White, "The Community Cyber Security Maturity Model the Center for Infrastructure Assurance and Security the University of Texas at San Antonio," Sciences-New York, pp. 1-8, 2007.

[38] G. Griffith, "Information technology preparations for the Pluto encounter from mission operations to science retrieval," in IEEE Aerospace Conference Proceedings, 2017.

[39] C. E. Irvine, "Call in the cyber national guard!" IEEE Security and Privacy, vol. 8, no. 1, pp. 56-59, 2010.

[40] L. H. Wei. *"The Challenges of Cyber Deterrence. Pointer",* Journal of the Singapore Armed Forces. Vol.41 No.1. Pages 1-14. 2014

[41] Policy Monitoring and Research Centre. *"Smart Zambia and the benefits of e-payslips"*. [Online] http://www.pmrczambia.com/smart-zambia-and-the-benefits-of-e-payslips-blog/ [Accessed on 9/08/2018]

[42] C. Carmen-Cristina. "*Cyber defence in the EU Preparing for cyber warfare?"* European Parliamentary Research Services. 2014

[43] J. Andress, S. Winterfeld. *"The Cyberspace Battlefield"* [Journal Article] 2011 pp: 19-36. DOI10. 1016/B978-1-59749-637-7.00002-2 ISBN 978-1-59749-637-7 [Online] www.sciencedirect.com/science/article/pii/B9781597496377000022 [Accessed on 14/062019]

[44] M. Robinsona, K. Jones, H. Janickea. "*Cyber Warfare: Issues and Challenges*". Article in Computers & Security · March 2015 DOI: 10.1016/j.cose.2014.11.007. https://www.researchgate.net/publication/276248097 [Online] https://www.researchgate.net/publication/276248097_Cyber_warfare_Issues_and_challenges [Accessed on 15/06/2019]

[45] A. Walls, Perkins E, Weiss J. Definition: “Cybersecurity”, G00252816. Gartner Inc.; 013. [Google Scholar] [Accessed on 12/03/2019]

[46] D. Galinec. The Ministry of Defense of the Republic of Croatia, Zagreb, Croatia Correspondence. Darko Možnik & Boris Guberina Cybersecurity and Cyber Defense: National Level Strategic Approach. Journal for Control, Measurement, Electronics, Computing and Communications. Volume 58, 2017 - Issue 3 [Online] http://orcid.org/0000-0003-4465-6143 [Accessed on 06/06/2019]

[47] R. Kaiser. The birth of cyberwar. Political Geography, Volume 46, May 2015, p11-20

[48] M. Robinson, K. Jones, H. Janicke. “*Cyber warfare: Issues and challenges Computers & Security”*, Volume 49, March 2015, Pages 70-94

[49] A. S. Peter. Cyber resilience preparedness of Africa’s top-12 emerging economies International Journal of Critical Infrastructure Protection, Volume 17, June 2017, p49-59

[50] J. A. Bullock, G. D. Haddow, and D. P. Coppola. Book chapter 8: Cybersecurity and Critical Infrastructure. Protection Homeland Security (Second Edition), 2018, p189-226

[51] P. Shakarian, J. Shakarian, and A. Ruef. Introduction to Cyber-Warfare: A Multidisciplinary Approach. Elsevier. New York. 2013.

[52] H. J. Hejase. Cyber Warfare Awareness in Lebanon: Exploratory Research. International Journal of Cyber-Security and Digital Forensics (IJCSDF) 4(4): 482-497. 2015

[53] C. Jeffrey. “*Inside Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners”*. O’Reilly Media. USA. 2010

[54] G. Ntulo, J. Otike. E – Government: Its Role, Importance and Challenges. School of Information Sciences. Moi University [Abstract] https://www.researchgate.net/file.PostFileLoader.html?id=564b965d6225ffe6e98b4595&assetKey=AS:296884838125570@1447794269180 [Accessed on 26/07/2018]

[55] T. A. Johnson. “*Cyber-security: Protecting Critical Infrastructures from Cyber Attack And Cyber Warfare.* CRC Press Taylor and Francis group. New York. 2015.

[56] T. Rid. Cyberwar and Peace: Hacking Can Reduce Real-World Violence, Foreign Affairs 92(6), 77-87 (2013).

[57] S. J. Shackelford. *“From nuclear war to net war: Analogizing cyber-attacks in International law”*. Berkeley J. Int'l Law, 2009, v27, p192.

[58] M. N. Schmitt, (Ed.). Tallinn manual on the international law applicable to cyber warfare.

Cambridge University Press. 2013

[59] A. Hemanidhi and S Chimmanee. Military-based cyber risk assessment framework For supporting cyber warfare in Thailand. Journal of ICT, 16, No. 2 (Dec) 2017, pp: 192–222.

[60] Y. S. Baker, "Analyzing security threats as reported by the United States Computer Emergency Readiness Team (US-CERT)," IEEE ISI 2013 - 2013 IEEE International Conference on Intelligence and Security Informatics: Big Data, Emergent Threats, and Decision-Making in Security Informatics, pp. 10-12, 2013.

[61] Cybersecurity Framework [Online] https://www.nist.gov/cyberframework [Accessed on 11/01/2019]

[62] N. Kshetri, "The quest to cyber superiority: Cybersecurity regulations, frameworks, and strategies of major economies," The Quest to Cyber Superiority: Cybersecurity Regulations, Frameworks, and Strategies of Major Economies, no. September 2014, pp. 1-240, 2016.

[63] Maritime Bulk. Liquids Transfer Cybersecurity Framework Profile. p.9 [Online] http://portalcip.org/wp-content/uploads/2017/05/Maritime_BLT_CSF.pdf p.9 [Accessed on 02/08/2018]

[64] G. M. Mancini, "Cyber and Chemical, Biological, Radiological, Nuclear, Explosives Challenges," pp. 311-325, 2017.

[65] W. Zhao, "A collaborative information sharing framework for community cyber security," in 2012 IEEE International Conference on Technologies for Homeland Security, HST 2012, 2012.

[66] L. Maglaras, "Cyber Security: From Regulations and Policies to Practice," pp. 763-770, 2019.

[67] R. Abeyratne, "Legal Priorities in Air Transport," Springer International Publishing, 2019.

[68] A. J. Schaap. Cyber warfare operations: Development and use under international law. AFL Rev., 2009. v64, p121.

[69] T. C. S. M. A. R. TOOL (CyberSMART), "Marshall, Jim," in Proceedings - Cybersecurity Applications and Technology Conference for Homeland Security, CATCH 2009, 2009.

[70] R. R Dipert, The ethics of cyberwarfare. Journal of Military Ethics, 2019, (4), 384-410.

[71] M. Robinson, K. Jones, H. Janicke. Cyber warfare: Issues and challenges. Computers & Security, Volume 49, March 2015, Pages 70-94

[72] J. A. Bullock, G. D. Haddow, and D. P. Coppola. Book chapter 8: Cybersecurity and Critical Infrastructure. Protection Homeland Security (Second Edition), 2018, p189-226

[73] D. Satola, H. L. Judy, Towards a Dynamic Approach to Enhancing International Cooperation and Collaboration in Cybersecurity Legal Frameworks: Reflections on the Proceedings of the Workshop On Cybersecurity Legal Issues At The 2010 United Nations Internet Governance Forum 37 William Mitchell Law Review, 1748-1749 (2011).

[74] Clough. Principles of Cybercrime 5. 2010; Brenner, Boston University Journal of Science & Technology Law, 24 - Weslaw Paging - (2004).

[75] A. S. Peter. Cyber resilience preparedness of Africa's top-12 emerging economies International Journal of Critical Infrastructure Protection, Volume 17, June 2017, p49-59

[76] K. Geers. *"Cyberspace and the Changing Nature of Warfare".* U.S. Representative Cooperative Cyber Defense, Centre of Excellence, Tallinn, Estonia. IST-076/RSY-017. [Online]https://ccdcoe.org/uploads/2018/10/Geers2008_CyberspaceAndTheChangingNatureOfWarfare.pdf. [Accessed on 15/06/2019]

[77] P. Shakarian, J. Shakarian, and A. Ruef. Introduction to Cyber-Warfare: A Multidisciplinary Approach. Elsevier. New York. 2013.

[78] M. Robinson, K. Jones, H. Janicke. "Cyber warfare: Issues and challenges Computers & Security", Volume 49, March 2015, Pages 70-94

[79] T. Wheeler. In Cyberwar, There Are No Rules: Why the world desperately needs digital Geneva Conventions. September 12, 2018. [Online] https://foreignpolicy.com/2018/09/12/in-cyberwar-there-are-no-rules-cybersecurity-war-defense/ [Accessed on 17/06/2019]

[80] A. Pelc, Lecture Notes in Computer Science: Preface, 2005, p. 3499.

[81] N. Sjelin, "Cyber-Physical Security," Cyber-Physical Security, pp. 161-183, 2017.

[82] E. A. Fischer. *"Cybersecurity Issues and Challenges: In Brief"* Congressional Research Service 7-5700. R43831. P1-12. www.crs.gov. August 12, 2016. [Online] https://pdfs.semanticscholar.org/65e3/4c9bb7330fcfec378394b5d308b6a323947d.pdf [Accessed on 15/06/2019]

[83] F. Skopik, "Designing a cyber attack information system for national situational awareness," Communications in Computer and Information Science, vol. 318 CCIS, pp. 277-288, 2012.

[84] J. E. Cartwright. *2010-11-joint Terminology for Cyberspace Operations.* United States of America Department of Defence. [Online] http://www.nsci-va.org/CyberReferenceLib/2010-11-joint%20Terminology%20for%20Cyberspace%20Operations.pdf [Accessed on 22/06/2019]

[85] J. A. Mattson, "Cyber defence exercise: A service provider model," in IFIP International Federation for Information Processing, 2007.

[86] Norwegian Intelligence Service, Focus 2012, 26, http://forsvaret.no/omforsvaret/organisasjon/felles/etjenesten/Documents/etj_lo-res.pdf. [Accessed on 9/02/2019]

[87] R. McDonald, "New considerations for security compliance, reliability and business continuity," in Papers Presented at the Annual Conference - Rural Electric Power Conference, 2008.

[88] E. Skoudis, "Evolutionary Trends in Cyberspace," Ch. 6 in Cyberpower and National Security, ed. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Washington, DC: National Defense University Press, 2009), p 165.

[89] L. McLeod, "Reconceptualising security?" Gender Politics and Security Discourse, pp. 70-90, 2018.

[90] Business Dictionary, [Online] http://www.businessdictionary.com/definition/denial-of-service-DOSattack.html. [Accessed on 9/02/2019]

[91] Techterms definitions, [Online] http://w;ww.techterms.com/definition/malware.

[Accessed on 9/02/2019]

[92] G. Mezzour, "Remote assessment of countries' cyber weapon capabilities," Social Network Analysis and Mining, vol. 8, no. 1, 1 December 2018.

[93] An overview of Cryptography, Ch. 2, [Online] http://www.garykessler.net/library/crypto.html#purpose. [Accessed on 20/02/2019]

[94] N. Mehravari, "Resilience management through use of CERT-RMM & associated success stories," 2013 IEEE International Conference on Technologies for Homeland Security, HST 2013, pp. 119-125, 2013.

[95] J. Mouton, "The identification of information sources to aid with Critical Information Infrastructure Protection," 2013 Information Security for South Africa - Proceedings of the ISSA 2013 Conference, 2013.

[96] E. Cody. *"Chinese Official Accuses Nations of Hacking",* Washington Post, September 13, 2007, http://www.washingtonpost.com/wp-dyn/content/article/2007/09/12/AR2007091200791_pf.html#. [Accessed on 15/06/2019]

[97] G. Mukelabai. *Cybersecurity in Zambia.* [Online] www.itu.int/ITU-D/cyb/events/2008/lusaka/docs/mukelabai-caz-zambia-lusaka-aug-08.pdf [Accessed on 22/06/2019]

[98] A.D. Divis, *"Protection not in place for electric WMD",* UPI, March 9, 2005. [Online] http://www.globalsecurity.org/org/news/2005/050309-electric-wmd.htm. [Accessed on 15/06/2019]

[99] A. Appazov. *"Legal Aspects of Cybersecurity"* p4-72. [Online] www.justitsministeriet.dk/sites/default/files/media/Arbejdsomraader/Forskning/Forskningspuljen/Legal_Aspects_of_Cybersecurity.pdf [Accessed on 15/06/2019]

[100] R. Buchan. *"Cyberspace, Non-State Actors and the Obligation to Prevent Transboundary Harm*". Journal of Conflict & Security Law. 2016 vol: 21 (3) pp: 429-453 [Online] http://eprints.whiterose.ac.uk/103386/11/Buchan%20FINAL%20Cyberspace.pdf [Accessed on 15/06/2019]

[101] M. Pomerleau. *State vs. non-state hackers: Different tactics, equal threat?* Aug 17, 2015. https://defensesystems.com/Articles/2015/08/17/Cyber-state-vs-non-state-haclers-tactics.aspx?Page=1 [Accessed on 15/06/2019]

[102] L. R. Blank. *"International Law and Cyber Threat from Non-state Actors'*. International Law Studies. p406 (2013)

[103] International Law Commission's Draft Articles on State Responsibility. 2001

[104] ABI research. Global Cybersecurity Index. Conceptual Framework [Online] https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCI_Conceptual_Framework.pdf [Accessed on 01/16/2019]

[105] K. B Stensboel. Norwegian Cyber Defense. Calhoun: The NPS Institutional Archive, 2013, p8-9.

[106] ITU Study Group Q.22/1 Report on Best Practices for a National Approach to Cybersecurity: A Management Framework for Organizing National Cybersecurity Efforts, ITU-D Secretariat. Geneva. (2008).

[107] T. A. Johnson. "Cyber-security: Protecting Critical Infrastructures from Cyber Attack And Cyber Warfare. CRC Press Taylor and Francis group. New York. 2015.

[108] U.S. Escalates Online Attacks on Russia's Power Grid. [Online] https://www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.html?searchResultPosition=1 [Accessed on 18/06/2019]

[109] P. Shakarian. The 2008 Russian Cyber-Campaign against Georgia. [Abstract]. [Online] https://www.researchgate.net/publication/230898147_The_2008_Russian_Cyber-Campaign_Against_Georgia [Accessed on 16/06/2019]

[110] Y. Soupionis, "Demo abstract: Demonstrating cyber-attacks impact on cyber-physical simulated environment," 2014 ACM/IEEE International Conference on Cyber-Physical Systems, ICCPS 2014, p. 222, 2014.

[111] T. L. Thomas. "Information Warfare in the Second (1999-Present) Chechen War: Motivator for Military Reform?" Foreign Military Studies Office, Fort Leavenworth, 2002, and in Chapter 11 of Russian Military Reform 1992-2002, Frank Cass Publishers, 2003, http://leavwww.army.mil/fmso/documents/iwchechen.htm. [Accessed on 16/06/2019]

[112] P. Goble. "Russia: Analysis from Washington -- a Real Battle on the Virtual Front," Radio Free Europe / Radio Liberty, October 11, 1999, http://www.rferl.org/features/1999/10/F.RU.991011135919.asp. [Accessed on 16/06/2019]

[113] B. Oliver. “Russians Wage Cyber War on Chechen Websites”, Reuters, November 15, 2002, http://seclists.org/isn/2002/Nov/0064.html. [Accessed on 16/06/2019]

[114] “Yugoslavia: Serb Hackers Reportedly Disrupt US Military Computer”, Bosnian Serb News Agency SRNA, March 28, 1999 (BBC Monitoring Service, March 30, 1999).

[115] “Evidence Mounts of Pro-Serbian Internet Attack on NATO Countries”, mi2g, April 19, 1999.

[116] G. Kenneth. Hacking in a Foreign Language, Black Hat 2005, http://www.blackhat.com/presentations/bhusa-05/bh-us-05-geers-update.pdf. [Accessed on 16/06/2019]

[117] “Israel lobby group hacked”, BBC News, November 3, 2000, http://news.bbc.co.uk/2/hi/middle_east/1005850.stm. [Accessed on 16/06/2019]

[118] IWS - The Information Warfare Site, http://www.iwar.org.uk/infocon/advisories/2001/01-009.htm. [Accessed on 16/06/2019]

[119] W. Jeremy. “The Internet could be the site of the next China-U.S. standoff”, The Wall Street Journal, April 30, 2001, http://online.wsj.com/article/SB98856633376453558.html?mod=googlewsj, and Allen, Patrick D. and Demchek, Chris C., “The Cycle of Cyber Conflict”, Military Review, March-April 2003. [Accessed on 16/06/2019]

[120] B. L. Boyd. “*Cyber Warfare: Armageddon in a Teacup?”* [Thesis] University of California, Irvine, California, 1996Fort Leavenworth, Kansas. 2009-02.

[121] R. Weisman. “California Power Grid Hack Underscores Threat to U.S.”, June 13, 2001.

[122] E. Nakashima, S. Mufson. “Hackers Have Attacked Foreign Utilities, CIA Analyst Says”, Washington Post, January 19, 2008, http://www.washingtonpost.com/wpdyn/content/article/2008/01/18/AR2008011803277_pf.html. [Accessed on 16/06/2019]

[123] J. Markoff. Before the Gunfire, Cyberattacks. New York Times. AUG. 12, 2008 [Online] https://www.nytimes.com/2008/08/13/technology/13cyber.html [Accessed on 16/06/2019]

[124] S. Khandelwal. “Having problems with your Internet service in Liberia? Someone is using Mirai Botnet to shut down the Internet for an entire country: Liberia!” http://www.tlcafrica.com/technology.htm [Accessed on 16/06/2019]

[125] M. Ward. Technology correspondent, BBC News. *“Could hackers turn the lights out?”* [Online] https://www.bbc.com/news/technology-35204921 [Accessed on 22/06/2019]

[126] What is Stuxnet, who created it and how does it work? | CSO Online [Online] https://www.csoonline.com/article/3218104/what-is-stuxnet-who-created-it-and-how-does-it-work.html [Accessed on 22/06/2019]

[127] Analysis of the Cyber Attack on the Ukrainian Power Grid Defense. Defense Use Case March 18, 2016 [Online] https://www.ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf [Accessed on 22/06/2019]

[128] Cyberattack suspected in Ukraine power outage. https://www.pcworld.com/article/3152010/cyberattack-suspected-in-ukraine-power-outage.html [Accessed on 22/06/2019]

[129] E. D. Knapp, Joel Thomas Langill, *Industrial Network Security (Second Edition)*, 2015 [Online] https://www.sciencedirect.com/topics/computer-science/stuxnet [Accessed on 22/06/2019]

[130] M. Holloway. Stuxnet Worm Attack on Iranian Nuclear Facilities. July 16, 2015 [Online] http://large.stanford.edu/courses/2015/ph241/holloway1/ [Accessed on 22/06/2019]

[131] P. W. Singer. Stuxnet and Its Hidden Lessons on the Ethics of Cyberweapons. Case Western Reserve Journal of International Law. 2015 vol: 47. Issue 1. [Online] https://scholarlycommons.law.case.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1009&context=jil [Accessed on 22/06/2019]

[132] N. Mims, *“In Computer and Information Security Handbook (Third Edition)”,* 2017. [Online] https://www.sciencedirect.com/topics/computer-science/stuxnet [Accessed on 22/06/2019]

[136] Liberia Telecommunications Authority, Public Consultation Document on the Definition of Relevant Telecommunications Markets. June 1, 2016

http://georgiaupdate.gov.ge/doc/10006922/CYBERWAR-%20fd_2_.pdf [Online] [Accessed on 16/06/2019]

[137] R. Picheta. CNN. Hacker who took down entire nation's internet is jailed. January 12, 2019 [Online] https://edition.cnn.com/2019/01/12/uk/hacker-liberia-cyber-attack-jailed-gbr-Intl/index.html [Access on 11/01/2019]

[138] M. Kan. "*2 Years for Hacker Who Crippled Liberia's Internet with Mirai Botnet"*. [Online] https://www.pcmag.com/news/365933/2-years-for-hacker-who-crippled-liberias-internet-with-mira [Accessed on 16/06/2019]

[139] Cybersecurity Standards and frameworks. https://www.itgovernanceusa.com/cybersecurity-standards [Accessed on 16/06/2019]

[140] R. Spousta, "Ocean data vulnerability to cyber manipulation and consequences for infrastructural resilience," in FTC 2016 - Proceedings of Future Technologies Conference, 2017.

[141] Part 5: Security best practices. https://www.itu.int/en/ITU-T/studygroups/com17/ict/Pages/ict-part05.aspx [Accessed on 18/06/2019]

[142] V. Subrahmanian, The Global Cyber-Vulnerability Report, The Global Cyber-Vulnerability Report, 2015, pp. 33-46.

[143] SADC Capacity Building Workshop on Cyber Security and SADC Regional Cyber Drill. Cyber Tower 1, CyberCity. EBENE, MAURITIUS. 2018. [Online] https://www.sadc.int/files/2515/3719/6602/Media_Statement_SADC_Capacity_Building_Workshop_on_Cyber_Security_and_Cyber_Drill.pdf [Accessed on 06/10/2019]

[144] R. Van Heerden, "Classification of cyber attacks in South Africa," in 2016 IST-Africa Conference, IST-Africa 2016, 2016.

[145] R. Van Heerden, "Major security incidents since 2014: An African perspective," 2018 IST-Africa Week Conference, IST-Africa 2018, pp. Page 1 of 11-Page 11 of 11, 2018.

[146] B. Van Niekerk, "Suppression of cyber-defences," in 2016 IST-Africa Conference, IST-Africa 2016, 2016.

[147] ICTs and development in Zambia: challenges and opportunities. [Online] http://panoslondon.panosnetwork.org/wp-content/files/2011/01/panos-london-zambia-policy-brief-web.pdf [Accessed on 22/06/2019]

[147] B. Van Niekerk, "Suppression of cyber-defences," in 2016 IST-Africa Conference, IST-Africa 2016, 2016.

[148] S. Habeenzu. Zambia ICT Sector Performance Review 2009/2010: Towards Evidence-based ICT Policy and Regulation. Volume Two, Policy Paper 17, 2010. P2. [Online] https://www.researchictafrica.net/publications/ICT_Sector_Performance_Reviews_2010/Vol%202%20Paper%2017%20-%20Zambia%20ICT%20Sector%20Performance%20Review%202010.pdf [Accessed on 22/06/2019]

[149] Cybercrimedata AS. https://www.cybercrimelaw.net/Zambia.html [Accessed on 22/06/2019]

[150] A. Kammani, A. Sultan and H. Date, "KM capability for software development: A case study of the Indian software firms," International Journal of Business Information Systems, Vol.12, no.1, pp.44-47, 2013.

[151] United Nations. OCHA What is preparedness? [Online] https://www.humanitarianresponse.info/en/coordination/preparedness/what-preparedness [Accessed on 20/02/2019]

[152] C. Zimmerman. *"Ten Strategies of a World-Class: Cybersecurity Operations Center"*. The MITRE Corporation. Bedford, MA. USA. 2014

[153] G. Mukelabai. Cybersecurity Efforts in Zambia. ITU Regional Cybersecurity Forum For Africa and Arab States. [Online] www.itu.int/ITU-D/cyb/events/2008/lusaka/docs/mukelabai-caz-zambia-lusaka-aug-08.pdf [Accessed on 22/06/2019]

[154] Ministry of Electronics & Information Technology, Government of India. National e-Governance Plan. [Online] http://meity.gov.in/divisions/national-e-governance-plan [Accessed on 22/07/18]

[155] S. L Dinesen, and H. B Sæther, Cyber Security - Securitizing cyber threats in Denmark. [Abstract] [Online] http://studenttheses.cbs.dk/bitstream/handle/10417/3949/sofia_lisa_dinesen_og_heidi_bruvik_saether.pdf?sequence=1 [accessed on 20/07/2018]

[156] S. Fred. *"On Cyberwarfare." in DCAF Horizon 2015 Working Paper Series. Geneva: Geneva Centre for the Democratic Control of Armed Forces*, Geneva. 2012.

[157] J. A Lewis. Assessing the risks of cyber terrorism, cyber war and other cyber threats. Center for Strategic & International Studies. 2002.

[158] M. Wimmer, R. Traunmuller, and K. Lenk. Electronic business invading the public Sector: considerations on change and design. In Proceedings of the 34th Annual Hawaii International Conference on System Sciences, 2001 (p. 10 pp.–).

[159] Information as a Commodity: New Imperatives of Commercial Law [Vol. 55: No. 3 p. 1-2 [Online] scholarship.law.duke.edu/cgi/viewcontent.cgi?article=4156&context=lcp [Access on 11/01/2019]

[160] ITU (2010f) "Resolution 174 (WGPL/1) - ITU's role with regard to International Public Policy Issues Relating to the Risk of Illicit Use of Information and Communication Technologies". In ITU Plenipotentiary Conference 2010 (PP-10), 4-22 October 2010, Guadalajara, Mexico, International Telecommunication Union (ITU).

[161] National Institute of Standards and Technology, Computer Security Division, "Identification and Authentication of Users," [Online] http://csrc.nist.gov/publications/nistpubs/800–11/node26.html. [Accessed on 20/02/2019]

[162] B. Mushimba. Minister Of Transport and Communication, Ministerial Statement on the Information and Communication Technologies and Electronic Government by the Hon Mr Mushimba Tuesday, 21 June, 2017 [Online] http://www.parliament.gov.zm/sites/default/files/images/publication_docs/MINISTERIAL%20STATEMENT%20BY%20HON%20MUSHIMBA.pdf [Accessed on 22/06/2019]

[163] M. Mushimba. Minister Of Transport and Communication. Ministerial Statement on the Electronic and Social Media Platforms by the Hon. Mr Mushimba, MP. Thursday, 5 July, 2018. [Online] http://www.parliament.gov.zm/sites/default/files/images/publication_docs/ministerial%2

0statement%20by%20the%20hon.%20minister%20of%20trans.%20and%20com.%20mr%20mushimba%2c%20on%20social%20media_0.pdf [Accessed on 22/06/2019]

[164] African Union Convention on Cyber Security and Personal Data Protection [Online] https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf [Accessed on 06/11/2019]

[165] Z. S. Zainudin. Advanced Persistent Threats Awareness and Readiness: A Case Study in Malaysian Financial Institutions. Proceedings of the 2018 Cyber Resilience Conference, CRC 2018, no. 2013, pp. 1-3, 2019.

[168] J. Krüger, The secure information society: Ethical, legal and political challenges, vol. 9781447147, The Secure Information Society: Ethical, Legal and Political Challenges, 2013, pp. 1-213.

[169] M. Albahar, "Cyber Attacks and Terrorism: A Twenty-First Century Conundrum," Science and Engineering Ethics, vol. 25, no. 4, pp. 993-1006, 2019.

[170] Kenya: building an offensive cyber operation strategy. The Kenya Ministry of Defense (n.d.). About MoD. Mod.go.ke. Retrieved from http://www.mod.go.ke/?page_id=338 [Online] medium.com/@johntroony/building-an-offensive-cyber-operation-strategy-a-kenyan-focus-b14908731be [Accessed on 12/03/2019]

7.0 APPENDICES

Appendix I: Instruments for data collection

Questionnaire

THE UNIVERSITY OF ZAMBIA

STRICTLY PRIVATE & CONFIDENTIAL

MASTER OF ENGINEERING IN ICT SECURITY PAPER

RESEARCH QUESTIONNAIRE

TOPIC	**An Assessment of Cyber Attacks Preparedness Strategy for Public and Sectors Private in Zambia**
RESEARCHER	**KINGSTONE ALI MWILA** C/O University of Zambia School of Engineering Department of Electrical & Electronic Engineering Great East Campus, Lusaka +260977689574; +260955689574
DATE	2019

Dear Participant,

You have been selected to participate in the University of Zambia academic research study which seeks to "**An Assessment of Cyber Attacks Preparedness Strategy for Private and Public Sectors in Zambia"**. The central goal of the research is to explore the resilience, performance and functioning of cybersecurity in the delivery of critical infrastructure and services to the nation.

To participate in this study, simply fill out the assessment questionnaire attached to this letter. You will be required to read the question or statement provided and then judge the question or statement provided and rate based on the extent to which you agree.

The purpose of the study will be to **An Assessment of Cyber Attacks Preparedness Strategy for Private and Public Sectors in Zambia**. In addition, the study will also explore the effects of cybersecurity on service quality delivery in relation to confidentiality, integrity and availability. Therefore, your honest and open participation is vital to our ability to accurately discover the above phenomena.

I anticipate that this survey should take no more than 20 minutes to complete. You may choose to skip any question you feel uncomfortable in answering. While you may not experience direct benefits from participation, information collected in this study will benefits UNZA for academic purposes. Return of the questionnaire will be considered consent. Participation in this survey is completely voluntary. All questionnaires are received anonymously and will be treated as such. Thank you for your participation!

If you have any comments, questions, or concerns with regards to the survey, the questions, or the purpose of the study, please contact Kingstone Ali Mwila on email kingstonmwila@gmail.com, mobile phone number + 26077689574 or +260955689574.

Yours Faithfully

Kingstone Ali Mwila

Student – Master of Engineering in Information and Communications Technology Security University of Zambia, School of Engineering, Department of Electrical & Electronics Engineering, Great East Campus, Lusaka.

PART A

General Information

1. Your Age …..?

15 – 25	26 – 35	36 – 45	46 – Above	Preferred not to say

2. What is your gender?

Male	Female	Preferred not to say

3. What is your position …….?

Lower Management	Middle Management	Senior Management	Others

4. Which department do you work under?

Human Resources	Information Technology	Operations	Executive Management	Marketing	Audit	Cyber Security	Finance/ Accounting	Others

5. How many years have you worked with the organisation?

0 - 3 years	4 – 6 years	7 - 9 years	10 years and above

6. What is the terms of employment that the organisation offer?

Permanent	Probationary	Temporal	Contract

7. What is the level of your education?

PhD	Masters	Degree	Diploma	Certificate	Others

PART B

Cyber-Attacks Preparedness Survey

1. Which of the following, if any, does your organisation currently have or use?

	Email addresses for organisation or employees
	Website or blog
	Online Bank Accounts
	Social media pages or accounts
	Customers Information
	Ability for customers to order, book or pay online
	Online Payments
	Data Centres
	Industrial control systems
	Others

2. How high or low a priority is cyber security to your organisation's directors, trustees or management

Very high	fairly high	fairly low	very low	do not know

3. How high or low a capability to attack back the intrude on the network

Very high	fairly high	fairly low	very low	do not know

4. Approximately how often, if at all, are your organisation's directors or senior management given an update on any actions taken around cyber security?

Never	less than once a year	annually	quarterly	monthly	weekly	daily	Each time there is a breach	do not know

a. Has your organisation sought information, advice or guidance in the last 12 months on the cyber security threats faced?

Yes	No	Not Sure

b. Awareness of Government cyber security initiatives and accreditation schemes.

Yes	No	Not Sure

c. Awareness on Investment in cyber security

Yes	No	Not Sure

d. What is the estimated investment (ZMW) in cyber security in last financial year?

More than 500,000,000	400,000,000	300,000,000	200,000,000	100,000,000	80,000,000	60,000,000	40,000,000	Less than 20,000	Not sure

5. What are the main reasons that your organisation invests in cyber security?

	Protecting customer or donor data.
	Protecting trade secrets, intellectual property or other assets (cash)*

	Business continuity or preventing downtime.
	Preventing fraud or theft.
	Protecting our staff and systems.
	Protecting reputation or brand.
	Customers or donors require it.
	Complying with laws or regulations.

6. How much do you agree or disagree with the following statements?

We have the knowledge and understanding we need to make an informed choice between outsourced cyber security providers.

Strongly agree	tend to agree	neither agree nor disagree	tend to disagree	strongly disagree	do not know	agree

7. How much do you agree or disagree with the following statements?

We have enough people dealing with cyber security in our organisation to effectively manage the risks.

Strongly agree	tend to agree	neither agree nor disagree	tend to disagree	strongly disagree	do not know	agree

8. How much do you agree or disagree with the following statements?

The people dealing with cyber security in our organisation have the right cyber security skills and knowledge to do this job effectively.

Strongly agree	tend to agree	neither agree nor disagree	tend to disagree	strongly disagree	do not know	agree

9. Organisations where staff have had cyber security training in the last 12 months?

Yes	No	Not Sure

10. Who in your organisation attended any of the training, seminars or conferences over the last 12 months?

	Directors or Senior Management
	IT Department
	Staff members whose job role includes governance
	IT/IS Auditors
	Cyber Security Department
	Others

11. Whether organisations have formal policies or document cyber security risks in any way

Yes	No	Not Sure

12. Which of the following, if any, are covered within your cyber security-related policies?

	What staff are permitted to do on the IT system of your organisation?

	Devices Remote or mobile working.
	Document management system.
	What can be stored on removable devices (example USB sticks).
	Use of personally-owned devices for business activities.
	Use of new digital technologies such as cloud computing Data classification.
	Others (Specify)

13. Which of the following, if any, have you done over the last 12 months to identify cyber security risks?

	Business-as-usual health checks that are undertaken regularly
	Risk assessment covering cyber security risks
	Ad-hoc health checks or reviews beyond regular processes Internal audit
	External audit
	Invested in threat intelligence to your organisation?
	Others

14. Which of the following rules or controls, if any, do you have in place?

	Applying software updates when they are available
	Up-to-date Antivirus/malware protection
	Firewalls with appropriate configuration
	Restricting IT admin and access rights to specific users
	Backing up data securely via other means

	Guidance on acceptably strong passwords
	Only allowing access via company owned devices
	Security controls on company owned devices (example laptops)
	Backing up data securely via a cloud service
	Monitoring of user activity
	Encryption of data
	Segregated wireless network
	Data Loss Detection/Prevention Rules
	Access/Role based rules
	Others (Specify)

15. Which of the following, if any, do you require your organisation and suppliers to have or adhere to?

	Payment Card Industry Data
	Security Standard (PCI DSS)
	Recognised standard such as ISO 27000 Series
	Independent service auditor's report (example ISAE 3402)
	Cyber Essentials
	COBIT
	Cyber Essentials Plus
	Others

16. Have any of the following happened to your organisation in the last 12 months?

	Fraudulent emails or being directed to fraudulent websites
	Others impersonating organisation in emails or online
	Viruses, spyware or malware
	Ransomware
	Unauthorised use of computers, networks or servers by outsiders
	Denial-of-service attacks
	Hacking or attempted hacking of online bank accounts
	Unauthorised use of computers, networks or servers by staff
	Any other breaches or attacks (Specify)

17. What was the one cyber security breach, or related series of breaches or attacks, that caused the most disruption to your organisation in the last 12 months?

	Fraudulent emails or being directed to fraudulent websites
	Others impersonating organisation in emails or online
	Viruses, spyware or malware
	Organisation in emails or online
	Ransomware
	Unauthorised use of computers, networks or servers by outsiders
	Denial-of-service attacks
	Hacking or attempted hacking of online bank accounts
	Unauthorised use of computers, networks or servers by staff
	Unauthorised use of computers, networks or servers by outsiders
	Any other breaches or attacks (Specify)

18. Approximately how often in the last 12 months did you experience cyber security breaches or attacks?

Only once	less than once a month	once a month	once a week	once a day	Several times a day	do not know

19. Thinking of all the cyber security breaches or attacks experienced in the last 12 months, which, if any, of the following happened as a result?

	Temporary loss of access to files or networks
	Software or systems corrupted or damaged
	Website or online services taken down or slowed
	Lost access to relied-on third party services Permanent loss of files (not personal data)
	Money stolen
	Lost or stolen assets, trade secrets or intellectual property
	Others

20. Have the breaches or attacks experienced in the last 12 months impacted your organisation in any of the following ways, or not?

	New measures needed for future attacks.
	Added staff time to deal with breach or inform others.
	Stopped staff carrying out daily work
	Other repair or recovery costs

	Prevented provision of goods and services
	Complaints from customers
	Loss of revenue or share value
	Discouraged from carrying out intended future business activity
	Reputational damage
	Goodwill compensation to customers
	Fines or legal costs

21. How long, if any time at all, did it take to restore business operations back to normal after the (most disruptive) breach or attack was identified?

No time at all	less than a day	less than a week	less than month	one month or more (or still not back to normal)	do not know

22. Average amount in Zambian Kwacha (ZMW) spent dealing with the most disruptive breach of last 12 months.

More than 1,000,000	400,000,000	300,000,000	200,000,000	100,000,000	80,000,000	60,000,000	40,000 000	Less than 20,000	Not sure

23. Average cost (ZMW) of all breaches or attacks identified in the last 12 months.

More than 1,000,000	400,000	300,000	200,000	100,000	80,000	60,000	40,000	Less than 20,000	Not sure

24. Average direct cost (ZMW) of the most disruptive breach from the last 12 months.

More than 1,000,000	400,000	300,000	200,000	100,000	80,000	60,000	40,000	Less than 20,000	Not sure

25. Average recovery cost (ZMW) of the most disruptive breach from the last 12 months.

More than 1,000,000	400,000	300,000	200,000	100,000	80,000	60,000	40,000	Less than 20,000	Not sure

26. Average estimated long-term cost (ZMW) of the most disruptive breach from the last 12 months.

More than 1,000,000	400,000	300,000	200,000	100,000	80,000	60,000	40,000	Less than 20,000	Not sure

27. How long was it, if any time at all, between this breach and attack occurring and it being identified as a breach?

Immediately	within 24 hours	within a week	longer than a week	Don’t know

28. Who was this (most disruptive) breach or attack reported to?

	Internet service provider
	Zambia Police Service
	Bank, building society or Credit Card Company
	Customers
	Action Fraud
	Website administrator
	Suppliers
	Company that was source of breach
	Regulators
	Chief Information Security Officer
	IT Department
	Cyber Security Department
	Chief Executive Officer
	Others (Specify)

a. Do you have or aware of the reporting procedure of any suspicious or cyber security breach in your organisation?

Yes	No

29. Do your organisation have a cyber security emergency response team?

Yes	No	Not sure

30. What, if anything, have you done since this (most disruptive) breach or attack to prevent or protect your organisation from further breaches like this?

	Installed, changed or updated antivirus or anti-malware software
	Additional staff training or communications
	Changed or updated firewall or system configurations
	Created or changed policies and procedures
	Hired an outsourced cyber security provider
	No action taken
	Others (Specify)

31. What is the size of your organisation?

Less than 50 employees	51 – 200 employees	More than 200 employees

32. Please state your industry……..

	Health
	Banking and financial Services
	Consumer services and products
	Manufacturing
	Mining, construction and engineering

	Government agencies, defence, regulator
	ICT, ISP, Telecoms
	Energy, power, oil, utility
	Others (Specify)

33. Number of Cyber security staff in your organisation

0	1 – 5	6 – 10	11 – Above	Not sure

34. Do you have a cyber security department in your organisation?

Yes	No	Not sure	maybe

35. Do you consider your organisation infrastructure and or services are critical to the nation?

Yes	No	Not sure	maybe

36. Which of the following security mechanism and technique is high regards in your organisation?

	Application and Data security (times patching, sensitive data and more)
	Hosting security (times patching of antivirus, restrict unwanted services, read/write protect etc.)
	Network security (corporate +ICS); firewall, sandboxing, IDS/IPS, VPN, Monitoring and filtering
	Physical security (ID Cards, CCTV, Fences, biometrics)

	Policies and procedures (risk management, incident response management, supply response management, audit and more)

37. In your own opinion, you do agree or disagree if your organisation have cybersecurity strategy?

Strongly agree	Disagree	Neutral	Agree	Strongly agree

38. How often do you perform cyber security (penetration) testing in your network?

Annually	Twice a year	Quarterly	Monthly	Not sure	never

PART C

Section 2.

In your view what do you think has been the cybersecurity challenges that affect service delivery in Zambia?

……

……

Section 3.

In your view or opinions what measures if any can improve on cyber warfare preparedness to protect critical infrastructures and services for the effectiveness and efficient of Service delivery in Zambia?

……

……

I thank you for your participation. Note, the answers you provided in this survey will remain anonymous.

Appendix II: Introductory Letters

THE UNIVERSITY OF ZAMBIA
SCHOOL OF ENGINEERING
OFFICE OF THE DEAN

Great East Road Campus | P.O. Box 32379 | Lusaka 10101 | Tel: (+260)-211-293 792 | 290 929 | 290 962
Fax: (+260)-211-293 793 | 290 962 | Email: dean-eng@unza.zm | info-eng@unza.zm | Website: www.unza.zm

27th March, 2019

The Director of Human Resource
Officer of the Auditor General
LUSAKA

Dear Sir/Madam,

RE: KINGSTONE ALI MWILA - 2017015312

This is to confirm that the bearer of this letter **Mr. Kingstone Ali Mwila** is a Master of Engineering Student in Master of Engineering in Information and Communication Technology Security, in the School of Engineering, Electrical and Electronics Engineering.

He is currently conducting a research titled **"An Assessment of Cyber Attacks Preparedness Strategy for Public and Sectors Private in Zambia".**

We will be most grateful for any assistance you may render to him as he carrics out this acadcmic assignmcnt.

The school commits itself to have the information used strictly for education research purposes only and be kept confidential within UNZA itself.

Yours faithfully,

Dr. Charles Kahanji
ACTING ASSISTANT DEAN (PG) – SCHOOL OF ENGINEERING

Cc Dean, School of Engineering

Excellence in Teaching, Research and Community Service

THE UNIVERSITY OF ZAMBIA
SCHOOL OF ENGINEERING
OFFICE OF THE DEAN

Great East Road Campus | P.O. Box 32379 | Lusaka 10101 | Tel: (+260)-211-293 792 | 290 929 | 290 962
Fax: (+260)-211-293 793 | 290 962 | Email: dean-eng@unza.zm | info-eng@unza.zm | Website: www.unza.zm

27th March, 2019

The Director of Human Resource
National Road Funds Agency HQ
LUSAKA

Dear Sir/Madam,

RE: KINGSTONE ALI MWILA - 2017015312

This is to confirm that the bearer of this letter **Mr. Kingstone Ali Mwila** is a Master of Engineering Student in Master of Engineering in Information and Communication Technology Security, in the School of Engineering, Electrical and Electronics Engineering.

He is currently conducting a research titled **"An Assessment of Cyber Attacks Preparedness Strategy for Public and Sectors Private in Zambia".**

We will be most grateful for any assistance you may render to him as he carries out this academic assignment.

The school commits itself to have the information used strictly for education research purposes only and be kept confidential within UNZA itself.

Yours faithfully,

Dr. Charles Kahanji
ACTING ASSISTANT DEAN (PG) – SCHOOL OF ENGINEERING

Cc Dean, School of Engineering

THE UNIVERSITY OF ZAMBIA
SCHOOL OF ENGINEERING
OFFICE OF THE DEAN

Great East Road Campus | P.O. Box 32379 | Lusaka 10101 | Tel: (+260)-211-293 792 | 290 929 | 290 962
Fax: (+260)-211-293 793 | 290 962 | Email: dean-eng@unza.zm | info-eng@unza.zm | Website: www.unza.zm

27th March, 2019

The Human Resource Manager
PWC Zambia
LUSAKA

Dear Sir/Madam,

RE: KINGSTONE ALI MWILA - 2017015312

This is to confirm that the bearer of this letter **Mr. Kingstone Ali Mwila** is a Master of Engineering Student in Master of Engineering in Information and Communication Technology Security, in the School of Engineering, Electrical and Electronics Engineering.

He is currently conducting a research titled **"An Assessment of Cyber Attacks Preparedness Strategy for Public and Sectors Private in Zambia".**

We will be most grateful for any assistance you may render to him as he carries out this academic assignment.

The school commits itself to have the information used strictly for education research purposes only and be kept confidential within UNZA itself.

Yours faithfully,

Dr. Charles Kahanji
ACTING ASSISTANT DEAN (PG) – SCHOOL OF ENGINEERING

Cc Dean, School of Engineering

THE UNIVERSITY OF ZAMBIA
SCHOOL OF ENGINEERING
OFFICE OF THE DEAN

Great East Road Campus | P.O. Box 32379 | Lusaka 10101 | Tel: (+260)-211-293 792 | 290 929 | 290 962
Fax: (+260)-211-293 793 | 290 962 | Email: dean-eng@unza.zm | info-eng@unza.zm | Website: www.unza.zm

27th March, 2019

The Director of Human Resource
ZESCO Limited
LUSAKA

Dear Sir/Madam,

RE: KINGSTONE ALI MWILA - 2017015312

This is to confirm that the bearer of this letter **Mr. Kingstone Ali Mwila** is a Master of Engineering Student in Master of Engineering in Information and Communication Technology Security, in the School of Engineering, Electrical and Electronics Engineering.

He is currently conducting a research titled **"An Assessment of Cyber Attacks Preparedness Strategy for Public and Sectors Private in Zambia".**

We will be most grateful for any assistance you may render to him as he carries out this academic assignment.

The school commits itself to have the information used strictly for education research purposes only and be kept confidential within UNZA itself.

Yours faithfully,

Dr. Charles Kahanji
ACTING ASSISTANT DEAN (PG) – SCHOOL OF ENGINEERING

Cc Dean, School of Engineering

THE UNIVERSITY OF ZAMBIA
SCHOOL OF ENGINEERING
OFFICE OF THE DEAN

Great East Road Campus | P.O. Box 32379 | Lusaka 10101 | Tel: (+260)-211-293 792 | 290 929 | 290 962
Fax: (+260)-211-293 793 | 290 962 | Email: dean-eng@unza.zm | info-eng@unza.zm | Website: www.unza.zm

27th March, 2019

The Director of Human Resource
National Assembly of Zambia
LUSAKA

Dear Sir/Madam,

RE: KINGSTONE ALI MWILA - 2017015312

This is to confirm that the bearer of this letter **Mr. Kingstone Ali Mwila** is a Master of Engineering Student in Master of Engineering in Information and Communication Technology Security, in the School of Engineering, Electrical and Electronics Engineering.

He is currently conducting a research titled **"An Assessment of Cyber Attacks Preparedness Strategy for Public and Sectors Private in Zambia".**

We will be most grateful for any assistance you may render to him as he carries out this academic assignment.

The school commits itself to have the information used strictly for education research purposes only and be kept confidential within UNZA itself.

Yours faithfully,

Dr. Charles Kahanji
ACTING ASSISTANT DEAN (PG) – SCHOOL OF ENGINEERING

Cc Dean, School of Engineering

THE UNIVERSITY OF ZAMBIA
SCHOOL OF ENGINEERING
OFFICE OF THE DEAN

Great East Road Campus | P.O. Box 32379 | Lusaka 10101 | Tel: (+260)-211-293 792 | 290 929 | 290 962
Fax: (+260)-211-293 793 | 290 962 | Email: dean-eng@unza.zm | info-eng@unza.zm | Website: www.unza.zm

27th March, 2019

The Director of Human Resource
Energy Regulations Board
LUSAKA

Dear Sir/Madam,

RE: KINGSTONE ALI MWILA - 2017015312

This is to confirm that the bearer of this letter **Mr. Kingstone Ali Mwila** is a Master of Engineering Student in Master of Engineering in Information and Communication Technology Security, in the School of Engineering, Electrical and Electronics Engineering.

He is currently conducting a research titled **"An Assessment of Cyber Attacks Preparedness Strategy for Public and Sectors Private in Zambia".**

We will be most grateful for any assistance you may render to him as he carries out this academic assignment.

The school commits itself to have the information used strictly for education research purposes only and be kept confidential within UNZA itself.

Yours faithfully,

Dr. Charles Kahanji
ACTING ASSISTANT DEAN (PG) – SCHOOL OF ENGINEERING

Cc Dean, School of Engineering

THE UNIVERSITY OF ZAMBIA
SCHOOL OF ENGINEERING
OFFICE OF THE DEAN

Great East Road Campus | P.O. Box 32379 | Lusaka 10101 | Tel: (+260)-211-293 792 | 290 929 | 290 962
Fax: (+260)-211-293 793 | 290 962 | Email: dean-eng@unza.zm | info-eng@unza.zm | Website: www.unza.zm

27th March, 2019

The Director Human Resource
Zambia Information and Communications Technology Authority
LUSAKA

Dear Sir/Madam,

RE: KINGSTONE ALI MWILA - 2017015312

This is to confirm that the bearer of this letter **Mr. Kingstone Ali Mwila** is a Master of Engineering Student in Master of Engineering in Information and Communication Technology Security, in the School of Engineering, Electrical and Electronics Engineering.

He is currently conducting a research titled **"An Assessment of Cyber Attacks Preparedness Strategy for Public and Sectors Private in Zambia".**

We will be most grateful for any assistance you may render to him as he carries out this academic assignment.

The school commits itself to have the information used strictly for education research purposes only and be kept confidential within UNZA itself.

Yours faithfully,

Dr. Charles Kahanji
ACTING ASSISTANT DEAN (PG) – SCHOOL OF ENGINEERING

Cc Dean, School of Engineering

THE UNIVERSITY OF ZAMBIA
SCHOOL OF ENGINEERING
OFFICE OF THE DEAN

Great East Road Campus | P.O. Box 32379 | Lusaka 10101 | Tel: (+260)-211-293 792 | 290 929 | 290 962
Fax: (+260)-211-293 793 | 290 962 | Email: dean-eng@unza.zm | info-eng@unza.zm | Website: www.unza.zm

27th March, 2019

The Chief Human Resource & Administration Officer
Zambia Telecommunication Company, HQ
LUSAKA

Dear Sir/Madam,

RE: KINGSTONE ALI MWILA - 2017015312

This is to confirm that the bearer of this letter **Mr. Kingstone Ali Mwila** is a Master of Engineering Student in Master of Engineering in Information and Communication Technology Security, in the School of Engineering, Electrical and Electronics Engineering.

He is currently conducting a research titled **"An Assessment of Cyber Attacks Preparedness Strategy for Public and Sectors Private in Zambia".**

We will be most grateful for any assistance you may render to him as he carries out this academic assignment.

The school commits itself to have the information used strictly for education research purposes only and be kept confidential within UNZA itself.

Yours faithfully,

Dr. Charles Kahanji
ACTING ASSISTANT DEAN (PG) – SCHOOL OF ENGINEERING

Cc Dean, School of Engineering

THE UNIVERSITY OF ZAMBIA
SCHOOL OF ENGINEERING
OFFICE OF THE DEAN

Great East Road Campus | P.O. Box 32379 | Lusaka 10101 | Tel: (+260)-211-293 792 | 290 929 | 290 962
Fax: (+260)-211-293 793 | 290 962 | Email: dean-eng@unza.zm | info-eng@unza.zm | Website: www.unza.zm

27th March, 2019

The Director of Human Resource
Bank of Zambia
LUSAKA

Dear Sir/Madam,

RE: KINGSTONE ALI MWILA - 2017015312

This is to confirm that the bearer of this letter **Mr. Kingstone Ali Mwila** is a Master of Engineering Student in Master of Engineering in Information and Communication Technology Security, in the School of Engineering, Electrical and Electronics Engineering.

He is currently conducting a research titled **"An Assessment of Cyber Attacks Preparedness Strategy for Public and Sectors Private in Zambia".**

We will be most grateful for any assistance you may render to him as he carries out this academic assignment.

The school commits itself to have the information used strictly for education research purposes only and be kept confidential within UNZA itself.

Yours faithfully,

Dr. Charles Kahanji
ACTING ASSISTANT DEAN (PG) – SCHOOL OF ENGINEERING

Cc Dean, School of Engineering

THE UNIVERSITY OF ZAMBIA
SCHOOL OF ENGINEERING
OFFICE OF THE DEAN

Great East Road Campus | P.O. Box 32379 | Lusaka 10101 | Tel: (+260)-211-293 792 | 290 929 | 290 962
Fax: (+260)-211-293 793 | 290 962 | Email: dean-eng@unza.zm | info-eng@unza.zm | Website: www.unza.zm

27th March, 2019

The Director of Human Resource
Bankers Association of Zambia
LUSAKA

Dear Sir/Madam,

RE: KINGSTONE ALI MWILA - 2017015312

This is to confirm that the bearer of this letter **Mr. Kingstone Ali Mwila** is a Master of Engineering Student in Master of Engineering in Information and Communication Technology Security, in the School of Engineering, Electrical and Electronics Engineering.

He is currently conducting a research titled **"An Assessment of Cyber Attacks Preparedness Strategy for Public and Sectors Private in Zambia".**

We will be most grateful for any assistance you may render to him as he carries out this academic assignment.

The school commits itself to have the information used strictly for education research purposes only and be kept confidential within UNZA itself.

Yours faithfully,

Dr. Charles Kahanji
ACTING ASSISTANT DEAN (PG) – SCHOOL OF ENGINEERING

Cc Dean, School of Engineering

THE UNIVERSITY OF ZAMBIA
SCHOOL OF ENGINEERING
OFFICE OF THE DEAN

Great East Road Campus | P.O. Box 32379 | Lusaka 10101 | Tel: (+260)-211-293 792 | 290 929 | 290 962
Fax: (+260)-211-293 793 | 290 962 | Email: dean-eng@unza.zm | info-eng@unza.zm | Website: www.unza.zm

27th March, 2019

The Director of Human Resource
Lusaka Water and Sewerage Company
LUSAKA

Dear Sir/Madam,

RE: KINGSTONE ALI MWILA - 2017015312

This is to confirm that the bearer of this letter **Mr. Kingstone Ali Mwila** is a Master of Engineering Student in Master of Engineering in Information and Communication Technology Security, in the School of Engineering, Electrical and Electronics Engineering.

He is currently conducting a research titled **"An Assessment of Cyber Attacks Preparedness Strategy for Public and Sectors Private in Zambia".**

We will be most grateful for any assistance you may render to him as he carries out this academic assignment.

The school commits itself to have the information used strictly for education research purposes only and be kept confidential within UNZA itself.

Yours faithfully,

Dr. Charles Kahanji
ACTING ASSISTANT DEAN (PG) – SCHOOL OF ENGINEERING

Cc Dean, School of Engineering

THE UNIVERSITY OF ZAMBIA
SCHOOL OF ENGINEERING
OFFICE OF THE DEAN

Great East Road Campus | P.O. Box 32379 | Lusaka 10101 | Tel: (+260)-211-293 792 | 290 929 | 290 962
Fax: (+260)-211-293 793 | 290 962 | Email: dean-eng@unza.zm | info-eng@unza.zm | Website: www.unza.zm

27th March, 2019

The Director of Human Resource
National Water and Sanitation Council of Zambia
LUSAKA

Dear Sir/Madam,

RE: KINGSTONE ALI MWILA - 2017015312

This is to confirm that the bearer of this letter **Mr. Kingstone Ali Mwila** is a Master of Engineering Student in Master of Engineering in Information and Communication Technology Security, in the School of Engineering, Electrical and Electronics Engineering.

He is currently conducting a research titled **"An Assessment of Cyber Attacks Preparedness Strategy for Public and Sectors Private in Zambia".**

We will be most grateful for any assistance you may render to him as he carries out this academic assignment.

The school commits itself to have the information used strictly for education research purposes only and be kept confidential within UNZA itself.

Yours faithfully,

Dr. Charles Kahanji
ACTING ASSISTANT DEAN (PG) – SCHOOL OF ENGINEERING

Cc Dean, School of Engineering

THE UNIVERSITY OF ZAMBIA
SCHOOL OF ENGINEERING
OFFICE OF THE DEAN

Great East Road Campus | P.O. Box 32379 | Lusaka 10101 | Tel: (+260)-211-293 792 | 290 929 | 290 962
Fax: (+260)-211-293 793 | 290 962 | Email: dean-eng@unza.zm | info-eng@unza.zm | Website: www.unza.zm

27th March, 2019

The Director of C.I.D
Zambia Police Service
ZP HQ
LUSAKA

Dear Sir/Madam,

RE: KINGSTONE ALI MWILA - 2017015312

This is to confirm that the bearer of this letter **Mr. Kingstone Ali Mwila** is a Master of Engineering Student in Master of Engineering in Information and Communication Technology Security, in the School of Engineering, Electrical and Electronics Engineering.

He is currently conducting a research titled **"An Assessment of Cyber Attacks Preparedness Strategy for Public and Sectors Private in Zambia".**

We will be most grateful for any assistance you may render to him as he carries out this academic assignment.

The school commits itself to have the information used strictly for education research purposes only and be kept confidential within UNZA itself.

Yours faithfully,

Dr. Charles Kahanji
ACTING ASSISTANT DEAN (PG) – SCHOOL OF ENGINEERING

Cc Dean, School of Engineering

THE UNIVERSITY OF ZAMBIA
SCHOOL OF ENGINEERING
OFFICE OF THE DEAN

Great East Road Campus | P.O. Box 32379 | Lusaka 10101 | Tel: (+260)-211-293 792 | 290 929 | 290 962
Fax: (+260)-211-293 793 | 290 962 | Email: dean-eng@unza.zm | info-eng@unza.zm | Website: www.unza.zm

27th March, 2019

The Human Resource Manager
Zambia National Data Centre
LUSAKA

Dear Sir/Madam,

RE: KINGSTONE ALI MWILA - 2017015312

This is to confirm that the bearer of this letter **Mr. Kingstone Ali Mwila** is a Master of Engineering Student in Master of Engineering in Information and Communication Technology Security, in the School of Engineering, Electrical and Electronics Engineering.

He is currently conducting a research titled **"An Assessment of Cyber Attacks Preparedness Strategy for Public and Sectors Private in Zambia".**

We will be most grateful for any assistance you may render to him as he carries out this academic assignment.

The school commits itself to have the information used strictly for education research purposes only and be kept confidential within UNZA itself.

Yours faithfully,

Dr. Charles Kahanji
ACTING ASSISTANT DEAN (PG) – SCHOOL OF ENGINEERING

Cc Dean, School of Engineering

THE UNIVERSITY OF ZAMBIA
SCHOOL OF ENGINEERING
OFFICE OF THE DEAN

Great East Road Campus | P.O. Box 32379 | Lusaka 10101 | Tel: (+260)-211-293 792 | 290 929 | 290 962
Fax: (+260)-211-293 793 | 290 962 | Email: dean-eng@unza.zm | info-eng@unza.zm | Website: www.unza.zm

27th March, 2019

The Human Resource Manager
Smart Zambia Institute
LUSAKA

Dear Sir/Madam,

RE: KINGSTONE ALI MWILA - 2017015312

This is to confirm that the bearer of this letter **Mr. Kingstone Ali Mwila** is a Master of Engineering Student in Master of Engineering in Information and Communication Technology Security, in the School of Engineering, Electrical and Electronics Engineering.

He is currently conducting a research titled **"An Assessment of Cyber Attacks Preparedness Strategy for Public and Sectors Private in Zambia".**

We will be most grateful for any assistance you may render to him as he carries out this academic assignment.

The school commits itself to have the information used strictly for education research purposes only and be kept confidential within UNZA itself.

Yours faithfully,

Dr. Charles Kahanji
ACTING ASSISTANT DEAN (PG) – SCHOOL OF ENGINEERING

Cc Dean, School of Engineering

THE UNIVERSITY OF ZAMBIA
SCHOOL OF ENGINEERING
OFFICE OF THE DEAN

Great East Road Campus | P.O. Box 32379 | Lusaka 10101 | Tel: (+260)-211-293 792 | 290 929 | 290 962
Fax: (+260)-211-293 793 | 290 962 | Email: dean-eng@unza.zm | info-eng@unza.zm | Website: www.unza.zm

27th March, 2019

The Human Resource Manager
KPMG Zambia
LUSAKA

Dear Sir/Madam,

RE: KINGSTONE ALI MWILA - 2017015312

This is to confirm that the bearer of this letter **Mr. Kingstone Ali Mwila** is a Master of Engineering Student in Master of Engineering in Information and Communication Technology Security at the University of Zambia, in the School of Engineering, Department of Electrical and Electronics Engineering.

He is currently conducting a research titled **"An Assessment of Cyber Attacks Preparedness Strategy for Public and Sectors Private in Zambia".**

We will be most grateful for any assistance you may render to him as he carries out this academic assignment.

The School commits itself to have the information used strictly for education research purposes only and be kept confidential within UNZA itself.

Yours faithfully,

Dr. Charles Kahanji
ACTING ASSISTANT DEAN (POST GRADUATE) - SCHOOL OF ENGINEERING

Cc Dean, School of Engineering

THE UNIVERSITY OF ZAMBIA
SCHOOL OF ENGINEERING
OFFICE OF THE DEAN

Great East Road Campus | P.O. Box 32379 | Lusaka 10101 | Tel: (+260)-211-293 792 | 290 929 | 290 962
Fax: (+260)-211-293 793 | 290 962 | Email: dean-eng@unza.zm | info-eng@unza.zm | Website: www.unza.zm

27th March, 2019

The Air Force Commander
ZAF HQ
LUSAKA

Dear Sir/Madam,

RE: KINGSTONE ALI MWILA - 2017015312

This is to confirm that the bearer of this letter **Mr. Kingstone Ali Mwila** is a Master of Engineering Student in Master of Engineering in Information and Communication Technology Security, in the School of Engineering, Electrical and Electronics Engineering.

He is currently conducting a research titled **"An Assessment of Cyber Attacks Preparedness Strategy for Public and Sectors Private in Zambia".**

We will be most grateful for any assistance you may render to him as he carries out this academic assignment.

The school commits itself to have the information used strictly for education research purposes only and be kept confidential within UNZA itself.

Yours faithfully,

Dr. Charles Kahanji
ACTING ASSISTANT DEAN (PG) – SCHOOL OF ENGINEERING

Cc Dean, School of Engineering

THE UNIVERSITY OF ZAMBIA
SCHOOL OF ENGINEERING
OFFICE OF THE DEAN

Great East Road Campus | P.O. Box 32379 | Lusaka 10101 | Tel: (+260)-211-293 792 | 290 929 | 290 962
Fax: (+260)-211-293 793 | 290 962 | Email: dean-eng@unza.zm | info-eng@unza.zm | Website: www.unza.zm

27th March, 2019

The Director of Human Resource
Electoral Commission of Zambia
LUSAKA

Dear Sir/Madam,

RE: KINGSTONE ALI MWILA - 2017015312

This is to confirm that the bearer of this letter **Mr. Kingstone Ali Mwila** is a Master of Engineering Student in Master of Engineering in Information and Communication Technology Security, in the School of Engineering, Electrical and Electronics Engineering.

He is currently conducting a research titled **"An Assessment of Cyber Attacks Preparedness Strategy for Public and Sectors Private in Zambia".**

We will be most grateful for any assistance you may render to him as he carries out this academic assignment.

The school commits itself to have the information used strictly for education research purposes only and be kept confidential within UNZA itself.

Yours faithfully,

Dr. Charles Kahanji
ACTING ASSISTANT DEAN (PG) – SCHOOL OF ENGINEERING

Cc Dean, School of Engineering

Appendix III: Introductory Letter Delivery Sign off Register

SN	Organization Name	Received by	Position	Signature	Date	
1	Zamtel	L. Mweemba	EA		29-5-19	
2	Zambia Police	M. Mwanda	A/D-Training		29.5.19	
3	NATIONAL ASSEMBLY	K. MUNTHALI	Asst Registry Sup		03/06/19	
4	Zieta	Faith Kalambeke	Receptionist		04.06.19	
5	~~Absa~~ Kenya ZNBC	Abel Kunda	Office Manager		04/06/19	
6	LUSC	M. Chibende	HR Assistant		05/06/2019	
7	ERB	N. Lisita	FDO		06.06.19	
8	PWC	M. Simaloka	Administrator		05.06.19	
9	KPMG	MWIINGA	RECEPTIONIST		05.06.19	
10	OAG	L. Mulala	Senior Auditor		06.06.19	
11	ZMAKI Zambia	Audrey Mwila	Snr HRMO		12.06.19	HRD
12	ZESCO	AGGIE	SECURITY		12/06/19	0211362513
13	ELECTORAL COMMISSION	P. LOUIE	REGISTRY OFFICER		12/06/19	253155
14	AIR FORCE ~~Headquarters~~	CAPT C MASA	REGISTRY OFFICER		18/06/19	0976157?4
15	NAPSA	cleopatra	FRONT OFFICE		20/6/19	211 253145
16	NWASCO	P. NKHOWANI	RECEPTIONIST		20/6/19	0211 226944
17	MIRRIAM Zimba	~~Engineers~~ Association of Zambia	PR & Admin. Office		26/06/19	0211 284208
18	BOZ	B. Sibalwa	Security Officer		26/06/19	0211 399 300

Appendix IV: Journal Publication Certificates

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN SCIENCE, ENGINEERING AND TECHNOLOGY

ISSN (Online) : 2319 – 8753 ISSN (Print) : 2347 - 6710

IJIRSET

PUBLICATION CERTIFICATE

This is to certify that

KINGSTONE ALI MWILA

P.G. Student, Department of Electrical and Electronics Engineering, School of Engineering, University of Zambia, Lusaka, Zambia

Published a research paper titled

"An Assessment of Cyber Attacks Preparedness Strategy for Public and Private Sectors in Zambia"

in IJIRSET, Volume 8, Issue 12, December 2019

Certificate No: V8I12C025
Date: 15th December 2019

IJIRSET
Impact Factor: 7.089
www.ijirset.com

Editor-in-Chief
IJIRSET

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN SCIENCE, ENGINEERING AND TECHNOLOGY

ISSN (Online) : 2319 – 8753 ISSN (Print) : 2347 - 6710

PUBLICATION CERTIFICATE

This is to certify that

CHARLES S. LUBOBYA

Head of Department, Department of Electrical and Electronics Engineering, School of Engineering, University of Zambia, Lusaka Zambia

Published a research paper titled

"An Assessment of Cyber Attacks Preparedness Strategy for Public and Private Sectors in Zambia"

in IJIRSET, Volume 8, Issue 12, December 2019

Certificate No: V8I12C026
Date: 15th December 2019

IJIRSET
Impact Factor: 7.089
www.ijirset.com

Editor-in-Chief
IJIRSET