CYBER SECURITY AS AN EMERGING THREAT TO KENYA'S NATIONAL SECURITY

by

Brian Njama Kiboi

Student Number: 29381097

Mini-dissertation submitted in partial fulfilment of the requirements

for the degree

Master of Security Studies (MSS),

Department of Political Sciences,

Faculty of Humanities, University of Pretoria

Supervisor: Prof. M Schoeman

Co-Supervisor: Mr R. Henwood

May 2015

DECLARATION

I declare that the dissertation, which I hereby submit for the degree Master of Security Studies at the University of Pretoria, is my own work and has not been previously submitted by me for a degree at this or any other tertiary institution.

Brian Njama Kiboi

May 2015

ABSTRACT

The rapid growth and development of the internet and information communications technology (ICT) has delivered economic growth at an unprecedented scale and enabled seamless connectivity across all corners of the world. However, this rapid growth has introduced new vulnerabilities in cyberspace. Cyber security threats are increasing and evolving at a rapid pace as the global economy, society and governments now rely heavily on ICT networks to communicate and perform essential functions on a daily basis. In addition, cyber attackers are constantly developing new sophisticated tools and methods aimed at damaging critical infrastructure, accessing sensitive information and stealing the intellectual property of governments, organisations and individuals. With the growing use of ICT globally, cyber security threats will continue to evolve and multiply, becoming even more dangerous than they are today.

This study focuses on emerging challenges within the cyber security environment that may pose a significant threat to Kenya's national security. Kenya has experienced remarkable growth in its ICT sector and it has positioned itself as a global ICT hub. Moreover, the Kenyan Government has underlined universal access to ICTs as a major objective of its economic blueprint, 'Vision 2030', in the hope of driving Kenya from a developing to a middle-income country. In this regard cyber security is of real importance to Kenya.

This study seeks to explain how the increased dependence on ICT and internet usage has exposed the Kenyan government, private sector and society to premeditated cyber security risks with possibly disastrous effects on the social, political and economic spheres of the state. The methodology employed an extensive literature survey to explain Kenya's response to cyber security threats by analysing the various legal and policy regulatory frameworks that govern ICT and cyber security. The purpose of the study is to contribute to the wider intellectual discourse on cyber security and it is specifically aimed at enhancing Kenya's cyber security posture, in order to prevent cyber security from becoming a major threat to its national security.

KEY TERMS

National security, cyber security, human security, securitisation, cyberspace, internet, ICT, cybercrime, cyber-attack, malware, Kenya, cyber power, cyber terrorism, hacktivism.

ACKNOWLEDGEMENTS

I am sincerely thankful to my supervisor, Professor Maxi Schoeman, and my co-supervisor, Mr Roland Henwood, for their untiring commitment, expert guidance and supervision from the beginning to the final stages of this study. Completing this dissertation would have not been possible without them and they helped me develop an understanding of the subject.

I wish to express my sincere appreciation to my mentor Lieutenant-General (retired) Njuki Mwaniki, who has helped me throughout my dissertation. I am deeply grateful for his support and professional assistance in helping me complete my dissertation.

I wish to thank my parents, Lucy Kiboi and Dr. Julius Kiboi, my brother, George, my sister, Michelle, and the rest of my family and friends. I would like to thank you for your tireless support, prayers and words of encouragement throughout the course of this study.

Lastly, I offer my warmest regards and blessings to all those who supported me in any respect during the completion of this work.

TABLE OF CONTENTS

TABLE OF FIGURES

ABREVIATIONS/ ACCRONYMS

AMISOM	African Union Mission in Somalia
ARPANET	Advanced Research Projects Agency Network
BBC	British Broadcasting Corporation
BFID	Banking Fraud Investigations Department
CAGR	Compound Annual Growth Rate
CAK	Communications Authority of Kenya
CCDCOE	Cooperative Cyber Defence Centre of Excellence
CCK	Communication Commission of Kenya
CERN	European Organisation for Nuclear Research
CIRT	Computer Incident Response Team
CNN	Cable News Network
COE	Council of Europe
COMESA	Common Market for Eastern and Southern Africa
DDoS	Distributed denial-of-service
DoS	Denial-of-Service
EAC	East African Community
EACO	East African Communications Organisation
EU	European Union
EULA	End User License Agreement
GAC	Governmental Advisory Committee

Gbps	Gigabit per second
GCCN	Government Common Core Network
GDC	Government Data Centre
IBM	International Business Machines
ICANN	International Corporation for Assigned Names and Numbers
ICC	International Criminal Court
ICG	International Crisis Group
ICT	Information Communications Technology
ICTA	Information and Communication Technology Authority
IDC	International Data Corporation
IETF	Internet Engineering Task Force
IFMIS	Integrated Financial Management Information System
IGAD	Intergovernmental Authority on Development
IMPACT	International Multilateral Partnership against Cyber Threats
INTERPOL	International Criminal Police Organisation
ISIC	International Standard Industrial Classification of All Economic Activities
ISIS	Islamic State of Iraq and Syria
ISS	Institute for Security Studies
ITU	International Telecommunications Union
KCA	Kenya Communications Act
KDF	Kenya Defence Forces
KE-CIRT/CC	National Kenya Computer Incident Response Team Coordination Centre

KENET	Kenya Education Network
KENIC	Kenya Network Information Centre
KHRC	Kenya Human Rights Commission
KICR	Kenya Information and Communications Regulations
KRA	Kenya Revenue Authority
Mbps	Megabits per second
MNC	Multinational Corporation
NATO	North Atlantic Treaty Organisation
NCIC	National Cohesion and Integration Commission
NCS	National Cyber-security Strategy
NCSC	National Cyber Security Committee
NCSF	National Cyber Security Framework
NCSMP	National Cyber Security Master Plan
NEPAD	New Partnership for Africa’s Development
NKCC	National KE-CIRT/CC Cybersecurity Committee
NOFBI	National Optic Fibre Broadband Infrastructure
NPKI	National Public Key Infrastructure
NSAC	National Security Advisory Council
NSC	National Security Council
NSFNET	National Science Foundation Network
NSPCC	National Society for the Prevention of Cruelty to Children
OECD	Organisation for Economic Co-operation and Development

OS	Operating System
PC	Personal Computer
PKI	Public Key Infrastructure
RMA	Revolution in military affairs
SPLM	Sudanese People’s Liberation Movement
START	Study of Terrorism And Responses to Terrorism
TCP/IP	Transmission Control Protocol/ Internetwork Protocol
TESPOK	Telecommunication Service Providers Association of Kenya
UCLA	University of California at Los Angeles
UN	United Nations
UNDP	United Nations Development Program
UNIDR	United Nations Institute for Disarmament Research
UNODC	United Nations Office on Drugs and Crime
UNSC	United Nations Security Council
USCYBERCOM	United States Cyber Command
USDoD	United States Department of Defense
USG	University System of Georgia
WWW	World Wide Web

CHAPTER 1: INTRODUCTION

1.1. Identification of the Research Theme

The African continent is witnessing a rapid growth in the usage and dependence on Information Communications Technology (ICT) in both the public and private sector. The shrinking costs of ICTs have made this widespread and decentralised, reaching far beyond the political and economic elites of Western societies, greatly benefiting the developing world and specifically Africa in many ways. As stated by Internet World Stats (2013), by mid-2012 Africa had over 167 million internet users with Nigeria representing more than 48 million internet users which in turn attracted numerous international investors seeking new business opportunities across the continent. ICT Africa believes that Africa is being promoted as the next global technology hub and the continent is said to be on the brink of unprecedented growth and prosperity (Moeng 2011). Given that over 60 per cent of internet users are in developing countries and 45 per cent are below the age of 25 (UNODC 2013), internet penetration will grow significantly around the world and particularly in Africa. This rapid growth can be accredited to innovation. McAfee (2011), claims that "innovation has expanded the availability, use, and functionality of the internet at an amazing rate. Today, there are more than two billion internet users globally, a vast increase from the 361 million users online in 2000". This is evident in the growing number of mobile phone and internet users across Africa as people continue to become more and more dependent on such technologies for everyday use.

Since the year 2000, ICT has played a vital role in building Kenya's economy and is considered a main government priority in the realisation of national development goals and objectives for wealth and employment creation, as stipulated in the 'Kenya Vision 2030' National Development Plan (Kenya 2014c: 5).Kenya has been experiencing a rapid increase in internet penetration in the last few years with the overall internet usage becoming cheaper, better and faster. Currently, Kenya is connected to the rest of the world through four undersea cables that deliver a capacity with a speed of 5.7 terabytes per second, resulting in cheaper and faster internet connectivity (CCK 2013).

Such internet speeds enable large volumes of data to be sent and stored in an instant, improving the efficiency among internet users. Kenya is regarded as the pioneer of mobile money transfers with the development of M-Pesa (mobile money in Swahili), which was commercially launched in 2007. As of September 2014, there were an estimated 26.9 million mobile money subscribers and an estimated 23.2 million internet users (CAK 2015).Additionally, in 2013 the ICT market in Kenya reached a value of US$5.16 billion, of which telecommunication services accounted for 71.9 per cent, hardware made up 22.3 per cent, and IT services and software represented 3.0 per cent and 2.8 per cent, respectively. Spending is expected to continue growing over the forecast period to reach a value of US$5.86 billion in 2017 (IDC 2014: 5).

The figures above give us an indication that more Kenyans are embracing ICT as it improves their perceived quality of life. Furthermore, the rapid increase in the number of internet and cell phone users in Kenya has encouraged the public sector to digitise its services. In this regard, the Kenyan government has "developed a Government Common Core Network (GCCN) which is meant to serve as a shared and secure interoperable Government-wide ICT architecture" (Kenya 2014a: 25). In addition, the government claims "the system will not only integrate work processes and information flows, but also improve the inter-departmental sharing of databases and exchange of information in order to eliminate duplication and redundancies, improve public access to Government services and ensure responsiveness in reporting, monitoring and evaluation" (Kenya 2013).

The rapid growth of Kenya's ICT sector has made it a leading African ICT hub in innovative technologies, and Kenyans have quickly become dependent on the services provided to them through government and business websites, banking connectivity, and ease of communications (Kenya 2014c: 6). As a result of the tremendous productivity gains and new capabilities enabled by growth of ICT in Kenya, the Kenyan government has incorporated ICT into a vast number of applications and virtually every sector of the country's critical infrastructure including: health, security, agriculture, financial services, and trade (Serianu 2014: 4).

In this regard, the Kenyan government has "implemented electronic systems in various state departments and other state-owned institutions, including the national tax system, the immigration information system, the legal information system, the integrated financial management system and the education system" (Kenya 2014a: 28). Furthermore, the majority of these systems are situated in the National Treasury, Kenya Revenue Authority (KRA), Home Affairs Department and the Immigration Office (Kenya 2014a: 28). The Kenya Revenue Authority (KRA) for example, now offers online services such as submission of tax returns and payments, as well as tax related information to citizens and businesses. For government institutions such as the KRA, the internet is of considerable importance to the deployment of a national single window for trade facilitation, and the integration of customs, port and transit processes, which in turn ultimately reduces the costs for government and trading enterprises (KRA 2014).

However, the increased internet penetration and technological advancement in Kenya has exposed the country to cyber security threats. In 2014, Kenya witnessed a huge increase in cyber-attacks targeting both public and private organisations. Consequently, the increased dependence on ICT and internet usage has exposed the Kenyan government, private sector and society to premeditated security attacks and threats with possibly disastrous effects on the social, political and economic spheres of the state. In this regard, Kenya's rapid growth and dependence on ICT has made cyber security an emerging threat to its national security. In response to increasing online vulnerabilities, Kenya has put in place a national cyber-security strategy to protect the country's online assets and to guide the management of cyber security in the country (Itosno 2014).

1.2. Study Objectives

In view of the above, this study will explore current trends and emerging challenges within the cyber security environment that may pose a significant threat to Kenya's national security. An analysis of the broadening and deepening of the security agenda from the post-Cold War era to include non-military threats to national security is a further objective of this study, in order to contextualise the threat of cyber security in the 21st century.

The sub-objectives are:

- To distinguish between the various forms of cyber insecurity, as well as its development and sophistication over time; and

- To describe the threats posed by cyber security with regard to Kenya's national security.

1.3. Literature Overview

According to Leiner, et al. (2009: 23), the internet is at once a world-wide broadcasting capability, a mechanism for information dissemination, and a medium for collaboration and interaction between individuals and their computers without the regard for geographic location. Furthermore, the internet has become a widespread information infrastructure, from the initial model of what is often called the Global Information Infrastructure. Its history is complex and involves many technological and organisational aspects. Its influence reaches not only the technical fields of computer communications but throughout society as development towards the increasing use of online tools to accomplish electronic commerce, information acquisition and community operations evolves (Leiner, et al. 2009: 23).

Schreier (2012: 34) believes that "it is the internet's openness that carries downsides in that it makes it easier to attack applications and operating systems that are not adequately defended". Because it was designed as a decentralized system, internet users are functionally unknown and can generate information capable of travelling in undifferentiated packets, which can be encoded to hide the origin (Schreier 2012: 34). This obscurity provided by the design of the internet leads to an attribution challenge that renders most cyber-attacks difficult to trace. In this regard, establishing and confirming the identity of an attacker online can be a tedious process (Schreier 2012: 34).

In the same way that the internet and ICT provides new prospects for governments and businesses to operate and increase their presence, Choo (2011: 719) notes that "ICT also presents opportunities for those with criminal intentions and leaves individuals, communities, organisations and nations, highly exposed to the threat of a cyber-attack".

In this regard, Julisch (2013: 2206) has identified four anti-patterns that undermine the cyber security of organisations. These include: an overreliance on intuition to make security decisions, where decision-makers generally rely on their intuition and experience often fraught with cognitive-biases; leaving cracks in the security foundation, where organisations lack fundamental security controls; overreliance on knowledge versus intelligence, where organisations continue to rely too much on the relatively static knowledge within products and finally; weak governance, characterised by unclear decision rights and processes, creating systemic control gaps and vulnerabilities. For Pfleeger and Caputo (2012: 598), these are common problems found in both public and private sector organisations and could result in serious implications if not dealt with appropriately, because aspects of everyday life such as operation and defence of critical infrastructure, protection of national security information and the operation of financial markets involve both government regulation and private sector administration. Thus, any effective approach to cyber-security will require cooperation between the private and public sectors both in a domestic and international context.

Brechbhl, Bruce, Dynes & Johnson (2010: 89) point out that an "effective cyber security policy requires a wide range of international collaborative activities". These activities must occur at different levels within governments and private sector stake-holders, with such contacts being both bilateral and multilateral in nature. The reasons for these international collaborations include information sharing on risks, vulnerabilities and best practices, developing formal and informal working relationships with key stakeholders in other countries with comparable roles and responsibilities, and enabling the assessment of one's efforts against those of similar countries. International cooperation is therefore essential in minimising cyber security threats, as "attacks on systems connected to the internet can originate from anywhere on that network" (Brechbhl et al. 2010: 89). In addition, "vulnerabilities in software developed in one country and installed in a second can be exploited remotely from a third, and failures in critical information infrastructures in one nation can cascade into dependent systems elsewhere" (Bajaj: 2010).

This therefore requires a new examination of the regulatory norms, international legal norms and approaches to cyber security (Schreier 2012: 46). Some key improvements that could be made include: strengthening frameworks for international cooperation and capacity building, as well as increasing the number of signatories to the international cyberspace treaties such as the Cybercrime Convention initiated by the Council of Europe (COE). The Convention on Cybercrime came into force on 1 July 2004 and is considered to be the first international treaty on crimes committed through the internet and other computer networks. Its main objective is to pursue a common criminal policy aimed at the protection of society against cybercrime by adopting appropriate legislation as well as fostering international cooperation (Council of Europe 2014).

With this in mind, Brechbhl et al. (2010: 89) adds that many multinational and inter-governmental organisations including the United Nations (UN), the International Telecommunications Union (ITU), the Internet Engineering Task Force (IETF), the World

Bank, the Organisation for Economic Co-operation and Development (OECD), the European Union (EU), and the African Union (AU) all have a role in developing cyber-security policies and practices. The Global Regulatory Exchange of the ITU for example, could be an important platform for broadening the current global dialogue on cyber-security policy-making between telecom regulators and ICT ministers, if they widen their audience via the widespread internet community. International law and norms are therefore fundamental to the prevention of cyber-attacks because nation-states share a common interest in implementing common standards for the behaviour of international relations, and in encouraging or prohibiting specific kinds of behaviour (Freeman 1997: 84). Thus, the "lack of international norms, laws, and definitions to govern state action in cyberspace has led to a grey area that can be exploited by aggressive states as long as their actions skirt the imprecise thresholds contained in the UN Charter" (Tikk, Kaska, Runnimeri et al. 2008: 7).

The above sources are important in exploring the concept of cyber security. However, the literature does not clearly link cyber security to the broader discourse on strategic studies. In this regard, this study attempts to present a more integrated academic approach to the analysis of cyber security within the current global trends and emerging threats, and its impact on states' national security.

1.4. Formulation and Demarcation of the Research Problem

Based on the specified study objectives, the fundamental research problem this study addresses is whether current trends in cyber security pose significant threats and vulnerabilities to Kenya's national security. More specifically, the study addresses the following sub-problems:

- Cyber security as a national security threat
- The changing context of cyber security and the implications for Kenya
- An assessment of Kenya's response to potential cyber security threats.

In view of the research objectives formulated above, the study is based on the following assumptions:

- Cyber security threats are increasing and evolving at a rapid pace as the global economy, society and governments now rely heavily on ICT networks and systems for many essential functions every day.

- Kenya's rapid growth and dependence in ICT has made cyber security an emerging threat to its national security.

The study focuses on the period 2000 to 2014 as it is during this period that the internet and ICT witnessed an exponential growth globally and in Kenya, and has become a key driver of globalisation and economic growth as well as an important element of everyday life.

1.5. Research Methodology

The research methodology that this study uses entails an analysis of current trends and emerging challenges of the cyber security sector: an analysis of the evolution of cyber security, as well as an analysis of the threats posed by and responses to cyber-attacks. Furthermore, the proposed study will take on a qualitative and analytical research methodology by constituting a literature-based analysis of the current debates within the field of security studies in relation to cyber security.

The concepts of strategic studies and human security will be discussed in detail in order to convey the meaning and understanding of security in the 21st century. The case study is focused on cyber security as an emerging threat to Kenya's national security.

The study uses both primary and secondary sources. Primary sources will consist of various official government strategies, policies and documents pertaining to cyber security, such as the Constitution of Kenya (2010), the National Cyber Security Strategy for the Government of Kenya (2014), the Kenya Cyber Security Master plan (2013), the Communications Authority of Kenya Sector Statistics Report (2013-14), the Kenya ICT Master Plan (2014), as well as other important government documents related to cyber security. The secondary sources this research uses include; books, journal articles, opinion editorials, press releases and web-articles, which will be critically explored in a bid to identify the current trends and emerging challenges faced within cyber security.

A major challenge experienced in the course of this research was the limited number of primary sources and scholarly articles available on cyber security in Kenya. Furthermore, due to time and financial constraints, the researcher was unable to conduct field research and obtain first-hand information from cyber security experts in Kenya. As a result, the researcher had to rely extensively on government documents and secondary sources during the course of this research.

1.6. Research Structure

Chapter 1 serves as the introduction in order to clarify the scope and focus of the research. An initial overview will be presented and the research methodology will be explained.

Chapter 2 will present a conceptual overview of the traditional and modern conceptions of security by tracing how the concept has evolved from a traditional realist state-centric approach to security, to a more broadened and widened approach that includes non-military security threats. The concepts of strategic studies and human security will be discussed in order to explain the meaning and understanding of national security in the 21st century. A brief overview of Kenya's national security in relation to the traditional and modern conceptions of security will also be introduced in this chapter.

Chapter 3 will provide a historical overview of the development of cyber space to establish its evolution from the period when the internet became a breakthrough in the information revolution to the current use of cyberspace by certain entities for harmful, illegal activity capable of causing devastating effects to individuals and the state. The chapter then explores the current trends and threats posed by cyber security to determine the extent to which it threatens the national security of states.

Chapter 4 will analyse Kenya's ICT environment in order to determine what issues are perceived as threats to the country. Kenya's current cyber security situation will then be investigated, paying attention to how the growing use and dependence on ICT networks and cyberspace is threatening Kenya's national security.

Chapter 5 will focus on Kenya's response to cyber security threats by analysing the policies and legal framework relating to cyber security adopted by the Kenyan government through its constitution, national cyber security strategy and master plan, in order to determine how prepared the Kenyan government is prepared to deal with emerging cyber security threats and challenges. A conclusion of the study and further recommendations will also be given. This chapter will also present a summary of the research and findings of the preceding chapters in relation to the broad focus of the research problem formulated in the first chapter.

CHAPTER 2: TRADITIONAL AND MODERN CONCEPTIONS OF SECURITY

2.1. Introduction

In order to understand how cyber security relates to national security, this chapter will provide a conceptual overview of the notion of security by tracing how the concept has evolved from a traditional realist state-centric approach to security to a more broadened and deepened approach that includes non-military and individual security threats. The concepts of national security, national interest, the revolution in military affairs (RMA), securitisation theory, and human security will be discussed in order to explain the meaning and understanding of security in the 21st century. A brief overview of Kenya's national security in relation to the traditional and modern conceptions of security will also be introduced in this chapter.

2.2. Defining National Security

The concept of national security lacks a generally accepted definition in the field of strategic and security studies. Agreeing with this statement are a number of scholars such as Haftendorn (1991: 15) who claims "that the field of security studies suffers from the absence of a common understanding of what security is, how it can be conceptualized, and what its most relevant research questions are". For Wolfers (1952: 483) the "term security is ambiguous in content as well as in format and it refers to different sets of issues and values". McSweeney (1999:1) describes security as "an elusive term which resists definition, as it is employed in a wide range of contexts and to multiple purposes by individuals, corporations, governments and academics". Also recognizing the difficulties of defining security, Schultze pointed out that "the concept of national security does not lend itself to neat and precise formulation. It deals with a wide variety of risks about whose probabilities we have little knowledge and of contingencies whose nature we can only dimly perceive" (Schultze 1973: 529-530).

In light of this, the term 'security' has come to mean different things at different times, and many scholars have attempted to define the concept of security. Bourne (2014: 1) states that in common usage security relates to survival, the protection from threats to existence, and being relatively free from harm inflicted by others. In its academic usage, the term generally relates to the protection of something that is valued such as: physical life, the organisation of political life (nation-state), democracy, identity, language, property, territory, and so on (Bourne 2014: 1). For Arnold Wolfers (1952: 484), security means “some degree of protection of values previously acquired”. He further describes security both in objective and subjective terms. In an objective sense, security measures the absence of threats to acquired values and in a subjective sense; security is the absence of fear that such values will be attacked (Wolfers 1952: 485).

Drawing upon Wolfers’ characterisation of security, David Baldwin (1997: 13) describes security as “a low probability of damage to acquired values. This description of security concentrates on the preservation of acquired values and not on the absence of threats. For Baldwin, security in its most basic sense can be defined in terms of two conditions: “security for whom, and security for which values” (Baldwin 1997: 14).

Bourne (2014: 2) contends that most understandings of state security do not question security but seek to explore how a state provides protection to its citizens and itself, particularly in relation to other states. So security is often considered in terms of ‘national security’. From the definitions, it is evident that national security remains a contested and ambiguous concept. Based on the above-mentioned conceptions, a working definition of national security would therefore include: the protection of a sovereign nation-state, its national interests and its entire people from any form of security threat and attack detrimental to the running and survival of the state.

2.2.1. Traditional conceptions of national security and national interest

The concept of national security has developed significantly over the years but it remains a contested concept. Since the Second World War, the scope and distinctiveness of the field of security studies has evolved and has been closely linked to the changing global landscape of security threats (Bourne 2014: 10). Traditionally, security was defined mainly at the nation-state level and almost entirely defined in military terms. According to this conventional concept, the state is both the object of security and the primary provider of security (Burgess 2008: 60). Baylis and Smith (2001: 255) claim that the main area of interest for both academics and statesmen tended to be on the military capabilities that their own states should develop to deal with the threats they faced.

This emphasis on external military threats to national security was predominant during the Cold War. During this era security was overwhelmingly a matter of the state's sovereignty, its territorial integrity and its political autonomy (Saleh 2010: 229). Furthermore, the notion of security during the Cold War was closely linked to the realist theory, which associated security with military issues and the state-centred use of force. Thus, when dealing with national security it is important to consider national interest and the role it plays in determining how states view national security threats.

Similar to national security, the concept of national interest has been considered to be an ambiguous field of study in strategic studies. However, Nuechterlein (1976: 247) gives us a stronger definition by describing national interest as the perceived needs and desires of one sovereign state in relation to other sovereign states comprising the external environment. In this regard it is the interests of the nation-state in its entirety, not of private groups, bureaucracies or political organisations. According to Wolfers (1952: 481), national interest indicates a policy designed to promote the demands ascribed to a nation rather than to individuals, sub-national groups or mankind as a whole. Furthermore, the national interest of a country can further be divided into four basic needs that underpin its foreign policies. These include: defence, economic, world-order and ideological interests. Through this categorisation, it becomes easier to map out the decision making process by assessing why leaders make the decisions they do (Nuechterlein 1976: 248).

It is important to note that the concepts of national interest and national security are closely related and have sometimes been used synonymously since the Cold War era. According to Wolfers (1952: 482), the impact of the Cold War as well as threats of aggression rather than depression and social reforms resulted in a synonymous approach to the formula and practice of national interest and national security. In this new environment national security and national interests have become complicated, often ambiguous and even inconsistent because of the unpredictable, uncertain and confusing characteristics of the international arena.

Thus determining the relationship between the two concepts is not easy as it involves a variety of linkages between national and domestic policies. In this regard, the domestic economic impact of certain national security policies can link domestic interests and policies to the international security arena. Take for example, economic sanctions and trade embargoes on one nation-state having serious implications for global and local markets.

Furthermore, besides the relationship and link between foreign and national security policies, domestic interests are important in establishing national security priorities and interests.

Having examined the traditional conceptions of national security and national interest, the following section will trace the post-Cold War developments that led to an evolution in strategic thinking and attempt to identify the main characteristics of the post-Cold War evolution in strategic thinking and how it has greatly transformed the traditional war fighting paradigm of nation-states.

2.2.2. The Post-Cold War Evolution in Strategic Thinking

The post-Cold War era brought about significant changes to strategic thinking in military affairs which was characterised by a changing global environment. This environment introduced a new range of non-state actors as well as new advances in technological innovation, which consequently led to both a transformation of and revolution in military strategic affairs. Furthermore, the major Western states restructured their armed forces to take account of the sudden disappearance of the old threat (nuclear warfare) and to meet the popular demand for a substantial ‘peace dividend’ (Freedman 1998: 5). The restructuring of the armed forces was necessary in order to appropriately deal with emerging threats that required a different modern approach. Freedman (1998: 5) asserts that the restructuring process was combined with a number of military operations. These military operations were widely spread around the world, including the Persian Gulf, the Balkans and Sub-Saharan Africa. They ranged from peace support operations to conventional warfare.

In order to remain relevant and effective, all military forces have to undergo a periodic change: both in terms of its hardware capabilities as well as in terms of its doctrines and strategies (Weng Loo 2005: 29). In this regard, the post-Cold War era brought about new technological innovation and greatly transformed military affairs. It can be argued that the Gulf War of 1991 could serve as a point of origin in how technological innovation greatly influenced strategic thinking and was considered to be a revolution in military affairs (RMA). According to Neuneck and Alwardt (2008: 5), the starting point for public perceptions of RMA weaponry was ‘Operation Desert Storm’, the US-led war against Saddam Hussein’s Iraq in 1991. The use of global positioning systems (GPS) or laser-guided weapons delivered by stealth fighters dominated TV coverage and created the perception that the operation was a ‘surgical and clean war’.

Furthermore, Rezk adds that “as a range of new and fantastic allied weapons systems descended upon Iraq’s desert terrain in 1991 with unprecedented precision, speed and technological prowess, militarists all over the Western world hailed the advent of a ‘revolution in military affairs’ (RMA). The combination of technology and information dominance would ensure that modern war would be quick and easy, with minimal casualties on both sides” (Rezk 2010). Reliance on precision weapons also has the potential to reduce casualties, both friendly and hostile, and to limit collateral damage among civilians. Improvements of this sort are by no means insignificant in an era when military budgets and force levels are declining in most advanced nations, and when aversion to casualties and humanitarian considerations can strongly affect domestic support for overseas operations (Guilmartin 2013).

The revolution in military affairs thus represents the post-Cold War evolution in strategic thinking. However, this new era also brought about new security challenges and threats which traditional military approaches to national security could not deal with effectively. This required a broadening and deepening of the security agenda in order to take account of the nature of security in the modern age.

2.2.3. The Nature of Security in the Modern Age

It can be argued that there have been two major events fairly recently that have transformed and broadened the conceptualisation of national security. These are the end of the Cold War and the terrorist attacks on US soil on September 11th 2001. According to Burgess (2008: 60), these events forced a major rethinking about the basic assumptions underlying security studies bringing about a general consensus among both scholars and practitioners that a wide range of security threats, both new and traditional, now confront states, individuals and societies. What this implies is that the state can no longer be the only referent object in security and the military can no longer be the sole actor responsible for maintaining that security.

Since the end of the Cold War, the agenda of security studies has been ‘broadened’ and ‘deepened’ to include new dimensions and referent objects (Abrahamsen 2005: 57). In this regard economic, societal, political and environmental risks have been added to military threats as the necessary security dimensions to be secured. Furthermore, individuals, groups, communities and even ecological systems have been conceptualised as referent objects alongside the state (Abrahamsen 2005: 57). Non-military threats to security and non-state actors now play a larger role within security studies. Burgess (2008: 60) gives us a few examples that include: new forms of nationalism, ethnic conflict and civil war, information communication technology (ICT) and cyber insecurity, biological and chemical warfare, resources conflicts, pandemics, mass migrations, transnational terrorism and environmental dangers.

Therefore, the changes in the conceptualisation of national security can be attributed to a number of factors, but the main underlying notion is that the twenty first century has brought with it new challenges and threats which traditional theories do not adequately cater for and explain. As Zelikow (2003: 28) suggests, there is need for a new understanding about the real problems through a flexible pragmatic approach towards building a common freedom project.

2.3. The Broadening and Deepening of National Security

Within security studies, the dimensions of national security can be described through the ‘broadening’ and ‘deepening’ of security debate. The ‘broadening’ aspect is concerned with extending the concept of security to include other issues or sectors besides the military, while the ‘deepening’ aspect asks the question whether non-state actors are capable of claiming security threats down to the individual level.

After the collapse of the Soviet Union and the end of the Cold War, International Relations scholars including Barry Buzan and Ole Waever gradually began to emphasise the need for a broadened understanding of security. They claimed that it was deceptive to limit “security analysis to traditional military threats to the territorial integrity of states, and criticised the intense narrowing of the field of security studies imposed by the role of the military as well as the Cold War nuclear obsessions” (Garnett, 1996: 14). They argued that there were more persistent non-military sources of threats to national security. Thus, the broadening of the national security debate provided a basis for the theory of securitisation to be conceived. The following section will focus on the conceptualisation and dynamics of securitisation theory.

2.3.1. Securitisation Theory

Securitisation theory is a school of thought that has originated from the broadening of the security debate. The theory of securitisation is primarily associated with scholars from the Copenhagen School who include Barry Buzan and Ole Waever. According to these scholars, the core idea behind security is survival. "It is when an issue is represented as posing an existential threat to the survival of a referent object" (Peoples & Vaughan-Williams 2010: 76). In this regard, a referent object refers to an entity (such as the state) perceived to be under threat and in need of protection, while an existential threat to a referent object basically represents a security issue. Peoples & Vaughan-Williams (2010: 77) carry on saying that when an issue comes to be treated as a security issue, "it is justifiable to use exceptional political measures to deal with it." In other words, it is securitised. However, before an issue becomes securitised, it begins as a non-politicised issue then proceeds to become politicised and if the threat escalates, the issue becomes securitised. Therefore, securitisation begins with security which means that it has to be initiated through a speech act from certain political actors with legitimate authority.

An important concept with regard to securitisation and the Copenhagen School is the Speech Act theory. Abrahamsen (2005: 57-58) argues that the social construction of security issues is analysed by examining the "securitising speech acts" through which threats become represented and recognised. In the words of Ole Waever quoted in Peoples & Vaughan-Williams (2010: 77), "by uttering 'security,' a state-representative moves a particular development into a specific area, and thereby claims a special right to use whatever means necessary to block it." What this means is that with the sufficient level of authority, by saying certain words or phrases, one can perform a particular function. "Certain speech acts are known as performatives whereby saying the word or phrase effectively serves to accomplish a social act" (Peoples & Vaughan-Williams 2010: 77). For this type of performative speech act to work, certain conditions have to be met. The words have to be said by someone in authority, in the right context and according to certain pre-established rituals or conventions. These conditions are what Peoples & Vaughan-Williams call felicity conditions in speech act theory (the conditions required for the successful accomplishment of a speech act). Thus, securitisation follows a general pattern of operation which requires a degree of acceptance between the agent (state representatives) of the securitising speech act and the relevant audience (citizens of the state) it is applied to.

Threats and vulnerabilities according to Buzan as quoted in Peoples & Vaughan-Williams (2010: 78) "have to be staged as existential threats to a referent object by a securitising actor who thereby generates endorsement of emerging measures beyond rules that would otherwise bind." Thus, securitisation according to Abrahamsen (2005: 60) is a political choice, a decision to conceptualise an issue in a particular way. In this regard, "invoking the concept of national security has an enormous power as an instrument of social and political mobilisation" (Abrahamsen 2005: 60). However, in order for securitisation to work, an audience (citizens of the state) has to accept a threat as being credible.

There are three conditions required for the successful accomplishment of a speech act and these conditions increase the likelihood of successful securitisation. The first condition follows the conventional argument of securitisation which claims that an existential threat is presented as legitimating the use of extraordinary measures to combat that threat. The second condition looks at whether the securitising actor is in a position of authority, and has enough social and political capital to convince the audience of the existential threat. The third condition concerns objects associated with the issue that carry historical connotations of threat, danger, and harm or where a history of hostile sentiments exist, such as competing rival states (Peoples & Vaughan-Williams 2010: 79). In short what Peoples & Vaughan-Williams argue is that none of these conditions on its own is sufficient enough to achieve successful securitisation.

2.3.2. The Dynamics of Securitisation

By understanding securitisation as a mode of thinking, a security analyst is able to investigate how the same logic might apply to non-military issues. One of the most noticeable efforts to broaden the security agenda is given by Barry Buzan. He stresses "that the security of human beings is affected by factors in five major sectors: military, political, economic, societal and environmental" (Buzan: 1991). Through dividing and categorising security into different sectors we are able to distinguish distinct patterns or dynamics of security found in each as well as identifying the likely securitising actors and prospects for securitisation. Each of these sectors shall be individually looked at below, paying attention to the referent objects in each dimension as well as the relevant actors responsible for maintaining security for each of them.

i. *Military sector*

The military sector concerns the two-level relationship of the armed offensive and defensive abilities of states, as well as states' perceptions of each other's intentions. According to

Buzan (1991: 116), military threats have traditionally been given the highest priority in national security issues, as military action has the capability of destroying the work of centuries in other sectors. Furthermore, military threats occupy a special category precisely because they involve the use of force breaching normal peaceful relations as well as disrupting diplomatic recognition. Therefore, a state's security agenda is always focused towards the goal of national security. Two important assumptions are made: firstly, military security is not the only sector worthy of consideration in security studies, and secondly, non-military threats do not necessarily have to be as dangerous as war, but they have to follow logic and have effects which parallel the traditional military political understanding of security.

ii. Political sector

This sector concerns the organisational stability of states, systems of government and the ideologies that make nation-states legitimate. Buzan (1991: 119) informs us that political threats are aimed at the organisational stability of the state thus the idea of the state, particularly its national identity and organising ideology, and the institutions which express it, are the normal target of political threats. The referent object, according to Peoples & Vaughan-Williams (2010: 81), is usually the 'constitutive principle', namely sovereignty. Anything that threatens the existence of this principle can be presented as a security issue.

Furthermore, "political threats also stem from a great diversity of organising ideologies and traditions found in the international system" (Buzan 1991: 119). Therefore, the competition among ideologies makes it difficult to define what should be considered a political threat and if it is serious enough to be considered a national security issue.

iii. Economic sector

The economic sector is concerned with accessing the necessary resources, finance and markets required to sustain adequate levels of prosperity and state power. Economic threats could be an issue when national or global markets become susceptible to financial collapse on a large scale with direct consequences on communities and individuals. In extreme cases, a financial crisis could compromise or deprive access to basic necessities. For example, security spill-overs from the economic sector can pose a potential threat to the funding of a national defence budget. The referent objects in this sector can be categorised into three distinct groups, that is: the individual, business organisations and the state. For the individual, Buzan (1991: 237) notes that a basic definition of economic security can be in terms of ready access to the means necessary to meet basic human needs. However, the idea of economic security becomes entangled with a range of highly politicised debates about employment, income distribution and welfare.

Business organisations are the most purely economic actors and therefore the least able to escape the fundamental inconsistencies of economic security (Buzan 1991: 238). With this in mind, organisations can seek security by staying on top of the market through greater adaptation and innovation, or by establishing either a monopoly or a politically protected market share. However, pursuing security by monopoly allows a high probability of contradictions between organisations security interests and the welfare interests of consumers (Buzan 1991: 239).

In view of the state as a referent object, Buzan (1991: 241) asserts that it is extremely difficult to determine when economic threats legitimately become national security issues because demanding for national security too frequently would simply mean increasing government intervention in the economy to a point where the market can no longer function independently.

iv. *Societal sector*

Societal security is concerned with the sustainability, within acceptable conditions for the evolution of traditional patterns of language, culture, religion, national identity and customs (Buzan 1991: 19). For Burgess (2008: 65), when speaking of societal dimensions of security, we are commonly referring to the threats to the identity of a group. This involves relationships of collective identity. Therefore, societal identities have the degree and consistency to function as a referent object. Within a civil society, there exists certain identities characterised by different traits and some groups might be more powerful than others. Securitisation occurs when issues are accepted as threatening the existence of a group’s identity. This could include migrants who enter a country and may hold contradicting ideologies and values. For Buzan (1998: 121), threats to societal security can be understood to fall along two axes: horizontal and vertical. The former refers to identities that compete with one another while the latter take the form of integrating practices from above.

v. *Environmental sector*

Environmental security is concerned with the maintenance of the local and the planetary biosphere as the essential support system on which all other human enterprises depend (Buzan 1998: 20). It is becoming more evident however that the increase in human activity is beginning to visibly affect the conditions for life on the planet. Environmental issues such as climate change, global warming, pollution, depleting of natural resources, etc. may be interpreted by securitising actors as threatening the very existence of animal species or even human life itself (Peoples & Vaughan-Williams 2010: 81). Furthermore, environmental issues can have a knock-on effect in other sectors of the state. For example, refugees escaping floods to neighbouring countries may threaten the societal economic and political integrity of neighbouring countries.

Buzan (1991: 19-20) stresses that the above mentioned five sectors do not "operate in isolation from one another, and each one defines a focal point within the security problem, but all are woven together in a web of linkages. Their common denominator is the threats to and defence by the state" (Buzan 1991: 19-20). In other words, "Buzan's concept of security, even constructed in terms of five sectors, has the nation state and state sovereignty as the core referent object of security to some extent" (Waever 1993: 24).

In recent years however, scholars have advocated for a broadening "of the security agenda to cover a variety of economic, social, ecological and demographic issues" (Gardner 2005). Some of the most debated non-traditional security issues include: transnational terrorism, organized crime, international migration, asylum seekers, arms proliferation, ethnic and religious warfare, environmental degradation and cyber insecurity. According to Klare and Chandrani (1998), "it is likely that the future security environment will be characterised by the presence of many threats, each demanding the attention of international policymakers, and all are likely to figure prominently in the global discourse on international peace and security" (Klare and Chandrani 1998: vii-viii).

The increasing influence of scholars looking to broaden the security agenda has significant repercussions for both policy and academic debates. There has been a growing tendency to develop a security concept that is capable of linking together a diverse range of issues. Moreover, the difference between internal security and external security has been blurred as the threat of conventional military attacks on nation-states has deteriorated, while the threat of asymmetric attacks by non-state actors has rapidly increased. Cyber security for example, presents a blurring of internal and external security based on the fact that the character of cyber-attacks is transnational in nature and does not recognise state sovereignty. The following section will focus on the deepening of the national security debate.

2.3.3. The Deepening of National Security

Besides the debate on broadening the focus of security studies to incorporate non-military issues, traditional conceptions of security were also challenged by scholars who criticized the state-driven methodology of realists. From a realist point of view, states are assumed to act in certain and similar ways no matter what the domestic political system is due to the constraining effect of international anarchy.

A number of scholars of security studies have criticised the state-driven understanding of security, and claim "that any attempt to rethink security in the post-Cold War era must move beyond the traditional focus on the state as the referent object for security discourse" (Wyn Jones, 1996: 197-8). Munster (2005: 2) points out that the "privilege given to the state is inadequate to address the problems of 'common' or 'human' security, which would need consideration on the level of the individual, sub-state groups or on the level of humanity as a whole". Adding to this, Wyn Jones (1996: 209) asserts that if the focus is "on security referents other than the state, it becomes apparent that 'existential' threats to those referents - be they individuals, nations and so on - are far wider than those posed by military force". Thus, these scholars have looked to deepen the security studies debate by moving the focus away from states to different levels of analysis including individual and human security. The concept of human security will be discussed in the following section.

2.3.4. Human Security

Several scholars and policy makers have broadened and deepened the concept of security significantly through the advancement of the notion of 'human security', which focuses on individual security and sustainable human development instead of state security and military force. The most revered conception of human security is derived from the United Nations Development Program (UNDP) which defines it as: "First, safety from such chronic threats as hunger, disease and repression. And second, it means protection from sudden and hurtful disruptions in the patterns of daily life -whether in homes, in jobs or in communities. Such threats can exist at all levels of national income and development" (United Nations Development Program 1994: 23).

In broad terms human security is defined as freedom from want (positive freedom) and freedom from fear (negative freedom) in relation to fundamental individual needs. Human security is therefore normative in nature as it argues that there is an ethical responsibility to re-orient security around the individual in line with internationally recognised standards of human rights and governance (Newman 2010: 78). It is important to note that all approaches to human security agree that the referent of security policy and analysis should be the individual, but they disagree about which threats the individual should be protected from and what means should be employed to achieve this protection (Newman 2010: 79).

In the twenty-first century however, global threats to human security are said to include at least six categories: inequalities in economic opportunities: environmental degradation, drug production and trafficking, unchecked population growth, international migration, and international terrorism (Dalby 2000: 5). Although not mentioned, cyber security is a new emerging global threat which continues to rapidly evolve in terms of the reach and damage it can cause to both individuals and nation-states. However, the interesting fact about these threats to human security is that many are caused more by the independent actions of millions of individuals rather than the deliberate aggression by specific states. Thus, under the traditional narrow formulation of the concept of security, the above mentioned would not be considered security threats (Dalby 2000: 5).

Having explored the traditional and modern conceptions of national security, it is necessary to briefly explain Kenya's external and internal national security environment in order to identify what issue is perceived to be the biggest physical threat currently affecting Kenya's national security.

2.4. Overview of Kenya's National Security

Kenya is surrounded by five neighbours including: Tanzania, Uganda, Ethiopia, South Sudan and Somalia. Kenya plays an important role as it is considered the region's biggest economy and an advocate for strong multilateral relations. Traditionally, Kenya has promoted itself as a modest, peace-loving nation with a firm respect for the norms of respecting the sovereignty of neighbouring states, good neighbourliness, the peaceful settlements of disputes and non-interference in the internal affairs of other states (McEvoy 2013: 1).

When Kenya gained independence in 1963, the Cold War was gaining momentum and Africa was gaining strategic importance with the Western powers. During the Cold War, Kenya's security interests were closely tied to Western external security interests and geopolitical considerations. However, instead of portraying a relationship of pure dependence which characterised most African relations at the time, Bachmann (2012: 130) notes that the Kenyan government mobilised Cold War tensions and managed to establish a system of 'balanced benefaction' in which Kenya gained assistance from a diversity of donors without becoming too reliant on a single one(Bachmann 2012: 130).

Despite the fact that the Cold War had devastating effects on the African continent, President Jomo Kenyatta's government promoted a foreign policy based on the principles of 'positive non-alignment', African unity, anti-colonialism, and UN multilateralism (Bachmann, 2012: 131). The country positioned itself as an independent and strong voice for 'what is right and just in international affairs'. Due to the country's strong commitment to African nationalism, Kenya was regarded as a neutral yet prestigious force on the continent throughout the 1960 and early 1970s (Bachmann 2012: 131).

Since then, Kenya has been involved in international cooperation with other countries through several regional initiatives including: the East African Community (EAC), Common Market for Eastern and Southern Africa (COMESA), Intergovernmental Authority on Development (IGAD), New Partnership for Africa`s Development (NEPAD), and the International Criminal Court (ICC) among others (ISS 2012).

From the mid-1990s however, Kenya under President Daniel Moi attained an important regional role in mediating the regional conflicts in Sudan and Somalia under the support of the Intergovernmental Authority for Development (IGAD). Kenya hosted negotiations between the Sudanese government and the Sudanese People's Liberation Movement (SPLM) of the South, which in the end led to the Comprehensive Peace Agreement, signed in 2005 in Naivasha, Kenya (Murithi, 2009). With regard to the conflict in Somalia, Kenya hosted a two-year reconciliation conference that resulted in the formation of the Somali Transitional Federal Government in 2004 (Bachmann 2012: 132).

Kenya's current President Uhuru Kenyatta has emphasised a more regional and Afro-centric approach in Kenya's foreign policy (Kisiangani 2014: 3). This is evident in a speech the president gave at Kenya's 'Jamhuri Day' celebrations on December 12 2014, stating:

> *From the struggle against colonialism to our current challenges, Africa has been true to us. We will keep this faith Africa. Let us celebrate African brotherhood and solidarity by embracing a strong Pan-African spirit aimed at ultimately consolidating African integration into a multinational federation in our time. Every African is our brother and sister, and we must treat them as such* (Kenyatta 2014a).

Kenya is understood to share humanitarian and security concerns similar to Western nations, as it has for a long time spearheaded a multilateral approach towards the mediation and resolution of the continent's conflicts. According to Bachmann (2012: 126), the country has accentuated its responsiveness to human security, which centres on the protection of the individual rather than the state, by contributing to UN missions, and a driving force in the implementation of the African Union's architecture on peace and security. The above-mentioned factors have enabled Kenya to play a significant role in the East African region and the continent. Consequently, Kenya's national security has an impact on the security of the East African region.

Kenya is considered to be the regional hub for trade and finance in East Africa due to its sound economic policies and a record of pragmatism in foreign policy and regional affairs, bringing the country to a position of relative leadership thus making it highly adaptable to global changes (Wanyama 2013: 5). In addition, Kenya's port of Mombasa is home to the largest seaport in East Africa, which controls access to the landlocked neighbouring countries of Uganda, Rwanda, Burundi, eastern DRC and South Sudan through its Northern Corridor (McEvoy 2013: 3). Moreover, with the East and Horn of Africa region developing into a 'prospective hydrocarbon province', Kenya aspires to be the hub for international investments in natural gas and petroleum resources (ISS 2012) after the discovery of oil and gas in the north eastern region of Turkana County and the Lamu Basin at the northern coast of Kenya.

In light of this, promoting regional security and stability in the East African region is in Kenya's best national interest, as regional instability can affect the country's gains in economic growth and development. Kenya has sought to advance its interests not by defining the regional political agenda, but by taking the regional environment as a given and then making pragmatic but cautious efforts to ensure the safeguarding of its economic and security interests (Kisiangani 2014: 1).

2.4.1. Perceived Threats to Kenya's National Security

National security threats that Kenya faces have a significant impact on the East African region. Unlike its other neighbours in the region, Kenya had not faced any external threats from aggressive state actors that required the use of military force up to now. With regard to external physical threats to Kenya's national security, transnational terrorist attacks by non-state actors have resulted in the biggest number of deaths and casualties.

Terrorism in Kenya

Terrorism poses an existential threat to Kenya's national security for several years. However, the target of major terrorist attacks in Kenya was initially linked to foreign nationals and carried out by transnational terrorist organisations. The most lethal terrorist attack in Kenya occurred on 7 August 1998, when Osama bin Laden's Al Qaeda organisation targeted the US Embassy in Nairobi, Kenya. A suicide truck bomb exploded killing 224 Kenyans and 12 Americans, and injured more than 5000 people in the surrounding area (Adan 2005: 32). Moreover, in Dar es Salaam Tanzania, a similar device simultaneously exploded at the US Embassy Killing 11 people and injured 85 people (START 2013: 2).

Four years later, another major terrorist attack occurred on 28 November 2002, targeting Israeli nationals at the coastal city of Mombasa. Suspected Al Qaeda operatives were believed to have carried out two terrorist attacks on the same day. The first attack was a car suicide bombing that targeted an Israeli-owned hotel known as 'Paradise Hotel'. During this attack, three suicide bombers killed 10 Kenyans and 3 Israeli's, and wounded 80 people (START 2013: 3).

After the Paradise Hotel bombing, terrorist attacks in Kenya declined and became less frequent. In 2008 however, a new regional terrorist organisation from Somalia known as 'Al Shabaab' began making inroads into Kenya. Al Shabaab began carrying out a string of small scale attacks in North-Eastern Kenya, targeting towns close to the Kenya-Somali border. In May 2008, for example, Al Shabaab targeted a police station in the North-Eastern Kenyan town of Wajir, freeing detainees who were suspected of being linked to Al Qaeda (START 2013: 3). However, Al Shabaab became an existential threat to Kenya's national security when the group took responsibility for carrying out various grenade attacks in public places such as bars, churches and bus terminals. To add insult to injury, Al Shabaab was accused of killing a British national and kidnapping a French woman in 2011. The Kenyan government regarded the kidnapping incident by Al Shabaab as a serious violation of Kenya's territorial integrity and threatened the country's multi-million dollar tourism industry (Malalo 2011).

Kenya retaliated by launching a military offensive 'Operation Linda Nchi' (Swahili for 'Protect the Nation') into southern Somalia in October 2011, with the intention of defending Kenya against terrorist threats and incursions by extreme Islamist group Al Shabaab (McEvoy 2013: 10). In February 2012, the United Nations Security Council (UNSC) added its support, authorising Kenya's inclusion into the African Union (AU) Mission in Somalia (AMISOM), which raised the troop numbers from 12,000 to 17,731 which allowed it to expand its mandate beyond Mogadishu(Blanchard 2013: 4). Kenya's intervention in Somalia marked a fundamental change from its traditional low-risk regional engagement policy. Despite being praised by Kenyans at the time as a demonstration of the use of the country's military power to protect its strategic interests, the incursion ran counter to the country's traditional core principles and overturned the country's policy of non-interference (Kisiangani 2014).

After Kenya launched its military offensive into Somalia, terrorist attacks by Al Shabaab escalated in Kenya. Since October 2011, Al Shabaab and its affiliates have conducted more than 50 separate grenade attacks in Kenya with the aim of causing deaths and large-scale panic in the country (Aronson 2013: 29). In November 2012, a bus exploded in the Nairobi Eastleigh Estate killing seven people and leaving dozens wounded. Other smaller grenade attacks have been conducted in other parts of the North Eastern and coastal regions of Kenya, targeting non-Somalis in public places such as restaurants, churches and nightclubs (ICG 2014: 4).

However, Kenya suffered one of its most devastating terror attacks by Al Shabaab on September 21 2013. Four masked gunmen allegedly attacked the 'Westgate Mall', an Israeli owned upscale popular shopping mall in Nairobi frequented by many foreign nationals and middle-class Kenyans. The attack resulted in hundreds of casualties including more than 60 deaths (START 2013: 1). According to an Al-Shabaab spokesman, Sheikh Abulaziz Abu Muscab, the reason for the attack on Westgate Mall was because it was a place where tourists, diplomats, and Kenya's decision-makers came to relax and enjoy themselves (Mohamed 2013).

More recently, on 23 November 2014, Al Shabaab gunmen hijacked a bus in the Northern Eastern town of Mandera travelling to Nairobi and killed 28 people. The gunmen separated the non-Muslim passengers by asking them to read from the Koran, and those who failed were shot in the head at point-blank range (BBC 2014). Al Shabaab claimed responsibility for the attack, saying it was a revenge for recent raids carried out by Kenyan security forces on mosques in the coastal city of Mombasa in which Kenyan police claimed to have found explosives and arrested 150 people during the mosque raids (Al Jazeera 2014).

The above-mentioned terror attacks have had a significant effect on Kenya's economy and have greatly affected its tourism sector and economy. Travel advisories have been issued by the US, British, French, and Australian governments to its citizens on travelling to Kenya. This has resulted in the loss of revenue and jobs in the tourism sector. In a recent CNN interview, President Uhuru Kenyatta strongly opposed the travelling warnings by Western nations and called them counter-productive in the fight against terrorism. He said:

> *The world needs to recognise the fact that this is a global threat which requires to be countered by a global partnership in order to defeat and secure not just Kenya, but the world* (CNN 2014).

Al Shabaab remains an existential threat to Kenya's national security and is responsible for the recent substantial increase in terrorism in Kenya. According to the International Crisis Group, Al Shabaab's terror attacks in Kenya are driven by the intent to "put pressure on the government's continued deployment with AMISOM in southern Somalia by hitting targets that directly affect the financial interests of the middle (political) class and divide them, and to insert cells and trained fighters into locations with pre-existing grievances and patterns of violence that the authorities have historically struggled to address and contain"(ICG 2014: 16).

2.5. Conclusion

The understanding of security in the modern age has been greatly influenced by the post-Cold War evolution in strategic thinking and the broadening and deepening debates outlined in this chapter have helped shape the traditional conception of security into a broader and more diffuse understanding of security. However, due to the rapid increase in globalisation and technological innovation, a new important form of threat is emerging in the cyberspace domain.

Cyberspace has greatly influenced the character of human activity and has had a significant impact on national security as it presents a new form of threat. According to Sheldon (2013: 315), the universality and omnipresent nature of cyberspace has had an impact on international relations and the privileged role of the state in international politics. This has resulted in the empowering of individuals and groups through the redistribution of power in cyberspace, and has undermined the monopoly of power traditionally enjoyed by states.

In this regard, the discourse on cyber security is gaining momentum in the field of security studies as the threats in cyberspace have become transnational and highly sophisticated with possible deadly effects. Furthermore, cyber threats and attacks affect both the individual and nation-states. In the next chapter the evolution of cyber security and its relation to the modern conceptions of national security will be examined.

CHAPTER 3: THE EVOLUTION OF CYBER SECURITY

3.1. Introduction

Having looked at the traditional and modern conceptions of national security in the previous chapter, the main focus of this chapter is to analyse the evolution of cyber security and how it relates to national security. In order to achieve this, a conceptual overview of cyber security is provided, followed by a brief historical overview of the development of cyberspace. The manifestation of cyber insecurity will then be explained in order to distinguish between the various forms of cyber insecurity, as well as its nature and development over time. In addition, the sources and motivations behind cyber-attacks will be explored in order to understand the emerging trends in cyber security.

3.2. A Conceptual Overview of Cyber Security

Cyber security is an ambiguous concept as there is no agreed definition. The concept and its usage has generated different conceptions for people in the political, military, industrial and academic spheres. In most literature however, cyber security is used as an all-inclusive term. There are certain terms and definitions that are essential for understanding the relationship between cyber security and other security domains.

Von Solms and van Niekerk (2013: 5) define cyber security as the protection of cyberspace itself, the electronic information, the information communication technologies (ICTs) that support cyberspace, as well as the users of cyberspace in their personal, societal and national capacity, including any of their interests (either tangible or intangible), that are vulnerable to attacks originating in cyberspace.

The International Telecommunications Union (ITU 2008) on the other hand conceptualises cyber security as the collection of tools, policies, security concepts, security safeguards, guidelines, risk-management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organisation and users' assets. Organisation and user assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cyber security therefore strives to ensure the attainment and maintenance of the security properties of the organisation and users' assets, and against real security risks in the cyber environment. Therefore, the general security objectives are comprised of the availability, integrity and confidentiality of information across cyberspace (ITU 2008).

Brechbhl et al. (2010: 85) believe that "cyber-security is essentially about managing future risk and responding to current and past incidents and attacks." In this regard, "managing future risk requires insight into current and future vulnerabilities and how to prevent or reduce these, the probabilities of a threat and the costs associated with the potential outcomes and how to mitigate these" (Brechbhl et al. 2010: 85). Furthermore, "responding to current and past incidents and attacks requires knowledge of what has happened, methods of preventing similar incidents from being successful in the future, and possible legal or other remedial actions against the perpetrators" (Brechbhl et al. 2010: 85). The full spectrum of cyber incidents will require the sharing of information among private firms, suppliers of products and services, as well as public agencies including intelligence and security agencies (Brechbhl et al. 2010: 85).

Nevertheless, Choo (2011: 728) argues that "cyber-security research is of a cross-disciplinary nature, and will potentially involve researchers from non-technical domains such as criminology, law, engineering and psychology". Because of this, more cyber security research is needed to provide policy and practice with relevant evidence that will enable policy makers and practitioners to formulate national regulatory frameworks and suitable policy responses to address the emerging cyber security environment (Choo 2011: 728). The following section will seek to analyse the history and development of the cyberspace environment.

3.3. The Development of Cyberspace

As a point of departure, the dictionary defines the term 'cyber' as relating to, or involving computers or computer networks including the internet (Merriam-Webster Dictionary 2012). In addition, Klimburg (2012: 8) posits that the cyberspace environment consists of: the internet, information communication technologies (ICT's) and the networks that it connects. Cyberspace also includes the hardware, software and information systems as well as the individual who interacts socially within these networks (Klimburg 2012: 8).

Cyberspace consists of all of the global computer networks and everything connected and controlled through cables, fibre-optics or wireless technology (Schreier et al. 2011: 9). Today, many citizens, communities, industry, academia, and governments worldwide rely on cyberspace. Furthermore, “the global expansion of digital media, networks, and information and communications technologies (ICTs) is quickly becoming the most powerful technological revolution in the history of humankind” (UNIDR 2013: x).

According to the United Nations Institute for Disarmament Research, the so-called ‘Information Revolution’ has given the global community the capability to rapidly and easily connect individuals, companies, governments, international institutions, and other entities (UNIDR 2013: x). Interconnectivity through digital networks is now considered the key characteristic of today’s global economy, and is increasingly required for global economic stability and development (UNIDR 2013: x). However, due to the fast pace of technological development, the increase in ICT usage, and the rapid growth of internet access, many political, legal, and societal aspects of the cyber environment are yet to be fully understood (UNIDR 2013: x).

Cyberspace resources can be characterised by six distinct components that represent the major divisions within cyberspace. Together these form the cyberspace infrastructure and environment. These are: hardware (comprising computers, printers, scanners, servers and communication media), software (which includes applications and special programs, system backups and diagnostic programs, and system programs like operating systems and protocols), data in storage (in transition or undergoing modification), people (including users, system administrators, and hardware and software manufacturers), documentation (including user information for hardware and software, administrative procedures, and policy documents), and supplies (including paper and printer cartridges) (Kizza 2014: 83).

Another important element to consider is the cyberspace infrastructure, which consists of: hardware nodes (as sourcing, transmitting, and receiving elements), software (as protocols), human-ware (as users of information), and finally pure information (that is either in a state of rest at a node or a state of motion in the linking media) (Kizza 2014: 32).

Cyberspace has consequently brought about an increasing reliance on these resources through computers running critical national infrastructures like telecommunications, banking and finance, transportation, electrical power systems, gas and oil storage, water supply systems, emergency services that include medical, police, fire, and rescue, and, of course, government services (Kizza 2014: 83). In order to further understand the cyberspace environment and its significance, the next section will explore the history and development of the personal computer as well as the internet.

3.3.1. The History and Development of the Personal Computer (PC)

A personal computer (PC) is defined as a small general-purpose computer equipped with a microprocessor and is designed for use by one person at home or in an office (Merriam-Webster Dictionary 2014a). In addition, a PC has many features that help us with simple to complicated tasks including writing up assignments on a word processor, storing information in files, research on a particular subject and so on. Personal computers can also be used for educational purposes, gaming and leisure, listening to music, watching movies, use of the internet and a lot more. Portable types of personal computers have been made such as the laptop, notebook computers and tablets (History Learning Site 2006).

PCs have become common items in many businesses and households' today but in 1955, 'there were only 250 computers in use throughout the world' (History Learning Site 2006). This is because a computer during that time was very large and could not have fitted into a normal room in a normal sized house. These computers frequently burned out and had a tendency to short-circuit (History Learning Site 2006).

In the late 1950s and early 1960s however, computers reduced in size because one of their main components (the valve) was replaced by the much smaller transistor (History Learning Site 2006). This was a big turning point as computers were becoming far more reliable with businesses taking a much greater interest in them (History learning site 2006). The introduction of transistor-based computer systems, which were smaller and cheaper compared to vacuum-tube based machines "led to an increase in the use of computer technology" (Gercke 2011: 31).

By the mid-1960s, transistor-based computer systems went on to be replaced by a miniaturised circuit known as the 'microchip' (which could have several transistors on it). This further led to a decrease in the size of computers, and by 1965 there were estimated to be around 20,000 computers in the world. The microchip subsequently led the production of computers small enough to get into the average sized room in a house, and by 1970 one microchip had the capability of 1000 transistors (History Learning Site 2006).

However, one of the most significant inventions that paved the way for the PC was the ‘microprocessor’. The first microprocessor on the market was developed in 1971 by an engineer from Intel, named Ted Hoff (History 2014). Microprocessors were the size of a thumbnail, and could do things the integrated-circuit chips could not, such as: running the computer’s programs, remembering information and managing data all by themselves. Before microprocessors were invented, computers were still very large and needed a separate integrated-circuit chip for each one of their functions (History 2014).

Innovations such as the microchip and microprocessor thus made it cheaper and easier to manufacture smaller and relatively cheaper microcomputers (History 2014). As a result, microcomputers became more prominent with the arrival of the personal computer (PC) in the early 1970s, regarded as the ‘first generation’ PCs. However, these PCs were considered to be expensive and highly technologically advanced for a general user, partly because early PCs were only available in parts, and had to be assembled by the user (Miller 1989: 29). These did not do much considering they had no keyboard and no screen, and their output was just a bank of flashing lights where users would input data by flipping toggle switches (History 2014). In addition, there was no hardware and software support for the user due to the limited number of both hardware and software developers at the time (Miller 1989: 29).

In the early 1970s personal computers were therefore used only by hobbyists. The first ‘hobby’ personal computer was introduced in 1974 and was called the ‘Altair 8800’ (History Learning Site 2006). For approximately $439 at the time, the Altair 8800 for the first time included an all-in-one kit that consisted of: assembly instructions, a metal casing, power supply, and all of the boards and components required. The process took many days and nights of careful soldering and assembly to hopefully create a working Altair, and only true computer hobbyists would be able to undertake such an endeavour (oldcomputers.net 2014).

In the following year two Harvard students named Paul G. Allen and Bill Gates developed the initial software for the Altair (known as Altair BASIC), which was much easier to use and considered to be the first software ever developed for a PC (Evans and Mack 1999). In April 1975 the two young programmers took the money they made from ‘Altair BASIC’ and formed a company called ‘Micro-Soft’ later changed to ‘Microsoft’ (History 2014). Microsoft became a dominant global company in the IT industry (History Learning Site 2006).

Another important breakthrough occurred in 1975 when Apple Computers was founded by two college students, Steve Jobs and Steve Wozniak in their parents' garage. They claim to have built the first 'home/personal computer' that could be used by anybody, and was known as the 'Apple I' (Briard 2008). The 'second generation' of PCs arrived towards the end of the 1970s and early 1980s, and became more popular and available to a much wider audience including the scientific and engineering community (Miller 1989: 29).

The second generation of PCs also saw the introduction of ready to run computers such as the Apple II which was launched in April 1977 and became an immediate success. The Apple II PC was sealed in a neat plastic casing, included a keyboard, colour screen and used removable floppy discs (History Learning Site 2014). In order "to make the Apple II as useful as possible, the company encouraged programmers to create applications for it" (History 2014). For example, a spread-sheet program known as 'VisiCalc' made the Apple II a practical tool for all kinds of individuals and businesses, not just hobbyists (History 2014). "It went on sale in 1979 and within 4 years it had sold 700,000 copies at $250 a unit" (History Learning Site 2006).

These improvements paved the way for the 'third generation' of PCs which came into existence in the 1980s. They received an even greater level of acceptance with businesses, corporations and individuals embracing them more and more. The 1980s saw an increased convenience and improved user support of PCs characterised by the astonishing rise of the hardware and software industry (Miller 1989: 29). Soon companies like Xerox, Tandy, Commodore and IBM had entered the market, and computers became widespread in offices and eventually homes. Innovations like the 'Graphical User Interface' (which allows users to select icons on the computer screen instead of writing complicated commands) and the computer mouse made PCs even more convenient and user-friendly (History 2014).

Towards the end of the 1980s, the 'fourth generation' of PCs arrived and they were much smaller and cheaper compared to the preceding technology. This generation formed the basis of a hugely successful industry and examples include: the Mac II, the IBM System 2, and the Compaq (Miller 1989: 29). These smaller PCs were considered to be very powerful and allowed several machines to connect with each other, which eventually led to computer networking and the internet (Techi Warehouse 2010). By the early 1990s, the PC revolutionised the lives of young people as it became easily affordable and accessible through schools, libraries, and homes. The sixth generation computers include the post 1990 computers to the present day computers, as well as those that are currently being developed such as mobile wireless communication devices which include smart phones, tablets and wearable devices.

3.3.2. The History and Development of the Internet

The internet is defined as a publicly accessible computer network connecting many smaller networks from around the world (Merriam-Webster 2014b). The internet was the result of some visionary thinking by people in the early 1960s that saw great potential value in allowing computers to share information on research and development in scientific and military fields (Howe 2012). Another catalyst in the formation of the internet was the heating up of the Cold War. The Soviet Union's launch of the Sputnik satellite spurred the U.S. Defence Department to consider ways information could be disseminated even after a nuclear attack (USG 2014). This eventually led to the formation of the Advanced Research Projects Agency Network (ARPANET), which ultimately evolved into what we now know as the ‘Internet’ (University System of Georgia 2014). ARPANET first went online in 1969 with connections between computers at the University of California at Los Angeles (UCLA), Stanford Research Institute, the University of California-Santa Barbara, and the University of Utah (Merriam-Webster 2014b).

ARPANET was a great success but membership was limited to certain academic and research organisations which had contracts with the US Defence Department (USG 2014). Its purpose was to conduct research into computer networking in order to provide a secure and survivable communications system in case of war. But as the network quickly expanded, academics and researchers in other fields began to use it as well (Merriam-Webster 2014b). More universities and hosts were added to ARPANET as the system stabilised, and by 1981 there were over 200 hosts on the system (WhoIsHostingThis.com 2014). ARPANET has been responsible for some major innovations including: the development of the first program for sending electronic mail (e-mail) over a distributed network in 1971, the use of mailing lists, newsgroups and bulletin-board systems (Merriam-Webster 2014b).

The 1st of January 1983 is regarded as the date of the internet’s official commencement. Before this, most computer networks did not have a standard way of communicating with each other. A new universal communications protocol was established called Transmission

Control Protocol/Internetwork Protocol (TCP/IP), which allowed different kinds of computers on different networks to 'talk' to each other. Thus the internet was established as all networks could now be connected by a universal language (USG 2014). Using this new protocol for data transmission, the National Science Foundation created a network (NSFNET) in 1986, capable of handling 1.5 megabits per second, and thus replacing an out-dated ARPANET (WhoIsHostingThis.com 2014). By 1990, ARPANET ceased to exist, leaving behind the NSFNET, and the first commercial dial-up access to the internet became available (Merriam-Webster 2014b).

However, the internet changed significantly when a computer programmer working for the European Organisation for Nuclear Research (CERN) in Switzerland, named Tim Berners-Lee, invented the 'World Wide Web' (WWW) in 1989 (History 2014). The web was originally conceived and developed to meet the demand for automatic information-sharing between scientists in universities and institutes around the world (CERN 2014). Today, the web works by giving users access to an immense array of documents that are connected to each other by means of hypertext or hypermedia links (hyperlinks are electronic connections that link related pieces of information in order to allow a user easy access to them) (Britannica 2014).

The internet became not just a simple way of sending files from one place to another but was itself a 'web' of information which anyone on the internet could retrieve (History 2014). The Web operates within the internet's basic 'client-server' format where the servers are computer programs that store and transmit documents to other computers on the network when asked to, while clients are programs that request documents from a server as the user asks for them. In addition, browser software allows users to view the retrieved documents (Britannica 2014).

The World Wide Web became universal by the mid-1990s, and the internet saw a massive growth which had not been seen with any preceding technology (Peter 2004). Furthermore, many businesses began to shift their attention onto the web and in several cases, "if a company was seen to be on the web, their stock prices would then shoot up" (Lumsden 2012). This was known as the internet 'dotcom' boom which marked the commercial growth of the internet since the beginning of the World Wide Web (Lumsden 2012). The aptly named 'dot-com boom' of the late 1990s saw many people move their businesses online, such as newspapers, retailers, and entertainment offices (WhoIsHostingThis.com 2014). Since then, the internet has continued to grow. By 1998 there were approximately 750,000 commercial sites on the World Wide Web, and businesses were beginning to see how the internet would bring about significant changes to existing industries such as travel and hospitality with online bookings and reservations (Peter 2004).

One of the recent milestones in the history of the World Wide Web has been accessibility via mobile devices. Up to this point accessing the web had fundamentally been from computers or laptops. “The number of users accessing the web from mobile devices is growing rapidly and is set to overtake desktop access by 2015” (Lumsden 2012). This trend began in 2007 with the release of the Apple ‘iPhone’, which revolutionised the way that we access the web from our phones by introducing the concept of mobile applications (apps). For example, because of mobile apps, the World Wide Web was now interactive and able to understand our location from anywhere in the world. It also enabled us to upload a photo taken instantly and put it directly onto our social networking profile (Lumsden 2012).

In this regard, the Web has changed everything from business communications to social interaction, and it will continue to do so as it continues to grow and develop (WhoIsHostingThis.com 2014). The internet is widely regarded as a development of vast significance that will affect nearly every aspect of human culture and commerce in ways still only partly understood (Merriam-Webster 2014b). However, it is important to note that the web is constantly changing and at a rapid pace. As we have observed from the history and development of cyberspace, the latest greatest technology that currently defines the web, will be superseded by something even greater, faster and better in the future (Lumsden 2012).

As the internet started to become essential to running governments and economies, it soon became an advantage, but also vulnerable and thus potentially a valuable target. The next section will explore how insecurities manifest within the cyberspace environment.

3.4. Manifestations of Cyber Insecurity

Cyber insecurity can result from the vulnerabilities of cyber systems, including flaws or weaknesses in both hardware and software, and from the conduct of states, groups, and individuals with access to them. It takes the forms of cyber warfare, espionage, crime, attacks on cyber infrastructure, and exploitation of cyber systems. Virtually all aspects of cyber insecurity have a transnational component, affecting users of cyber systems throughout the world (Sofaer, Clark and Diffie 2010: 179).

The above mentioned activities can expose every member of society from the level of the individual user up to the nation-state level with severe consequences. Some of the consequences of cyber insecurity can include the loss of critical and sensitive information, loss of revenue, lack of access to legitimate online services, violation of privacy, exposure to cyber-attacks, and exposure to cyber fraud (Serianu 2014: 9).

It can be argued that the conception of threats arising in cyberspace has grown out of the fear of increased vulnerability and loss of control, as a result of moving from an industrial to an information society (Eriksson and Giacomello 2006: 225). Conceptions of cyber-threats have originated in both the private and public sphere, among military as well as civilian actors. Recently however, "cyber exploitation and malicious activity are becoming increasingly sophisticated, targeted and serious" (Eriksson and Giacomello 2006: 225). In order to further understand the manifestations of cyber insecurity, the following sub-sections will explore the development of cybercrime as well as the characteristics of cyber-attacks.

3.4.1. The development of cybercrime

In the 1980s, as the number of personal computers grew, software codes and programs became readily available in the market. Curious young people took advantage of this, quickly became experts in software programming, and soon realised that they could easily manipulate computer systems for personal gain by use of malicious software (malware). Furthermore, new forms of computer crime became recognised including: the illegal use of computer systems, the manipulation of electronic data and computer-related fraud (Gercke 2011: 32).

The interconnection of computer systems introduced a new form of crime as the networks enabled offenders to penetrate a "computer system without being present at the crime scene" (Gercke 2011: 32). Consequently, more and more computer viruses were discovered, as the likelihood of distributing software through networks allowed offenders to spread malware discreetly (Gercke 2011: 33). It is believed that a group of curious young gifted kids got involved with these new tools in large numbers and gave birth to the first generation of hackers and cyber criminals. These so called 'gifted kids' are held responsible for leading the second generation of cybercrimes (Kizza 2014: 4).

The second generation of cybercrimes started during the 1990s and lasted till 2000. As the number of internet users grew exponentially, there was also an explosion of malware, in both quantity and quality (Geers 2011: 23). This period also saw an unprecedented growth in interconnected and interdependent computer networks around the globe, which became a very good channel for the spread of serious, often devastating, and widespread computer virus attacks (Kizza 2014 : 5).

According to Kizza (2014: 5), certain factors were responsible for fuelling the rise and destructive power of computer virus attacks. These included: the large volume of free hacker tools available on the internet, the widespread use of computers in homes, organisations and businesses, the large numbers of curious young people growing up with computers in their bedrooms, the growing interest in computers, the anonymity of users on the internet and lastly, the ever-growing dependence on computers and computer networks (Kizza 2014: 5).

As in previous decades, “new trends in computer crime and cybercrime continued to be discovered in the 21st century” (Gercke 2011: 34). At the turn of the new millennium, the third generation of cybercrimes emerged. Virus attacks had become the greatest source of financial losses globally. This period was characterised by small, less powerful, sometimes specialised but selective and targeted attacks. The targets were preselected to maximize financial gains (Kizza 2014: 5). Thus, “the first decade of the new millennium was dominated by new, highly sophisticated methods of committing cybercrimes” (Gercke 2011: 34).

The fourth generation of cybercrimes began a decade later and has been driven by a dramatic change in communication technologies as well as the nature of the information infrastructure. This has resulted in the exceptionally fast growing infrastructure of social networks enabling a more threatening computing environment. This changing nature of ICTs against the changing background of user demographics has created a dynamic variety of security threats and problems (Kizza 2014: 6). In this current generation of cyber-attacks, there are two major trends: first, the emergence of cyber-criminal enterprise cartels and secondly, a growth in state-sponsored hacking activities (Kizza 2014: 6).

3.4.2. Characteristics of Cyber Attacks

According to the UNIDR, cyber-attacks are often defined broadly as the unauthorized penetration and exploitation of computers or digital networks (UNIDR 2013: xi). In addition, cyber-attacks are "intended to prevent users from access to services or to disrupt computer-controlled machines, while cyber exploitation is conducted to penetrate computers and obtain information" (Lin 2012: 77). A cyber-attack is carried out by individuals known as hackers. The term 'hacker' refers to any individual or group that bypasses security mechanisms in order to access unauthorised data from a computer system. Most hackers are regarded to be highly skilled computer programmers who are able to locate security gaps and access secure systems using unique analytical skills (Techopedia 2014c).

Choo (2011: 724) further explains "that cyber-attacks can either be a so-called 'syntactic' or 'semantic' attack, or a combination of these called 'blended' attacks". A syntactic attack is one that exploits technical vulnerabilities in software and hardware to commit cyber-crime, such as the installation of malware on systems to steal data (Choo 2011: 724). Semantic attacks, alternatively exploit social vulnerabilities to gain personal information such as scam solicitations and online auction fraud. In recent years however, there has been "a continuing movement from either of the above attacks to blended attacks (that is attacks using technical tools to facilitate social engineering in order to gain privileged information)" (Choo, 2011: 724). Social engineering can be described as a form of online psychological manipulation in which an attacker misleads an individual into divulging sensitive information in order to gain access to a system. Cyber-attacks can be further broken down into two categories, malicious software attacks and denial of service (DoS) attacks. They shall be briefly discussed below.

i. *Malicious Software (malware) attacks*

Malicious software also known as malware refers to any software that brings harm to a computer system and its user. Hackers are frequently developing new techniques and tools to exploit vulnerabilities. Schreier (2012: 41) believes the problem is that it is cheap to develop malware, while protecting against it costs a lot. In 2010 for example, McAfee (2011: 7) "identified more than 20 million new pieces of malware or an average of nearly 55,000 per day, each one representing a new cyber weapon for attackers". It also reported increases in targeted attacks in their sophistication and in the number of attacks on new smart devices in 2010 (Schreier 2012: 41). This illustrates how thousands of known vulnerabilities in IT systems exist, with new ones being discovered each day.

Thus, the changing nature of both technology and the cyber threat environment makes the risk of a cyber-attack difficult to anticipate and quantify. The most common forms of malware consist of: viruses, worms, Trojan horses and spyware. They will be discussed briefly below:

- ***Viruses****:* Computer viruses are malicious programs that can self-replicate and cause damage to the system they infect. In addition, these programs can delete information, infect programs as well as infect the vital part of the operating system that ties together how files are stored (Reveron 2012: 8). Interestingly, a computer virus spreads similar to a biological virus, which injects DNA into a host cell in order to replicate itself and cause the cell to burst, then releases the replicated viruses to spread to other cells (Graham, Howard and Olson 2011: 198).

  Viruses are spread when their host is connected with the target system, either through a computer network, the internet, or a form of removable media. Meyers, Powers and Faissol (2009: 14) note that "the spread of viruses is dependent on user interaction, in particular in the execution of the corresponding virus code". The security community further divides viruses into two groups based on how the virus infects other files after it is executed. These are resident and non-resident viruses. The latter refers to a virus which infects other files only when the infected file runs, while the former differs by "loading itself into memory and continuing to run after the infected file closes" (Graham, Howard and Olson 2011: 200).

- ***Worms***: "Computer worms constitute a large class of malware that spreads between computers by distributing copies of themselves in a variety of ways" (Graham, Howard and Olson 2011: 195). The worm is one of the earliest forms of malware and may be either benign or destructive. However, malware is only considered to be "a worm if it spreads to other systems by duplicating itself without attaching to other files" (Graham, Howard and Olson 2011: 195). Worms are similar to viruses but are distinct for their ability to self-replicate without infecting other files in order to reproduce (Reveron 2012: 8). Another difference between worms and viruses is that while viruses always hide in software as surrogates, worms are stand-alone programs (Kizza 2014: 89).

  Worms typically have two roles. The first is to spread to additional computers, but most also have a secondary task known as a payload. A worm's payload is what the attacker programs the worm to accomplish after it spreads (Graham, Howard and Olson 2011: 195). Many worms spread by targeting vulnerabilities in popular network servers, as well as e-mails, peer-to-peer (P2P) networks, social networks, and mobile device communication protocols. However, these methods depend on deceiving the user into executing a program and worms cannot spread without any human interaction (Graham, Howard and Olson 2011: 197).

The latest versions of the worm are now spreading through mobile devices and social networking sites. In mobile devices, worms can spread by sending copies of themselves attached to short message service (SMS) messages, "or by including links to Web pages that host a copy of the worm" (Graham, Howard and Olson 2011: 197). In 2009, for example, a worm known as 'Sexy View' spread to phones that were running on the Symbian mobile operating system (OS) and further collected information about each device it infected (Fortinet 2009).

- ***Trojan Horses***: Trojan horses are stealthy codes that work under the guise of a useful program but performs malicious acts such as the destruction of files, the transmission of private data, and the opening of a back door to allow a third-party control of a machine (Reveron 2012: 8). "Much like the mythical Trojan horse, Trojan attacks function by concealing their malicious intent. They masquerade as a piece of software that performs a desired function, while secretly executing malicious content" (Meyers, Powers and Faissol 2009: 14). Users are misled into installing the Trojan through one of many paths mostly through online downloads or email links. "The most common types of Trojans install a 'backdoor' on infected systems to allow remote access, or engage in data destruction" (Meyers, Powers and Faissol 2009: 14).

- ***Spyware***: "Spyware is a type of malware that gained its name based on its main intention of spying on a user's activity without the user's consent" (Graham, Howard and Olson 2011: 224). However, to "qualify as spyware, programs must lack an End User License Agreement (EULA) or a privacy policy, and if a program has an agreement or policy that is intentionally deceptive, it also qualifies as spyware" (Graham, Howard and Olson 2011: 224).

An attacker installs spyware onto a system in order to monitor a user's activity without his or her knowledge, with the overall goal of stealing information. Examples of information stolen from systems that have been infected with spyware include: "typed keys, raw data, e-mail addresses, credentials, certificates, pictures and videos from attached Web cams, audio from an attached microphone, documents, software licenses, network activity, and cookies" (Graham, Howard and Olson 2011: 224). The motives behind attackers' use of "spyware to steal sensitive information and credentials generally involve identity theft or account access" (Graham, Howard and Olson 2011: 226). Besides gaining access to sensitive information and data, targeted attackers use spyware to gather intelligence and sensitive documents from compromised systems (Graham, Howard and Olson 2011: 226).

ii. *Denial of Service (DoS) attacks*

A denial-of-service (DoS) is any type of attack where the attackers (hackers) attempt to prevent legitimate users from accessing the service (Techopedia 2014a). DoS attacks do not change, alter, destroy, or modify system resources but affect a system by diminishing the system's ability to function: hence, they are capable of bringing a system down without destroying its resources (Kizza 2014: 96). Attackers execute DoS attacks by overwhelming the targeted computer system with data and requests that cause the system to cease functioning (Kesan and Hayes 2012: 837).

However, a bigger threat exists in the form of a distributed-denial-of-service (DDoS). Unlike a DoS attack which uses a single host, a DDoS attack uses several "hosts to overwhelm a server, causing a website to experience a complete system crash" (Techopedia 2014b). In recent years, DDoS attacks have been the most dominant form of cyber-attacks. A standard DDoS attack begins when an attacker takes advantage of vulnerabilities in a computer system. The compromised computer then becomes the DDoS master. Using this master system, the hacker is able to detect, communicate and infect other systems while making them a part of the compromised systems (Techopedia 2014b).

A compromised computer system controlled by "a hacker is called a zombie, while a set of compromised computers is called a zombie army or a botnet" (Techopedia 2014c). A zombie in this case refers to a computer that has been silently compromised and is controlled by a third party, while a botnet is a network of zombie machines used by hackers for massive coordinated system attacks (Reveron 2012: 8). “Using a single command, the hacker instructs these zombie machines to initiate several flood attacks toward a particular target which causes a denial of service” (Techopedia 2014c). In a DDOS attack, both the final target and all the compromised computer systems are victims of this kind of attack (Techopedia 2014b).

According to a recent report by security firm Incapsula, DDoS attacks are growing in size and frequency as cybercriminals evolve their methods of attack in reaction to improved security measures. The report also claims that traffic created by DDoS attacks had risen by 240 per cent in 2014 compared to the same period in 2013 (Gilbert 2014a). According to another recent survey, four out of ten organisations (41 per cent) globally suffered a DDoS attack in 2014, with more than three quarters of those (78 per cent) targeted twice or more (Ranger 2014a). On February 10th 2014 for instance, an internet security firm known as Cloudflare claimed to have protected one of its clients from what might have been the largest DDoS attack documented so far. At the height of this attack, the near 400 gigabytes per second (Gbps) assault was about 30 per cent larger than the largest attack documented in 2013 (Apps 2014).

3.5. Motivations Fuelling the Growth of Cyber Attacks

In recent years, cyber-attacks have grown in both number and severity. Cyber- attacks have now become bolder and designer-tailored with capabilities of infiltrating more systems than ever before. This can be attributed to five main reasons: The first reason deals with the rapid growth in technology. The phenomenal growth in both the computer and telecommunication industries has empowered millions of people to access the internet from virtually anywhere (Kizza 2014: 114). Devices such as portable laptops, tablets and smartphones have made internet access easier because people can now log on to the internet anytime and anywhere. This has widened the arena for cyber-attacks to grow (Kizza 2014: 114).

A second reason for the growth of cyber-attacks has been the easy availability of hacker tools online. Kizza (2014:114) notes that “There are an estimated 30,000 hacker- oriented sites on the internet, advertising and giving away free hacker tools and hacking tips, and with time, one can go through a good number of hacker sites, picking up tips and tools and coming out with a ready payload to create mayhem in cyberspace”. The ability to download hacking tools means that a determined 12-year old with some basic computer skills, if he or she has an internet connection, can become a successful hacker. For the more advanced, there are cyber-crime black markets that sell personal data, credit card information, tools, passwords, and successful exploits. Criminals can rent 'botnets' from the cybercriminal underworld or even purchase complete online stores to collect personal information or to sell bogus products (Lewis 2014: 4).

Anonymity is a third reason for the growth of cyber-attacks. As computers become smaller and people with those small internet accessible gadgets become more mobile, hacker tracing, tracking, and apprehending has become more difficult than ever before. Now hackers can hide in smaller places and spend a lot of time producing deadlier viruses drawing very little attention (Kizza 2014: 114). The fourth factor to consider is faster communication speeds. With the latest developments in broadband and wireless connectivity, bandwidth and high volumes of data can be moved in a short space of time. Kizza (2014: 114) says "this means that intruders can download a payload, very quickly log off and possibly leave before detection is possible".

The fifth and final factor behind the growth of cyber-attacks stems from our increasing dependency on computers. "The evidence lies with the ever-increasing access to cyberspace, coupled with the increasing capacity to store huge quantities of data, the increasing bandwidth in communication networks to move huge quantities of data, the increased computing power of computers, and plummeting computer prices have all contributed to an environment of human dependency on computers" (Kizza 2014: 115). This in turn, creates an enabling environment for hackers to expand their scope of cyber-attacks.

3.6. Sources of Cyber Attacks

Having identified the motivations fuelling the growth of cyber-attacks, it is important to note that cyber-attacks originate from a variety of sources. These include nation-states, terrorists' use of cyberspace, organised cybercriminal organisations and hacktivists.

3.6.1. Nation-States and Cyber-power

Nation-states are regarded as the most powerful actors in cyberspace considering the fact they are capable of utilising a wide range of cyber-attack capabilities and methods, ranging from the most sophisticated and precise malware to the more simpler method of DoS attacks targeting leading persons, or organisations (Sheldon 2012: 7). However, not all states possess the same cyber-power capabilities. In this regard, cyber-power can be understood to be the national ability to disrupt an obscured actor somewhere in the digitised globe, whether non-state or state, in proportion to its motivations and capabilities to attack with violent effects and remain resilient against imposed or enhanced nasty surprises across all critical nationally sustaining systems (Demchak 2011: ix).

Cyber-power is a useful strategic instrument for nation-states since it can be wielded globally with a certain degree of anonymity during times of peace, crisis, and war. It also enables global reach, creating the ability to attack critical systems such as national infrastructure remotely, deceive individuals into divulging sensitive information, and disrupting services (Sheldon 2013: 316). Thanks to cyber-power, modern militaries have been exposed to greater efficiencies and magnified effects, which in turn have created leaner force structures with more automated capabilities, placing a premium on recruiting more highly skilled personnel (Sheldon 2013: 316). The pervasiveness of cyber-power will continue to influence and change modern militaries in terms of organisation, structure, and the use of force.

Nation-state cyber activities can primarily involve: espionage and military/covert operations that require large numbers of specialist personnel and the bureaucracies to manage them, infrastructure ranging from research and development entities able to provide cutting edge technologies and methodologies to hardware and facilities, financial and human resources, and also the political legitimacy and/or veil of secrecy required for potentially controversial cyber warfare operations (Sheldon 2012: 6). As such, the last ten years have seen rapid investments in cyber-power by governments and the military across the world despite this being a time of declining budgets, as it is now considered a basic requirement for national security. Another growing trend has been the shift in investment from cyber-defence initiatives to cyber-offensives (Ranger 2014b). The director of the Centre for 21st Century Security and Intelligence at the Brookings Institution Peter W. Singer recently stated that around 100 nation-states are in the process of building cyber military commands of which about 20 nation-states are serious players, with a smaller number capable of carrying out a full cyber war campaign (Ranger 2014b).

Some nation-states have the capability of pursuing specific targets within cyberspace in line with achieving their strategic interests. Kesan and Hayes (2012: 434) give us an example of how in 2010, a highly sophisticated piece of malware known as 'Stuxnet' believed to be developed by Israel and the USA, was used to cause a significant disruption in Iran's nuclear enrichment programme, damaging most of the centrifuges at the Natanz uranium enrichment plant. Such an assault could potentially signify a revolution in military affairs in which a cyber-attack can be used to cause massive physical damage to critical infrastructures at very low costs, making it a favoured weapon of choice for the military. Thus, it can be argued that nation-states are generally motivated by the constant need for information on the intentions and activities of other governments, terrorists and criminal organisations, as well as commercial entities (Sheldon 2012: 6).

Nation-states have also been able to take advantage of cyberspace in achieving strategic political objectives with the minimal use of resources. The spread of high-speed global networks has made it easier for nation-states to extract massive quantities of data and information. It is believed that some powerful government agencies are able to target companies similar to competitors and private hackers seeking intellectual property and confidential business information (Lewis 2014: 2).

Some cyber-attacks initiated by governments could target the private sector of another state. China for example, has become associated with cyber-attack and cyber espionage activities on other states. According to Jourdan (2014), the allegations are that Chinese state-owned firms employ a range of cyber-attack methods to illegally gather corporate information from mostly USA firms in order to give Chinese companies a competitive edge. In 2009 for example, Google announced that it had been the target of a 'highly sophisticated' and coordinated hack attack against its corporate network which was said to have originated from China. The hackers had stolen intellectual property and sought access to the Gmail accounts of human rights activists (Zetter 2010). This event became known as 'Operation Aurora' (Andress and Winterfeld 2011: 14).

More recently, a private American company, 'Sony Pictures Entertainment' made international headlines after it underwent a series of cyber-attacks in late November 2014. The attacks targeted personal employee information, confidential entertainment data, business documents and unreleased movies that were later leaked online. This resulted in a massive loss of revenue to the company as well as a violation of privacy of many senior employees. However, there were speculations as to where the attack originated from, and the Federal Bureau of Investigation concluded that North Korea was behind the attack by saying:

"North Korea's actions were intended to inflict significant harm on a U.S. business and suppress the right of American citizens to express themselves" (Robb 2014). North Korea was suspected of carrying out the attack because Sony had planned to release a comedy film called 'The Interview', portraying the assassination of President Kim Jung-un which North Korea strongly condemned. In this regard, the example of North Korea represents a cyber-attack initiated by a government on the private sector of another state.

3.6.2. Cyber Terrorism

Terrorist organisations seek to commit acts of terror against public targets in order to make political statements, or even trying to achieve political objectives (Sheldon 2012: 7).Cyber-terrorism can be understood to be the use of Web-based information technology to conduct enabling, disruptive, or destructive operations in cyberspace in order to create and elicit fear through violence or the threat of violence at the command of a radical militant belief system (Brickey 2012). Cyber-attacks by terrorist groups (such as Al-Qaeda) are usually well-funded and highly secretive, while young individuals that engage in such activities possess exceptionally high skills, and are also motivated by extremist ideology normally after being disillusioned by society (Meyers, Powers and Faissol 2009: 10).

Cyberspace can have an enabling function for terrorist organisations by: facilitating recruitment, radicalising young extremists, inciting hatred, delivering training, communicating commands, financing, planning, and conducting actual terror operations. At present cyberspace is useful to terrorist organisations since it provides a virtual presence for various groups (Rudner 2013: 455). A number of terrorist groups engage in cybercrime in order to raise money for their terror operations. Moreover, terrorists also use social engineering methods to identify human targets and also use cyberspace to gather intelligence in support of operations (Sheldon 2012: 7).

Another form of cyber-terrorism is disruptive cyber hacking, which involves the defacing or taking down of targeted on-line services, as well as gaining unauthorised access to, and disclosure of sensitive or private information (Rudner 2013: 455). Similarly to conventional terrorism, cyber terrorists are most likely to choose targets that are highly disruptive and publicly obvious (Andress and Winterfeld 2011: 198). On 12 January 2015 for example, the US Central Command's Twitter and YouTube accounts were suspended for a few hours after being hacked by a group claiming to support the terrorist organisation known as the Islamic

State of Iraq and Syria (also known as ISIS/ ISIL) (BBC 2015). During this cyber hacking incident, the group posted messages stating "In the name of Allah, the Most Gracious, the Most Merciful, the Cyber Caliphate continues Cyber Jihad… American soldiers, we are coming, watch your back" (BBC 2015). Such an attack may not necessarily be a national security threat but the consequences may result in creating widespread fear and panic to the general population.

Terrorists can also use cyberspace to influence the general public into a particular line of activity or thinking, such as fear and panic (Andress and Winterfeld 2011: 199). At present, terrorists generally use social engineering and data mining methods to support their efforts in the physical world, as well as tools commonly used to conduct cybercrime in order to fund their terror operations (such as online credit card fraud). In the near future, however, it is not unreasonable to assume that certain terrorist organisations will start using more powerful capabilities to achieve devastating effects (Sheldon 2012: 8).

Recently, ISIS has proven to be quite effective in using online channels to promote a jihadist cause through videos of beheadings posted online, a digital magazine distributed to followers worldwide, as well as a major presence on social media networks (Guzman 2014). The terrorist organisation has rapidly emerged as an international security threat comprised of an estimated 30,000 fighters who control large areas of Iraq and Syria (Guzman 2014).

With a deliberate mission to spread terrorist propaganda, ISIS published a gruesome video online on August 20th 2014 showing the tragic execution of an American journalist called James Foley. "The video spread through the internet despite efforts from social media administrators to block the graphic content" (Guzman 2014). Although editors and journalists at news organisations tried to self-censor the graphic video, it spread through social media networks and forums (Guzman 2014). As stated by Limnell (2014), what ISIS accomplishes in social media counts as a new form of warfare that wins hearts and minds without shots been fired. "It creates impressions of might, sophistication, and inevitability similarly to the same impressions made by the Kaiser's military machine in 1914 as Germany sought to define its own sphere of influence" (Limnell 2014).

3.6.3. Organised Cyber Crime

Criminal organisations use cyberspace mostly for power and monetary gain. Besides dealing with fraudulent activities online, organised cybercrime also involves the selling of personal identifying information (such as financial information and social security numbers) to other criminal organisations, terrorists, and even governments (Sheldon 2012: 9). It also involves espionage activities where individual proprietary information is sold off for the theft of money from individuals and institutions (Sheldon 2012: 9). Those involved in organised cybercrime make use of tools such as: malware, DDos attacks, identity theft, cyber warfare, as well as a wide range of tactics that might be regarded as a means to a particular end they wish to accomplish (Andress and Winterfeld 2011: 201).

Organised cybercrime features a complicated range of actors and networks whose relations change constantly depending on the criminal opportunities available. For example, hackers who steal financial information can either use the information themselves or sell it to groups who specialise in exploiting stolen details, who in turn hire teams of 'mules' or 'cashers' to launder money either through their bank accounts, or by buying goods with stolen credit card details and then repackaging and sending them on (Ranger 2014b).

More recently however, it has been claimed that dozens of cybercrime groups have reached high levels of sophistication where their technical capabilities are on par with those of nation-states. In this respect, organised criminal gangs are now capable of building complex systems aimed at stealing money and intellectual property on a grand scale, and is costing the global economy more than $400 billion (Ranger 2014b). In early August 2014, an unknown Russian organised crime ring amassed the largest known collection of stolen internet credentials, including 1.2 billion user names and password combinations and more than 500 million email addresses, security researchers say (Perloth and Gelles 2014). Initially, the gang acquired databases of stolen credentials from fellow hackers on the black market, who then used these databases to attack e-mail providers, social media networks, and other websites in order to distribute spam to victims and install malicious redirections on legitimate systems (Hold Security 2014).

3.6.4. Hacktivism

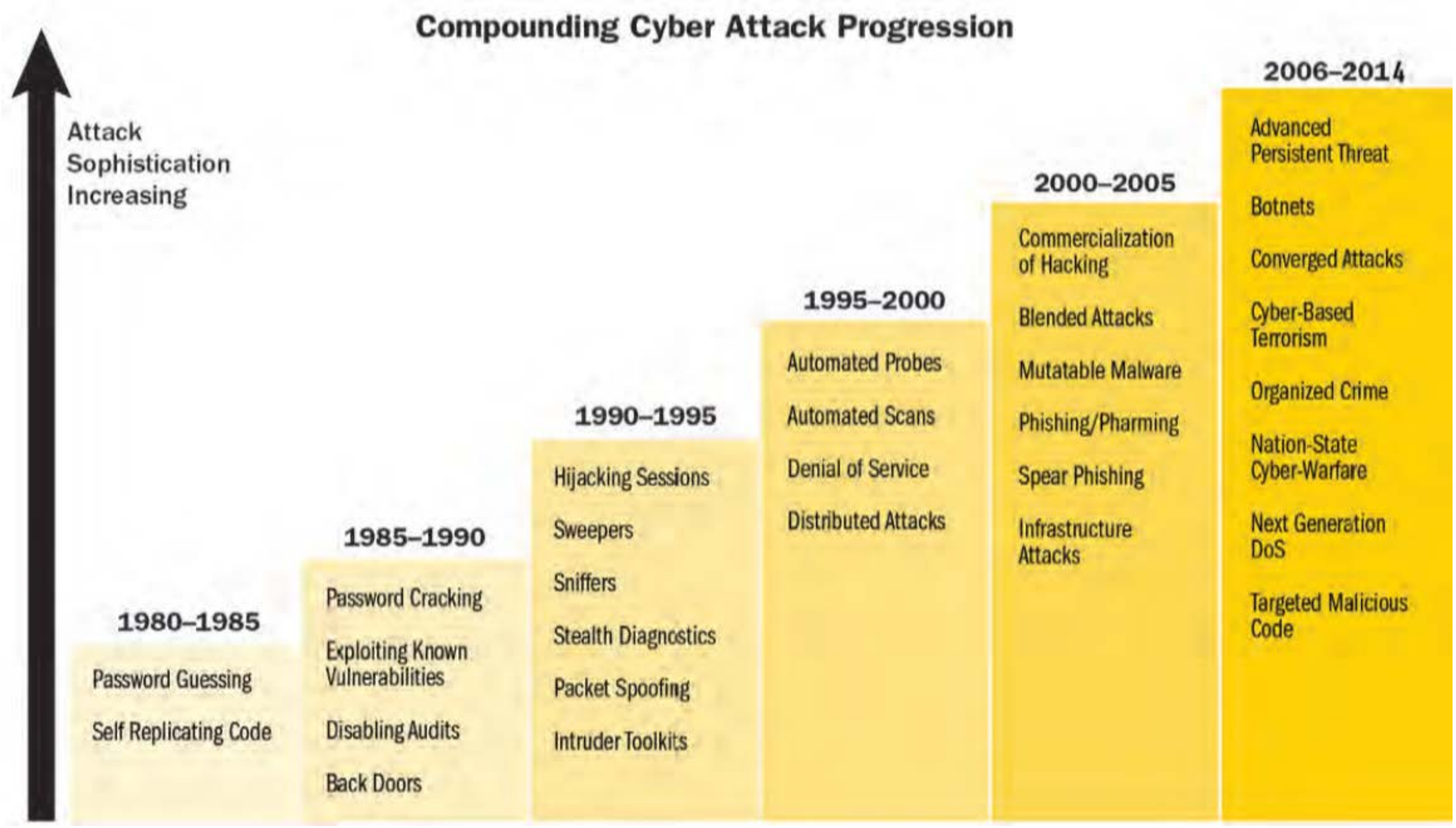
Hacktivists are hackers who use their skills to support a particular ideology. These attackers differ from the other classes in that they are motivated by a political cause rather than a form of personal monetary gain. Some of the causes supported by hacktivists include topics such as free speech, civil rights, religious rights, etc. In essence, nearly every issue we can find supported or attacked by activist groups and protestors, will have some element of hacktivism, even if discreet (Andress and Winterfeld 2011: 197).

Hacktivist methods include: overloading of email servers, website defacement, DDoS attacks and hacking into websites to send a political message (Reveron 2012: 12).Although they have also been known to use worms and viruses, their maliciousness is highly focused against the targeted organisations, though it can still have far-reaching consequences (Meyers, et al. 2009: 7). For example, around three years ago an international hacktivist group known as ‘‘Anonymous’’ was successful in temporarily disabling the online payment site of credit card company PayPal for refusing to transfer donations to the WikiLeaks organisation (Rudner 2013: 463).

More recently, the hacktivist group Anonymous knocked multiple official Israeli government websites offline in retaliation for the killing of one of its members in the West Bank on 27 June 2014 (Gilbert 2014b). Among the websites attacked by the group were the Ministry of Justice website, the state archive portal, as well as the national advertising agency. However, most of the attacks were repelled within hours, and all agencies went back online (RT News 2014).

Figure 1 illustrates how cyber insecurity has manifested itself since the inception of the personal computer.

Figure 1: The Changing Nature of Cyber Insecurity



Source: Kenya National Cybersecurity Strategy (2014: 7).

3.7. Cyber Security as a National Security Issue

Although the concept of cyber security is defined and understood in different ways, all conceptions narrow down to the protection of cyberspace. Furthermore, cyber security has also gained a national security dimension as the public, businesses, governments and the military have become increasingly dependent on computers and networked technologies (Boulanin 2013: 218). It would therefore be reasonable to argue that cyberspace itself has been securitised.

The securitisation of cyberspace is the "process that transformed the security of cyberspace into a national security issue" (Boulanin 2013: 219). From a political perspective, cyber security manages the challenges arising from cyberspace as a new platform for threatening activities such as cybercrime, cyber-terrorism, cyber espionage or even cyber-warfare. The belief is that a lack of cyber security might affect the security of the economy, the state as well as the society in general (Hansen and Nissenbaum 2009: 1161).

The securitisation of cyberspace is believed to have begun in the late 1980s, focusing first on issues of military relevance. “As individual states began to rely increasingly on network systems for the management of weapon platforms and critical infrastructure, military institutions also began to identify the potential threat of cyber-attacks capable of paralysing arsenals or even leading to the leakage of strategic information” (Boulanin 2013: 219). Consequently, these military institutions “began developing both defensive and offensive capacities to take action within cyberspace. For some analysts, cyberspace has since become a fourth ‘battle space’ after air, land and sea” (Rid 2012).

In the 1990s economic activities and social infrastructures became increasingly reliant on the internet and networked technologies (Boulanin 2013: 219).The securitisation process accelerated and gained a civil dimension, in the sense that “it became a national security issue beyond the traditional military sense” (Dunn 2008: 2). Information technology (IT) experts and security analysts monitored vulnerabilities arising from the interconnectivity of computer systems, and warned of the cascading effects of cyber-attacks on the economy, society and therefore, on national security (Boulanin 2013: 219).

Considering the fact that no major cyber disaster has yet happened, a number of events in recent years have strengthened the credibility of such a scenario, leading to political and institutional responses from international and national security communities (Boulanin 2013: 219). The Estonian Government and its agencies were among the victims of a large-scale cyber-attack in 2007. In April and May 2007, hackers unleashed a wave of cyber-attacks that crippled dozens of government and corporate sites in Estonia, which is considered to be one of Europe's most connected countries. Estonian authorities traced the so-called denial of service attacks to Russia, and suggested they had been coordinated by the Kremlin, a charge Moscow strongly denied (Associated Press 2009). Nevertheless, this event was portrayed as the ‘first war in cyberspace’ and caused alarm across the Western alliance, compelling them to urgently examine the implications of the attack on Estonia (Traynor 2007).

This attack subsequently led Estonia and nine other EU member states to adopt national cyber security strategies (Landler and Markoff 2007). It also prompted the North Atlantic Treaty Organisation (NATO) to adopt a policy on cyber defence, under which it formed a cyber-defence management authority and supported the creation of a cooperative cyber defence centre of excellence (CCDCOE) in Tallinn, Estonia, in 2008 (CCDOE 2014). In the United

States, President Barack Obama has made cyber security a priority of his presidency (White House 2009). The US Army followed suit in 2010 by creating a US Cyber Command (USCYBERCOM), and by 2011 the US Department of Defence had published a new cyber security strategy titled ‘Cyber 3.0.’ (US DOD 2011).

By 2012, cyber security had been pushed up on the agendas of the international political and security communities. The discovery of cyber weapons such as Stuxnet (the virus believed to have targeted Iran) made headlines and inspired new discussions about the growing use of cyber weapons and cyber warfare (Kaspersky 2012). However, while there is no substantial proof, a growing number of countries (including China, Iran, Israel, Russia and the USA) have been suspected of using cyber weapons and making offensive interventions through cyberspace (Perloth 2012).

In early 2013, two important developments related to cyber security occurred. The first happened in February 2013 when the European Union published its cyberspace strategy (European Commission 2013), and the second occurred in March 2013 when US officials stated that cyber-attacks had now replaced al-Qaeda as the greatest threat to US national security (Dilanian 2013). Since then, the US government has continued to intensify its cyber security efforts by increasing cyber security budgetary allocations and integrating cyber security through all government security agencies.

During his State of the Union address on 20 January 2015, US President, Barack Obama, outlined his administration’s legislative proposals for cyber security. These include a Cybersecurity Information Sharing Bill, the establishment of the US Cyber Threat Intelligence Integration Center (CTIIC), and a trans-Atlantic joint cyber cell in collaboration with the UK government made up of cyber defence experts (Open Briefing 2015: 11). The legislative proposals are said to be driven by “the combination of cyber espionage campaigns against the military and finance sectors, the potential loss of technological competitive edge, the low cost asymmetrical warfare capabilities of adversaries, and attacks on government institutions” (Open Briefing 2015: 11)

The rise of cyber security has thus had a significant effect on the political, economic and military sectors of the state (Boulanin 2013: 221). In the economic sector, the global public and private spending on cyber security was estimated to be approximately $60 billion in 2011

(PWC 2011). The USA was the biggest spender on cyber security, accounting for half of the total, and the only country that had equal levels of public and private spending on cyber security (PWC 2011). For the rest of the world however, the private sector accounted for the majority of national spending on cyber security (PWC 2011). According to some forecasts, the cyber security market should double in size by 2017, to about $120 billion (PRNewswire 2012).

Due to this strong growth as well as global reductions in military spending in some key weapon markets, many arms producing and military services companies have begun to show an increasing interest in the cyber security market. Diversifying into cyber security will enable these companies to develop technical capabilities for cyber warfare and cyber defence for the military sector (Boulanin 2013: 222). However, this will depend on whether or not cyber security will continue to grow in political, economic and strategic importance, levels of technical expertise in the public sector as well as governments' political room to manoeuvre in cyberspace (Boulanin 2013: 225). Such developments may transform the way in which states define and manage their cyber security and cyber defence policies (Boulanin 2013: 226).

It is plausible to suggest that as the organisation and structure of the military sector changes due to the pervasiveness of cyber-power, the way in which military force is used might also change. These changes could therefore culminate in "a twenty-first century revolution in military affairs (RMA) if they lead to new military doctrines, force structure, and changes in the conduct of war" (Sheldon 2013: 317).

3.8. Conclusion

In conclusion, cyber insecurity has noticeably evolved from a mischievous group of cyber hackers, to a wide range of profit-making professionals and organised criminal enterprises within a relatively short space of time. In this regard, cyber-attacks are increasing in occurrence, complexity and sophistication as a result of an increase in globalisation as well as the rapid growth and expansion of the internet. With this in mind, cyber-power is quickly becoming a valuable strategic instrument for governments as it can be utilised globally and covertly when securing specific national security interests.

Moreover, the absence of a sovereign authority in cyberspace has created an enabling environment for the development of cyber weapons by both state and non-state actors. In this regard, cyber-attacks have become the perfect instrument for asymmetric warfare by non-state actors due to the low barriers of entry. However, more worrying is the fact that cyber security today is evolving at a pace which many governments, organisations and even security providers are struggling to keep up with.

The next chapter will provide a case study of Kenya with regard to cyber security as an emerging threat to its national security.

CHAPTER 4: CYBER SECURITY IN KENYA

4.1. Introduction

This chapter will analyse Kenya's cyber security in order to determine the issues perceived as security threats in cyberspace. To achieve this, Kenya's current state of cyber security will be investigated by explaining the growing use and dependence on ICT networks and cyberspace as a potential threat to Kenya's national security.

4.2. Overview of Kenya's ICT Environment

Since the year 2000, ICTs have continued to play a vital role in the growth of the Kenyan economy. However, according to the International Standards of Industrial Classifications of All Economic Activities (ISIC) Rev. 4, Kenya's ICT sector is not yet considered a single sector in the annual economic survey but is classified under the 'Transport, Storage and Communications' sector. This makes it very difficult to track the actual contribution of ICT to the Kenyan economy unlike in many countries where ICT is defined as a single sector (Kenya 2014a: 32).

Between the years 2000 and 2012, Kenya's wider transport and communications sector (which ICT is a part of) grew by a Compound Annual Growth Rate (CAGR) of 7.7 per cent, overtaking all other sectors of the national economy (Ndung'u and Waema 2012: 1). By 2013, Kenya's ICT market had reached a value of US$5.16 billion, with telecommunication services accounting for 71.9 per cent, hardware making up 22.3 per cent, as well as IT services and software representing 3.0 per cent and 2.8 per cent, respectively. In this regard, ICT spending in Kenya is expected to continue growing and reach a value of US$5.86 billion by 2017 (IDC 2014: 5).

Due to this rapid growth in Kenya's ICT sector, the country has emerged as a leading African ICT hub in innovative technologies especially in the mobile telecommunication sector. The most significant innovation was the implementation of mobile money transfer services (commonly known as M-Pesa) by mobile operator Safaricom in 2007, which put Kenya on the world map and has led to increased financial inclusion of previously disadvantaged groups within society. At present, all the mobile operators in Kenya offer mobile money transfer services (Kenya 2014a: 30). Total mobile money transfer subscriptions grew by 1.4 per cent and stood at 26.9 million as of September 2014 (CAK 2015). Since 2013, 31 per cent of Kenya's GDP is now transacted through M-Pesa mobile telephone banking where 74 per cent of the country's adult population are active users (IDC 2014: 7).

Kenya has recently witnessed an expansion of local ICT development laboratories and centres including iLab Africa, Nailab, and iHub to name a few. iLab Africa is a partnership between local and foreign ICT corporations (such as Google, Samsung, Microsoft, Oracle, IBM, Ericson and Intel), the Kenya Education Network (KENET), and Strathmore University in developing a research and incubation facility that will help support entrepreneurship programmes in software and application development (Mwenesi 2014). Nailab is a start-up accelerator offering short entrepreneurship programmes focused on nurturing innovative ICT driven ideas (Nailab 2014). The iHub is a centre of innovation, offering a networking venue for the technical and professional community (Souter and Makau 2012: 49). It provides a community workspace, incubator and meeting place with high-speed internet connection, for computer engineers, programmers, web designers and other internet entrepreneurs (KHRC2014: 62).

Such developments have attracted a number of multinational ICT firms to establish their regional centre of operations in Kenya, as a way of expanding their local footprint and maximising their profits within the region (IDC 2014: 5). Kenya now serves as a base for multiple African regional hubs including IBM's first African Research lab, Nokia's Africa Headquarters, Google's first Sub-Saharan Africa office outside of South Africa, Huawei, Samsung, Qualcomm, Microsoft and General Electric (IDC 2014: 5). In this regard, multi-national companies (MNCs) have brought significant contributions to the country such as job creation, the remittance of requisite taxes, and the creation of awareness about the importance of ICT through capacity building initiatives (IDC 2014: 5).

4.3. Key Developments in Kenya's ICT Environment

The rapid growth of Kenya's ICT sector can be attributed to some of the government's policies and actions over the years. The key interventions by the Kenyan government include: the lowering of mobile operation rates and the issuing of unified telecommunications licenses (IDC 2014: 4). In 2006 the Kenyan government unveiled its strategic blueprint for economic and social development known as 'Vision 2030', which positions ICT as a key development pillar (IDC 2014: 5). Other official documents that put a strong emphasis on ICT growth for socio-economic development include: the Jubilee Coalition Government Manifesto (the

Jubilee Coalition is the current political party that came into power after the March 2013 national elections) and the '2017 ICT Master Plan'(IDC 2014: 5).There are two key developments in Kenya's ICT environment that are worth mentioning. The first is the rapid growth of internet usage in the country and the second is the government's adoption of e-government services. These are explained in the following section.

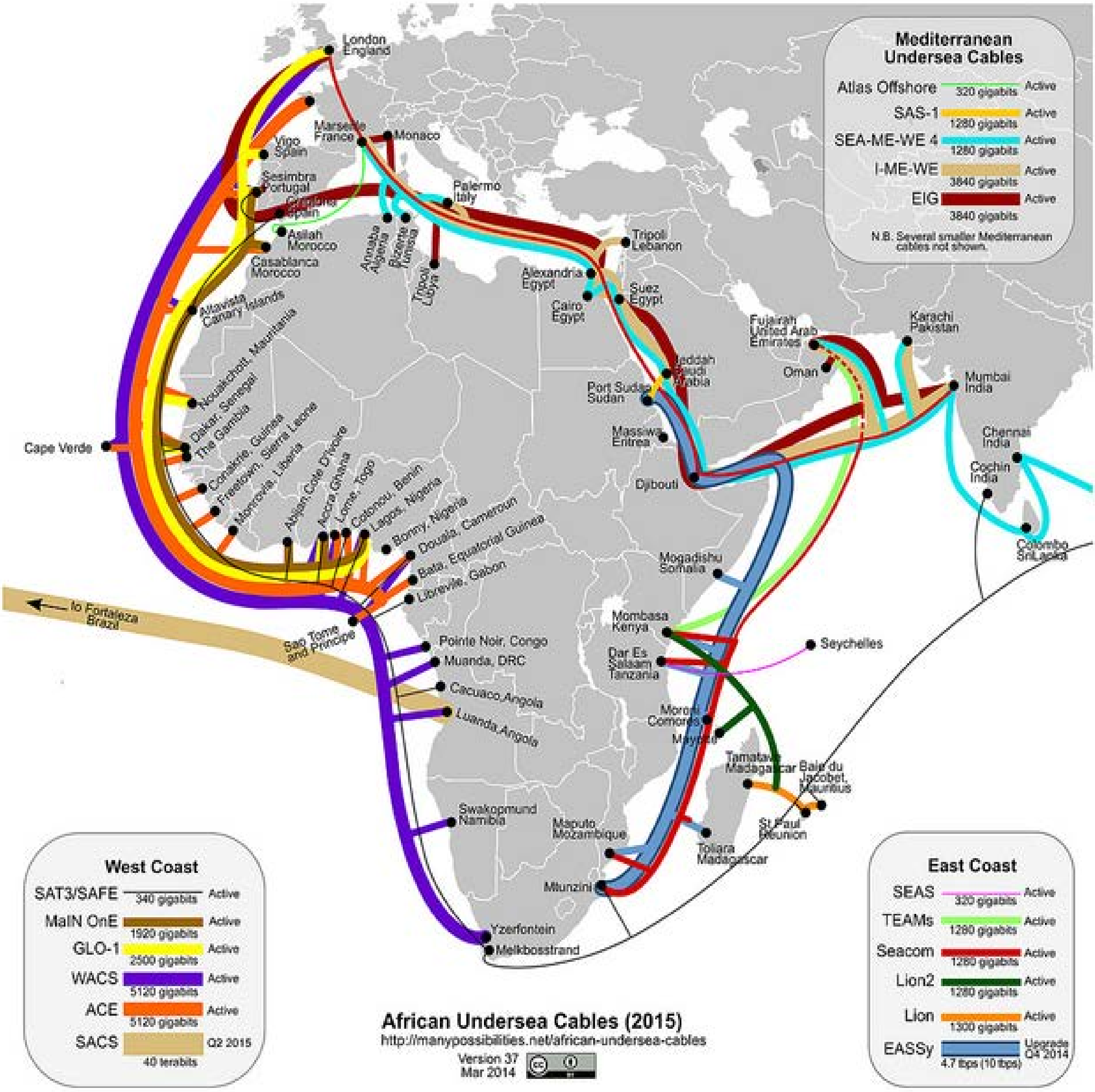
4.3.1. The rapid growth of Internet use in Kenya

The number of people accessing the internet in Kenya has been on a steady rise. As stated by the Communications Authority of Kenya (CAK), there were approximately 14.8 million people with internet subscriptions as of September 2014, a 5.8 per cent increase from the 14.0 million recorded in the previous quarter. In addition, the estimated number of internet users stood at 23.2 million in September 2014 up from 22.3 million in the previous quarter (CAK 2015). Until mid-2009, Kenya (like most African countries) depended solely on satellite technology to connect to the internet and communicate internationally. However, increased bandwidth through access to new undersea fibre-optic cables has led to the rapid growth of internet usage in Kenya. Currently, Kenya "is connected to the international broadband highway through the SEACOM, TEAMS, EASSY, and LION undersea fibre cables" (Kenya 2014a: 23). In 2006, the Government, in partnership with Emirates Telecommunication Establishment (Etisalat), built its own 5,000 Km fibre optic cable linking Mombasa on the coast of Kenya to Fujairah in the United Arab Emirates. The cable which was commissioned in 2009 has increased connectivity speeds and capacity and lowered the cost of internet access (Kenya 2009). Figure 2 illustrates Kenya's access to undersea fibre-optic cables in comparison to its neighbours and the rest of Africa.

In this regard, Kenya is now considered to be the leader of internet access and connectivity in the region. Kenya is reported to have the highest bandwidth per person in Africa and is said to have more undersea fibre-optic cables than any of its neighbours in the region. This has resulted in Kenya receiving international bandwidth speed of up to 20 gigabytes per second (Wangalwa 2014).

In addition, the government of Kenya has invested in the National Optical Fibre Backbone Infrastructure (NOFBI), which forms part of its ICT-related projects intended at enhancing service delivery to citizens and reaching up to 29 counties under the County Connectivity project (Kenya 2013). Most major towns in Kenya are connected through the National Optic Fibre Backbone Infrastructure (NOFBI) (Kenya 2014a: 24).

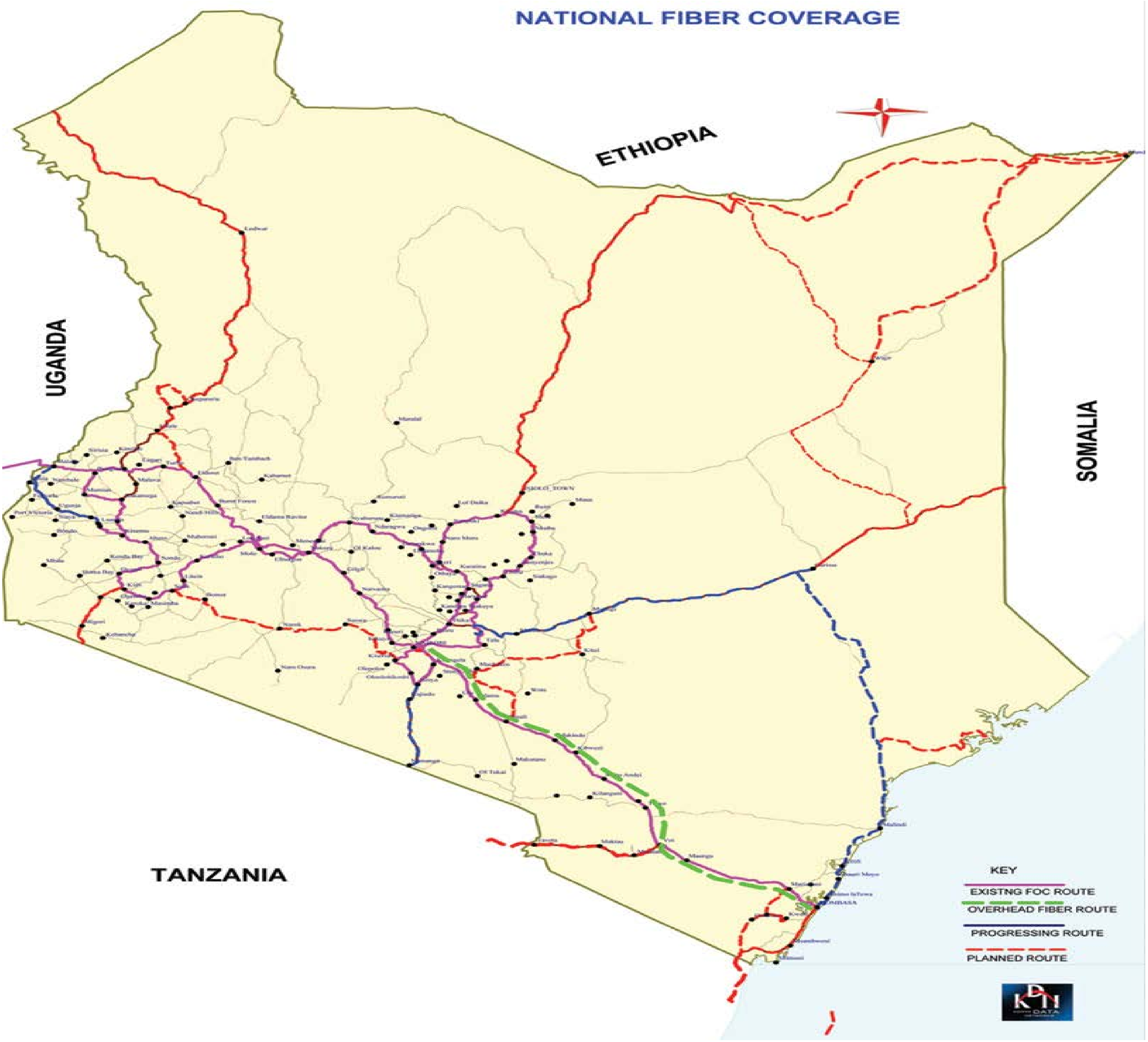
Figure 2: Africa Undersea Cables



Source: manypossibilities.net/african-undersea-cables

"In order to extend fibre capacity to all parts of the country, the Government is reviewing NOFBI with a view of extending and building additional links to enhance redundancy" (Kenya 2014a: 24). To complement the NOFBI, the ministry of ICT is in talks with private sector stakeholders in building a framework to develop a wireless national broadband network (Kenya 2014a: 24). Figure 3 illustrates Kenya's national fibre-optic coverage.

Figure 3: Kenya National Optic Fibre Backbone Infrastructure



Source: Kenya National broadband strategy: 2013

The $60 million project covering 5,000Km is managed by Telkom Kenya and service providers pay fees to access the network. NOFBI was established to enable government agencies to provide services online (e-government), lower costs of entry to business for internet Service Providers and ultimately, offer faster internet access in rural areas not covered by fibre deployment (Schumann, Robert and Kende 2013: 41). The NOFBI project is intended to connect Nairobi to all the 47 counties and the entire country to high speed broadband internet, in order to enhance communication and sharing of information between the national and county governments, as well as creating job opportunities (Owili 2014).

The deployment of Infrastructure by many internet service providers in Kenya has resulted in increased competition, leading to a further reduction of tariffs as well as an increased usage of mobile phones and internet. Kenya is still considered to have one of the lowest costs for internet access in sub-Saharan Africa, thus resulting in a higher penetration of users (Schuman and Kende 2013: 16 &23). According to the Communications Authority of Kenya, by September 2013 there were an estimated 31.3 million mobile subscribers with a mobile penetration rate of 76.9 per cent nationally. The estimated number of internet users stood at 19.1 million with 47.1 per 100 inhabitants having access to internet services. The available international internet bandwidth was 60,900 megabits per second (Mbps) of which 41.8 per cent was being utilised (CAK 2014).

Recently, the Kenyan Government launched the National Broadband Strategy for the period 2013–2017, with the goal of providing quality services to all citizens. The Strategy aims to: increase the minimum broadband speeds from the current 256 Kilobits per second (Kbps) to 5 Mbps in rural areas and up to 40 Mbps in urban areas by 2017 and, increase broadband penetration in households from the current 6.3 per cent to 35 per cent. Additionally, the National Broadband Strategy seeks to further reduce the cost of broadband per Mbps in relation to the average national income from the current 30 per cent to 10 per cent as a means of promoting fast and affordable Internet connectivity to the Kenyan people (Kenya 2013).

4.3.2. Kenya’s E-Government System

In recent years the Kenyan government has continued to increase the efficiency of its electronic government services in relation to other international and African peer nations by seeking out opportunities to deliver more all-inclusive, citizen-focused, transparent, and automated public services (IDC 2014: 8).The goals and objectives of the e-Government

Strategy include: “delivery of government information and services to the citizens, promote productivity among public servants, encourage participation of citizens in government, and empower all Kenyans in line with development priorities outlined in the Economic Recovery Strategy for Wealth and Employment Creation” (KHRC 2014: 22).

Highlighting the benefits of having an e-government in place, President Kenyatta has made it a priority in his administration to have a fully functioning electronic system.

> *The benefits of doing so are significant: the employment opportunities created through IT-enabled services, e-services to Kenyans, deployment of e-agriculture, e-health, e-learning, e-policing, e-connectivity and e-commerce. And the combination of skilled professionals, a robust ICT infrastructure, coupled with affordable rates for connectivity, will turn Kenya to an exceptional destination for foreign investors in the sector* (Kenyatta 2014b).

The Kenyan government has introduced electronic systems in several state ministries and various state-owned institutions including: the legal information system, the national tax system, the integrated financial management system, the immigration information system, and the education system (Kenya 2014a: 28). “Most of these systems are found in the National Treasury, Kenya Revenue Authority (KRA), Home Affairs State Department and Immigration Office. In addition, information is manually exchanged by and between departments and institutions using fax, e-mail and electronic media. These systems provide partial electronic services to citizens and businesses through Government portals” (Kenya 2014a: 28). The Kenya Revenue Authority (KRA), for example, offers online services such as submission of tax returns and payments, and tax related information to citizens and businesses. For KRA, the internet is of considerable importance for the deployment of a national single window for trade facilitation, and integration of customs, port and transit processes, ultimately reducing costs for government and trading enterprises (KRA 2014).

The Kenyan Government has also developed a ‘Government Common Core Network’ (GCCN), which is meant to serve as “a shared and secure interoperable Government-wide ICT architecture” (Kenya 2014a: 26). The system is meant to “incorporate government work processes and information flows, improve the inter-ministerial sharing of databases and exchange of information in order to eliminate duplication and redundancies and, improve public access to government services and ensure responsiveness in reporting, monitoring and evaluation" (Kenya 2013). Bandwidth support to government departments and agencies has also been steadily growing (Kenya 2014a: 26). The Kenyan government also established the tier-2 Government Data Centre (GDC) infrastructure to ensure security of Government data and applications (Kenya 2014a: 26).

"All of Kenya's government entities will be able to offer multichannel choices of communication as well as deploy innovative tools and practices that make it easier for the public to engage with government and each other", and "citizens who access government information online through Web 2.0 technologies can now count on the e-government system to respond to requests with agility, accuracy, and consistency" (IDC 2014: 10).Consequently, each citizen will also be issued with a Public Key Infrastructure (PKI) that has a unique online identity and digital certificate, which will be required whenever Kenyans take part in online transactions as a way of safeguarding sensitive personal information (KHRC 2014: 45).

4.4. The Importance of Kenya's ICT Sector

Kenya's ICT sector is considered crucial to the development of its economy and everyday life. Evidence from developed and newly industrialised countries (NICs) suggests that ICTs are capable of facilitating poverty reduction and promoting development through creating employment, enhancing economic activities, facilitating reduction of production costs, improving quality of service delivery, and facilitating decentralisation of growth and development (Aligula and Etta: 2006: 1).

In a speech delivered by President Kenyatta, he emphasized the importance of Kenya's ICT sector:

> *We in Kenya now recognize ICT as a key driver of our economy. Indeed, this is why it is anchored in our national long-term development blue print, the Vision 2030, which aims to transform Kenya into a knowledge economy… Our Vision 2030 identifies the ICT sector and IT-enabled services as potential contributors to more than 10% of our national cake (GDP). With the developments we are witnessing in the ICT industry today, coupled with the determination of the industry players, I am confident that this target will be achieved by 2030, if not earlier… I am convinced that ICT will spur the efficiency and effectiveness we seek in delivering government service. My Government is making every effort to ensure that*

public services are delivered to every Kenyan securely and in real time. In this, your industry is our closest partner (Kenyatta 2014b).

ICT is considered to be one of the pillars for socio-economic development in the second Medium-term Plan of Kenya's economic development blueprint known as 'Kenya Vision 2030', with the theme 'strengthening the foundation for a knowledge economy' (Kenya 2014a: 20). ICT thus plays an essential role in realising Kenya's vision of "a knowledge based economy, which aims at shifting the current industrial development path towards sustainable innovation" (Kenya 2014a: 20). As a pillar of the second medium-term plan, ICT would deal with: "upgrading the national ICT infrastructure, improving public service delivery, developing the ICT industry, and upgrading ICT capacity" (Kenya 2014a: 20).

According to the ICT Master Plan Taskforce Report (Kenya 2014a: 63), six sectors have been prioritised in carrying out flagship projects for ICT-enabled industries in realising Kenya's Vision 2030. The sectors include: health, education, security, agriculture, financial services and, trade, transport and logistics.

- ***Health Sector**:* The Kenyan Government is developing "an integrated national health system that will integrate the various systems that are developed and implemented in the health sector, including the physician management system, drug supply chain system, and hospital management system" (Kenya 2014a: 64)). A central health data repository will be created and shared by all health institutions, as well as a health e-portal that will provide services and summary statistics to the relevant and authorised stakeholders (Kenya 2014a: 64).
- ***Education sector:*** Currently, there is a planned school laptop project aimed at providing free laptops for pupils beginning their first year of primary education. The current Jubilee Coalition Government elected into office in March 2013 is putting in place measures to implement its manifesto promise of providing solar powered laptop computers equipped with relevant content for every school-age child in Kenya (Jubilee Coalition 2012). In addition, funds will directed towards the development of digital content, building capacity of teachers and the setting up of computer laboratories in schools throughout the country(KHRC 2014: 23). Furthermore, the automation of academic and administrative processes at all levels of education is underway, in order to have all education information online. This includes an

education e-portal that will provide information and services to the public (Kenya 2014a: 64).

- ***Security sector:*** The Kenyan government intends to implement "an integrated security, intelligence and surveillance system" (Kenya 2014a: 65). Fundamental to this will be "a personal information data hub, a cross-agency database and master data platform, data warehouse, crime analytics, and profiling platform, as well as broadband connectivity in police stations. The system will provide law enforcement with real-time data on incidences and suspects" (Kenya 2014a: 65).On 25 November 2014, the Kenyan government signed a security surveillance contract with the country's largest mobile network Safaricom, estimated to be worth 14.9 billion shillings (approximately $165.2 million) (Kiplagat 2014). "Under the terms of the contract, Safaricom will install and run a communication and surveillance system that is linked to police stations to help combat crime, initially operating in Nairobi and Kenya's second-largest city, Mombasa" (Macharia and Potter 2014).
- ***Agricultural sector****:* "A National Agriculture Commodity Exchange will be implemented to facilitate commodities trading by providing reliable, timely and accurate marketing information and intelligence to farmers and other stakeholders via mobile phones and other end-user devices and enable farmers sell produce via the exchange" (Kenya 2014a: 65). Furthermore, "an electronic animal monitoring system that is able to track livestock ownership for security reasons and feeding practices will be implemented. This will provide end-to-end data of farm animal produce" (Kenya 2014a: 65).
- ***Financial services sector:*** "A national payment gateway project will be implemented in order to facilitate secure online payments by supporting multiple financial institutions to carry out electronic transactions and simplify the processing of payments" (Kenya 2014a: 66).
- ***Trade, transport and logistics****:* "A single window system is being created to facilitate cross border trade through the submission of regulatory documents (including custom declarations, applications for import/export permits, certificates of origin, trading invoices, etc.) on a single entry screen" (Kenya 2014a: 66). The Kenyan Government will also implement a national physical address system that "will provide street addressing, numbering and coding of all properties in order to facilitate logistics-

> based economic activities" and a "transport integrated management system (TIMS), which includes the automation of key processes in the transport industry, including driver testing, PSV/TLB licensing, traffic violations and prosecutions, motor vehicle inspection, etc." (Kenya 2014a: 66).

The above mentioned flagship projects highlight the government's commitment to improving Kenya's ICT infrastructure, service delivery and security sector as a way of achieving its 'Vision 2030' goal. However, if these new developments and systems are not properly secured, they may become potential targets for cyber attackers who may want to undermine Kenya's national security. In this regard, the more Kenya invests in its ICT critical infrastructure, the more vulnerable it becomes to cyber threats and attacks.

4.5. Cyber Security as an Emerging Threat to Kenya's National Security

As the number of internet users increases, the number of cyber-attacks has consequently increased over the same period. With more than 23 million internet users out of a population of around 44 million, Kenya is now ranked the fourth highest in Africa regarding cybercrime cases, slightly behind Algeria, Egypt and South Africa (Misiko 2014). This has been attributed to the increase of online activity which has attracted the attention of cyber criminals (Serianu 2014: 13). President Kenyatta has also raised concern of the growing cyber threats in a speech he made recently.

> *I am aware criminals have somewhat discovered the internet and other ICT systems as a tool to further their criminal activities. This has deterred many Kenyans from transacting online because they fear online identity theft or unauthorised access to personal data* (Kenyatta 2014b).

Cyber insecurity in Kenya is evolving rapidly and more organisations are becoming vulnerable to breaches and exploitation of their computer networks. The fast-growing cyber threat environment in Kenya is characterised by increasingly sophisticated hackers who are launching more frequent and targeted attacks (Serianu 2014: 12). According to a recent annual cyber security report from the Telecommunications Service Providers of Kenya, the number of cyber-attacks detected in Kenyan cyberspace grew by 108 per cent in 2013 to 5.4 million attacks, in comparison to 2.6 million cyber-attacks detected in 2012 (Serianu 2014: 11). During this period, the cyber-attacks detected had originated from both local and international cyber space. However, it is difficult to locate the exact origin of cyber-attacks because attackers use masquerading techniques and hidden servers to shield the identity of the computer system they are using to conduct cyber-attacks (Serianu 2014: 12).

A number of foreign cyber attackers compromise and take over government and corporate websites by carrying out distributed denial of service (DDoS) attacks (KHRC 2014: 33). Domestic cyber-attacks are also increasing as Kenyan hackers widen their scope on various cyber-attack techniques (Serianu 2014: 41). A survey conducted by Telecommunications Service Providers of Kenya revealed that the top attacking countries of Kenyan cyberspace networks and sources of malware were identified as China, United States, Korea, Brazil and South Africa, to name a few (Tespok Kenya 2013). It is important to note that these countries represent the origin of the individual attacker and not the actual government institutions.

While cases of cyber-attacks have been on the increase, government has been the victim, rather than the proponent of the attacks. In the past two years, hundreds of websites operated by Kenyan government ministries and state institutions have been hacked, cracked and defaced. However, the biggest cyber-attack occurred in January 2012 when103 websites were struck down overnight by an Indonesian hacker known as ‘Direxer’ (Misiko 2014). In August 2013, the website of the Department of Immigration and Registration of Persons suffered a similar fate (Daily Nation 2013). More concern rose over the security of government websites when, in March 2014, the Ministry of Transport website was hacked and defaced and anyone who accessed the site was welcomed by an image that read “All Muslims are together, the CYBER WAR will be appeared in all countries which are not respecting Islam” (Serianu 2014: 36).

On 21 July 2014, the Kenya Defence Forces’ Twitter account (@kdfinfo) was hacked into by a Latin-American based anonymous group that goes by the name of ‘Anon_oxo3’, who left a series of misleading and abusive tweets. This can pose a serious threat as the Kenya Defence Forces have been deployed in Somalia since 2011 to track down the Al-Shabaab Islamic extremists militants. Therefore, “any misleading information posted on KDF accounts might complicate issues for people who rely on these accounts for any official communication on the situation on the ground” (Mutegi 2014).

The examples of cyber-attacks on the Kenyan government illustrate how hackers can easily penetrate government websites with state secrets, classified security information and sensitive financial information for personal gain. Cyber security thus poses a significant threat to Kenya's national security especially when the government continues to invest large amounts of money on its digital infrastructure and ICT development nationwide. A look at the emerging cyber security threats facing Kenya will be discussed in the following section.

4.5.1. Current Cyber Security Threats facing Kenya

In the past few years there has been a substantial rise in cyber security incidents and cyber-criminal activity targeting both public and private organisations in Kenya. The fastest growing threats to Kenya's cyber security can be put into three main categories: malware attacks, social media attacks, and cyber fraud. These will be discussed briefly.

i. *Malware Attacks*

As mentioned in the previous chapter, malicious software also known as malware is any software that brings harm to a computer system and its user. The three biggest malware attacks emergent in Kenya's cyber environment include: DDoS attacks, Botnet attacks and mobile malware attacks.

- ***Distributed Denial of Service (DDoS) attacks:*** The continued growth of new online services launched by organisations in Kenya is increasing the country's vulnerability to Distributed Denial of Service attacks (Serianu 2014: 11). A number of attacks originate from compromised servers at hosting providers who are normally slow to respond to malware clean-up requests, as well as servers that are out of reach of international authorities(Serianu 2014: 11).With the introduction of a number of online enabled services by the government such as the Integrated Financial Management Information System(IFMIS), iTax system and the KenTrade single window system, both the public and private sector are highly susceptible to DDoS attacks (Serianu 2014: 11). For example, on 29th July 2013 between 7.10pm and 7.18pm there was a massive DDoS attack targeting one Kenyan ISP provider. The attack lasted for eight minutes with a peak data rate of 1629 mbps (Tespok Kenya 2013: 10). The attack caused a major slowdown of internet speeds by overloading the

ISP servers with too much traffic, preventing its customers from accessing the internet.

- ***Botnet attacks:*** According to Serianu (2014: 12), due to the increasing number of broadband and high speed internet connections, the number of botnet attacks in Kenyan cyberspace continues to grow. "In 2013, the number of botnet activity detected, increased by 100 per cent from 900,000 events for the period ending December 2012 to 1,800,000 events for 2013" (Serianu2014: 12). The growth of internet connectivity is exposing new unprotected computers and routers to the internet, thus greatly increasing the number of computers capable of being compromised by cybercriminals. "Once these devices are compromised, they can be used to spread viruses, generate spam, and commit other types of online crime and fraud. The attackers then utilize this highly distributed network to attack targeted infrastructure such as financial institutions and government ministries in attempts to defraud, cripple or steal information" (Serianu 2014: 12).
- ***Mobile malware attacks****:* According to Mcafee (2014), "mobile malware will be the driver of growth in both technical innovation and the volume of attacks in the overall malware 'market' in 2015. In 2013 the rate of growth in the appearance of new mobile malware, which almost exclusively targeted the Android platform, was far greater than the growth rate of new malware targeting PCs" (Mcafee 2014). Where Kenya is concerned, mobile malware poses a significant threat as more than half of the population use mobile phones. It is estimated that 99 per cent of internet traffic in Kenya is accessed through mobile phones as it is considered to be the cheapest way of accessing the internet for most Kenyans. In a recent survey conducted by Kaspersky Lab and INTERPOL, Kenya now ranks third in mobile malware attacks behind Nigeria and South Africa, with Android-based mobile smartphones being the biggest victims. The survey also claims that one out of five Android users is susceptible to cyber-attacks (Matinde 2014).

ii. *<u>Social Media Attacks</u>*

Social media websites are considered to be a popular platform which many Kenyan individuals and organisations use to build new relationships and networks. However, the use of social media websites by certain individuals in carrying out various cybercrimes is on the rise in Kenya (Serianu 2014: 11). The majority of social media attack cases identified in

Kenya was largely related to posting of defamatory hate speech, cyber-bullying, and terrorists' use of social media (Serianu 2014: 11).

- ***Hate speech:*** According to the National Integration Cohesion Commission (NCIC) Act of 2008, "hate speech includes using threatening, abusive and insulting words, behaviour, displays or written material, publishing or distributing such written material, distributing, showing a play or recording of visual images or producing or directing a programme which is threatening abusive or insulting that intended to stir up ethnic hatred" (NCIC 2014). The continued use of social media for hate speech in Kenya continues to grow at an alarming rate and appears to be based strictly on ethnicity.
- ***Cyber bullying:*** Cyber-bullying refers to the use of electronic communication and social media to bully a person online by sending threatening and intimidating messages, or even embarrassing pictures or videos (NSPCC 2014). Cyber-bullying in Kenya is a growing problem to which more and more individuals are becoming victims on social media. 2013 saw an increase in cyber bullying incidents such as: the use text messages or emails, malicious rumours spread via email or posted on social networking sites, as well as sharing embarrassing pictures or videos (Serianu 2014: 37).
- ***Terrorism and social media:*** Terrorists have now taken full advantage of social media with regard to achieving their strategic interests. On December 7, 2011, the terrorist organisation 'Al-Shabaab' allegedly began using the social media network 'Twitter' as a way of countering Kenya's military spokesman, who was updating journalists and the public through Twitter after the Kenyan Defence Forces (KDF) incursion into Somalia (Serianu 2014: 37). At present, Al Shabaab's Twitter handle 'HSMPress', has attracted more than 8000 followers (Serianu 2014: 37). Social media platforms like Twitter have given al-Shabaab an "effective tool to spread its propaganda and empowered internal factions, giving them a powerful voice of dissent that Somali citizens, group members and the world at large could easily reach and hear" (Serianu 2014: 37). During the deadly attack on the Westgate Mall on September 21 2013, Al-Shabaab was able to live-tweet the attack, "a move that revealed how social media can be used by criminals to spread propaganda" (Serianu 2014: 37). Currently, the militant group uses social media to recruit young radical

fighters as well as claim responsibility for terror attacks on innocent civilians carried out in the region (Otieno 2014).

iii. *Cyber Fraud*

Cyber fraud is regarded as the largest contributor to cybercrime in Kenya and the government considers financial fraud among the top cyber security threats (Serianu 2014: 40). However, online and mobile banking is the biggest form of cyber fraud in Kenya and this is attributed to the country's extensive use of innovative mobile money services (Wanjiku 2014). It comes as no surprise when more than $1.7 trillion passed through Kenyan mobile phones in 2013 alone (Caulderwood 2014).

In the private sector, financial institutions have been adversely affected by cybercrimes. According to the Banking Fraud Investigations Department (BFID), approximately $17.52 million was stolen from customers' bank accounts between April 2012 and April 2013, with only a mere $6.2 million being recovered (Kimani 2013). The BFID report cites identity theft, electronic funds transfer, bad cheques, credit card fraud, loan fraud, forgery of documents and online fraud as the key methods used to defraud these institutions (KHRC 2014: 33).

The growing innovation in online and mobile banking services has exposed customers as well as local financial institutions to new vulnerabilities thanks to the many financial institutions creating vulnerable web and mobile applications, a majority of which do not have a strong security control. Online and mobile banking attacks are based on misleading the user and stealing login data by using tools such as malware and Trojan horses (Serianu 2014: 12). Moreover, the growth of mobile money technology in the region has attracted criminals to the lucrative money transfer platform, and fraudsters are getting creative each day in finding loopholes in new security controls implemented by financial institutions, organisations and individuals (Serianu 2014: 12).

4.6. Conclusion

This chapter sought to analyse how the growing use and dependence on ICT systems and networks has exposed Kenya to harmful cyber-attacks that may pose a potential threat to its national security. As Kenya moves forward in realising its 'Vision 2030', a better understanding of Kenya's cyber security threats and vulnerabilities is needed at all levels including all government departments, internet service providers, public and private organisations, and the individual. Currently, the three main cyber threats that Kenya is facing include: malware attacks, social-media attacks, and cyber fraud. With internet access growing at a rapid rate in Kenya, these attacks will only continue to grow in magnitude. It is therefore crucial that more awareness and education is given to the public on how to secure themselves online. Additionally, public and private organisations must adapt better security practises in the workplace to be able to respond to cyber threats quickly.

The following chapter will conclude the study by explaining Kenya's response to cyber security threats in relation to the legal policy and regulatory framework it has adopted in protecting Kenya's cyber security. A summary and conclusion of the study will also be provided.

CHAPTER 5: KENYA'S RESPONSE TO CYBER SECURITY THREATS

5.1. Introduction

In light of the growing threat of cyber-attacks in Kenya as described in chapter 4, the government has taken action through its institutional and regulatory frameworks within the ICT sector. In a recent speech made by President Kenyatta, he emphasised the urgency of the issue.

> *I would like to assure Kenyans that my government is working round the clock through various agencies to identify mechanisms that will strengthen national security, and cut crime. I have recently established a Technology-Enabled Transformation of the Public Sector: an initiative that will help us realise a digital registry eco-system, better intelligence for national security, and a more service-oriented culture in government* (Kenyatta 2014a).

This chapter will focus on Kenya's response to the emerging cyber security threats it faces by analysing its national security policies and legal framework adopted by the Kenyan government through its constitution, national cyber security strategy and master plan. A brief overview of existing ICT legislation will be given to provide the context for cyber security. Some recommendations will be given on how Kenya can uphold its cyber security.

5.2. Kenya's National Security Framework

Chapter fourteen of the Kenyan Constitution defines national security as "the protection against internal and external threats to Kenya's territorial integrity and sovereignty, its people, their rights, freedoms, property, peace, stability and prosperity, and other national interests" (Kenya 2010: 144). From this statement, it is evident that Kenya's constitution recognises both human security and state security in its definition of national security, thus embracing both traditional and modern conceptions of national security. With regard to national interest, Kenya's vital national interests are like those of several other countries and they include "the preservation of territorial integrity, establishing peace and security and law and order, consolidating the development of the country's new political system as well as guaranteeing national development" (Kenya 2010: 144).

The national security organs in Kenya comprise the Kenya Defence Forces (consisting of the Kenya Army, the Kenya Air Force and the Kenya Navy), the National Intelligence Service, and the National Police Service (Kenya 2010: 144). The primary objective of these organs is to promote and assure national security in accordance with the principles mentioned in Article 238 (2) of the Kenya Constitution (2010). In this regard, there are four principles outlined in Article 238 (2) that guide Kenya's national security. Firstly, national security is subject to the authority of the constitution as well as Parliament. Secondly, the pursuit of national security will comply with and respect the rule of law, democracy, human rights and fundamental freedoms. Thirdly, national security organs must respect the diverse cultures of the Kenyan people while performing their duties and exercising their powers. Lastly, national organs must reflect a fair and equitable representation of the Kenyan people while recruiting personnel (Kenya 2010: 145).

In addition to the national security organs, Kenya has an established National Security Council (NSC) which exercises supervisory control over all the national security organs, as well as performing other obligations prescribed under national legislation (Kenya 2010: 145). The National Security Council consists of: the President, Deputy President, Cabinet Secretaries responsible for defence, foreign affairs and internal security, the Attorney-General, Chief of the Kenya Defence Forces, Director-General of the National Intelligence Service and the Inspector-General of the National Police Service (Kenya 2010: 145). Other functions of the National Security Council include: incorporating the domestic, foreign and military policies relating to national security in order enable the national security organs to function effectively and allow stronger cooperation among them and evaluating and assessing the objectives, commitments and security threats to Kenya in respect of its actual and potential national security capabilities (Kenya 2010: 144). Moreover, with approval from parliament, the National Security Council has the power to deploy the Kenya Defence Forces outside Kenya for regional, international, or other peace support operations (Kenya 2010: 144).

According to Kenya's National Security Intelligence Service Act (No. 11 of 1998), a threat to the national security of Kenya is characterised by: firstly, "any activity relating to espionage, sabotage, terrorism or subversion or intention of any such activity directed against, or detrimental to the interests of Kenya and includes any other activity performed in conjunction with any activity relating to espionage, sabotage, terrorism or subversion, but does not include any lawful advocacy, protest or dissent not performed in conjunction with any such activity” (Kenya 2012: 6); secondly, “any activity directed at undermining, or directed at or intended to bring about the destruction or overthrow of, the constitutionally established system of the Government by unlawful means” (Kenya 2012: 6); thirdly, “any act or threat of violence or unlawful harm that is directed at or intended to achieve, bring about or promote any constitutional, political, industrial, social or economic objective or change in Kenya and includes any conspiracy, incitement or attempt to commit any such act or threat” (Kenya 2012: 6); and lastly, “any foreign-influenced activity within or related to Kenya that is detrimental to the interests of Kenya, and is clandestine or deceptive or involves any threat whatsoever to the State or its citizens or any other person lawfully resident in Kenya” (Kenya 2012: 6).

5.2.1. Institutions in Support of Cyber Security in Kenya

The liberalisation of the telecommunications market has been a key facilitator in the improvement and development of ICTs as it introduced competition in the information and communications sector. “In 1999, there were approximately 15,000 mobile subscribers throughout the country before the first two mobile licenses were issued” (IDC 2014: 3). The number of mobile subscriptions is currently estimated to be at 32.8 million as of September 2014, which translates to a mobile penetration level of 80.5 per cent nationally (CAK 2015). The liberalisation was triggered by the splitting up of the Kenya Post and Telecommunications Corporation in 1999, which resulted in the creation of five separate bodies that include: “the Postal Corporation of Kenya, Telkom Kenya Ltd (later privatised), The Communications Commission of Kenya (CCK) the industry regulator, The National Communications Secretariat (NCS) to advise on policy issues and, an Appeals Tribunal for arbitrating in cases where disputes arise between parties” (Kenya 2014a: 22).

“ICT matters in Kenya fall under several pieces of legislation, including the Kenya Communications Act (KCA) of 1998, Science and Technology Act (Cap. 250) of 1977, and Kenya Broadcasting Corporation (KBC) Act of 1988” (Kenya 2014a: 22). Recently, the “Kenya Communication Act 1998 was amended to the Kenya Information and Communications (Amendment) Act, 2013 (no. 41A)” (Kenya 2014a: 22). Today, Kenya’s cyber security regulatory issues fall under the Ministry of ICT, the Communication Authority of Kenya (CAK), (formally known as the Communication Commission of Kenya (CCK)), as well as the Kenya ICT Authority (Kenya 2014a: 22).

i. *Ministry of Information, Communications and Technology (ICT)*

Kenya's Ministry of ICT is in charge of all matters related to information, communication and technology. The ministry together with the Communication Authority of Kenya (CAK) are the bodies that take part in internet policy consultations. They are the formulators and implementers of government policies that have to do with ICT including the internet (Kenya 2014a: 23).

The Ministry is charged with the formulation and implementation of ICT policy with some of its priorities being: ensuring a knowledge-based society, developing an enabling framework that will foster ICT's contribution to the fulfilment of Vision 2030, establishing a culture of cyber security, including consumer protection, and strengthening the country's capacity to meet technological challenges (Kenya 2014a: 23).

ii. *Communications Authority of Kenya*

The Communications Authority of Kenya (CAK), formerly known as the Communication Commission of Kenya (CCK), is the regulatory authority for communications and is charged with the responsibility of technical areas of the internet such as in the deployment of the infrastructure necessary for the internet, broadband, regulation of internet service providers, mobile termination rates, regulating competition in the telecoms market, and protection of consumer rights (CCK 2013).

It is tasked with the regulation of the national success of the internet. This role is entrenched in the Kenya Communications (Amendment) Act of 2009, and is based on the recognition of the rapid changes and developments in technology that have distorted the traditional distinctions between telecommunications, Information Technology (IT) and broadcasting (CCK 2013). This statute therefore enhanced the regulatory scope and jurisdiction of CAK, and effectively transformed it to a converged regulator (KHRC 2014: 41).

The Ministry of ICT in conjunction with the CAK have embraced a multi-stakeholder approach to the policy-making processes. They have also held consultations with relevant stakeholders in formulating various guidelines, sector regulations and legislation (including the national broadband strategy, the universal service policy, and the cyber security master plan) (KHRC 2014: 42). Examples of key stakeholders include internet and mobile service providers in the private sector.

Additionally, the Ministry of ICT and the CAK participate in international internet policy dialogues on behalf of the government. For example, they are the main points of interaction for Kenya with the International Telecommunications Union (ITU) and its activities. In addition, CAK represents Kenya at the Internet Governance Forum (IGF) and the Government's advisory committee (GAC) of ICANN. In other words, the most important governmental authority in ICT issues resides with CAK which has the powers to influence the direction of policy (KHRC 2014: 41).

iii. The Kenya Information Communication Technology Authority (ICTA)

The ICT Authority is a State Corporation under the Ministry of Information, Communication and Technology (ICT) and was formed in August 2013 after absorbing the assets of three former bodies: the Directorate of e-Government, the Government Information Technology Services (GITs) and the Kenya ICT Board (Kenya 2014b). "The Authority has a broad mandate to foster the development of ICTs in Kenya (including businesses, innovation and capacity building), implement and maintain systems and technology for the Government, overseeing the development of integrated information and communication technology (ICT) projects, and to develop and enforce ICT standards for the Government" (Kenya 2014b).The ICT authority has also been tasked with improving the management of the government electronic communication under the national message 'One Government, One Voice' (Kenya 2014b).

The Ministry of ICT has proven to be efficient in streamlining Kenya's ICT sector by merging the government bodies responsible for ICT as a way of improving service delivery and minimising the waste of resources. With ICT as a key pillar of Kenya's Vision 2030, the above mentioned institutions will continue to play an important role in dealing with emerging cyber threats. However, the successful implementation of Kenya's cyber security framework and strategy will determine the efficacy of these institutions.

5.2.2. Kenya's National Cyber Security Framework

The Kenyan government has prioritised the securing of its critical ICT infrastructure in order to facilitate the economic growth for the country and its citizens (Kenya 2014c: 5). However, due to the rapid sophistication and growth of cyber-attacks, keeping up with current trends in cyber defence is a growing problem for the Kenyan government.

The Kenyan Government has taken measures to improve cyber security "including the Kenya Information and Communications ACT, CAP 411A as amended by the Kenya Information and Communication (Amendment) ACT, 2014 , the formation of the National Kenya Computer Incident Response Team Coordination Centre (KE-CIRT/CC), and the establishment of the National Certification Authority Framework, which provides a foundation for public key infrastructure implementation and partnership with regional and international cyber security bodies and forums including the International Telecommunications Union (ITU) and the East Africa Communications Organisation (EACO)" (Kenya 2014c: 8).

Kenya's cyber security policy is currently steered by the ICT Authority through the National Cyber Security Master Plan (NCSMP). This is considered to be the "first step towards building a cyber-security framework to suit Kenya's unique cyber threats. The key components the policy addresses are: Training & Awareness, Economic Impact, Governance, Policy and Legal framework" (Serianu 2014: 40).The Kenyan government has received assistance from foreign nations including the U.S, South Korea and Israel on various areas regarding cyber security policy formulation (Serianu 2014: 40).

"The cyber security management framework incorporates the Kenya Information and Communications Technology Sector Policy of 2006, the Kenya Information and Communications Act of 1998, the Kenya Information and Communications (Electronic Certification and Domain Name Administration) Regulations of 2010" (KICR 2010), as well as "the relevant provisions of international cybercrime conventions –including the proposed draft African Union Convention on Cybercrime, among other legal instruments" (Nyange 2014: 7).

Kenya's National Cyber Security Framework (NCSF) is intended to enhance the security of Kenya's critical ICT infrastructure as well as create confidence in the use and adoption of ICTs in Kenya (Kenya 2014c: 8). "The NCSF consists of the following: the National Cyber-security Strategy (NCS), the National Public Key Infrastructure (NPKI) and its licensing regime, the Electronic Certifications Service Provider (E-CSP) and the National Kenya

Computer Incident Response Team Coordination centre (KE-CIRT/CC)" (Kenya 2014c: 8). The current NCSF was launched on 24 June 2014 at the Communications Authority of Kenya (CAK) grounds, Nairobi. The objective of the launch was to "formally present the reviewed NCSF to the public in order to create awareness of the Government's efforts towards the management of cybercrime" (Nyange 2014: 10).

Kenya's cyber security framework illustrates the government's commitment to securing its critical ICT infrastructure from cyber threats. However, its success will depend on the cooperation of individuals, as well as the involvement of the public and private sector in raising cyber security awareness. Kenya's cyber security framework will only be effective if the human component is trained and educated accordingly on the cyber threat landscape.

5.2.3. Kenya's National Cyber Security Strategy

It is important to note that Kenya still has a relatively immature cyber security posture where the growing complexity and sophistication of cyber threats is concerned (Kenya 2014c: 8). However, the Kenyan government has committed itself to maturing its cyber security posture by "providing a strategic cyber security direction, with accompanying implementation actions to secure the nation's critical cyber infrastructure against existing and emerging threats" (Kenya 2014c: 8).

The Kenyan government identified several key challenges emanating directly from emerging risk areas inside Kenya, the East African Community (EAC), and internationally. By addressing these risks and understanding the impact of Kenya's cyber security efforts, technology growth and economic development will be significantly enabled by cyber security implementation (Kenya 2014c: 7).

As part of their acknowledgement of the importance of the ICT sector to the Kenyan economy, the Kenyan government has developed a National Cyber Security Strategy (2014). In conjunction with the Kenya National Cyber Security Master Plan (2012), the government seeks to address emerging cyber security threats and challenges that Kenya's ICT environment may face in the future. The National Cyber Security Strategy complements the three pillars of Kenya's Vision 2030 as well as the National ICT Master Plan (Kenya 2014c: 7).

The purpose of the National Cyber Security Strategy “is to clearly define Kenya’s cyber security vision, goals, and objectives to secure the nation’s cyberspace, while continuing to promote the use of ICT to enable Kenya’s economic growth” (Kenya 2014c: 7).

To promote the Kenyan government’s commitment to cyber security, the Strategy includes four strategic goals. The first goal deals with “enhancing the nation’s cyber security posture”, with an objective of protecting critical ICT infrastructure (Kenya 2014c: 11). The Kenyan government has acknowledged that threat actors can exploit ICT vulnerabilities to perpetrate crimes against the government and the public who rely extensively on ICT to perform electronic transactions or obtain vital government services (Kenya 2014c: 11). The Kenyan government is taking steps to increase the security and resilience of its critical information infrastructure through a coordinated effort with other countries and relevant stakeholders to increase the security of global cyberspace by building cyber security capabilities focused on operations, infrastructure and mission assurance (Kenya 2014c: 11).

The second goal of the strategy looks to build national capability with two objectives. The first objective deals with “awareness and training to inform and educate the Kenyan public and workforce to secure the national cyberspace” (Kenya 2014c: 11). The government is partnering with other government organisations, the private sector and academia to ensure that people with cyber security responsibilities possess the appropriate level of cyber qualifications and competencies (Kenya 2014c: 11). The Kenyan government is also working with academia to develop cyber security curriculums for higher education and specialized training programs to ensure competency building for cyber security professionals (Kenya 2014c: 11).

The second objective deals with “communications and outreach in order to elevate cyber security awareness for government, private sector, and the Kenyan public” (Kenya 2014c: 12). Through targeted communications and outreach activities, the Kenyan government is promoting the understanding of cyber threats and empowering the Kenyan public to adopt safe and secure online practices, as well as communicating approaches and strategies for the public to keep themselves and their families and communities safer online (Kenya 2014c: 12).

The third goal of the strategy seeks to "foster information sharing and collaboration" with an objective of developing "a comprehensive governance framework to leverage resources, reduce conflict and duplication of effort, and work toward Kenya's long-term cyber security goals" (Kenya 2014c: 12). The Kenyan government acknowledges that implementing the strategy requires the development of a comprehensive governance model that includes meaningful participation by relevant stakeholders, working together toward the common goal of securing Kenya's cyberspace (Kenya 2014c: 12).

"Through this governance framework, the Government of Kenya intends to: develop the required laws, regulations and policies required to secure the nation's cyberspace, solicit stakeholder input and feedback, as appropriate, and balance information security, privacy considerations and economic priorities" (Kenya 2014c: 12). Successful implementation will require the sharing of cyber security information across all government departments and sectors in a trusted and structured manner and the Kenyan government intends to develop and manage a secure information-sharing capability to promote knowledge and lessons learned among relevant stakeholders (Kenya 2014c: 12).

The fourth goal of the Strategy is to "provide national leadership" with an objective of developing and coordinating the implementation of the National Cyber Security Strategy and Master Plan (Kenya 2014c: 12). The government has committed itself to providing a single unified agenda that will guide all relevant stakeholders. The Ministry of ICT has been given the mandate to frequently revise the Strategy's vision, goals and objectives as well as to establish a tactical roadmap for achieving national cyber security objectives (Kenya 2014c: 12). The Ministry of ICT will also use the Strategy and complementary Master Plan to identify and implement relevant cyber security initiatives, in collaboration with the relevant stake holders (Kenya 2014c: 12).

Kenya's Ministry of ICT has been given the mandate of "leading the process of developing the National Cyber Security strategy and has since invited stakeholders and all Kenyans in general to contribute in the review of the draft strategy" (Kenta 2014c:11). Kenya's Ministry of ICT has been given the mandate of "leading the process of developing the National Cyber Security Strategy and has since invited stakeholders and all Kenyans in general to contribute in the review of the draft strategy" (Kenya 2014c: 11). The strategy "defines Kenya's cyber security vision as an on-going commitment to support national priorities by encouraging ICT growth and aggressively protecting critical information infrastructure" (Kenya 2014c: 11).

The NCS covers "the Kenyan government's regulatory, policy and legal framework; cyber security governance maturity analysis; NCS goals; Development impact and key benefits" (Kenya 2014c: 11).

The Kenyan Government's Regulatory, Policy, and Legal Framework essential inputs include: "Analysing Kenya's Government baseline cyber security governance model: Evaluating the Government's cyber security maturity; Highlighting national cyber security master plan considerations from other nations; and, Providing recommendations for a Government Regulatory, Policy, and Legal Framework that; Identifies the needed laws, regulations and policies; Define governance roles and responsibilities; Prescribe measures to secure critical cyber infrastructure in the public and private sectors; Involve the private sector in policy development; Facilitate international cooperation; Define and protect against cybercrime; Balance information security and privacy considerations; and, Promote secure online transactions through trusted identities"(Kenya 2014c: 12).

The NCS proposes the governance of cyber security as follows:

- ***The National Security Advisory Council (NSAC);***

This is the general advisory committee led by the Head of Public Service and draws its membership from different Kenyan Government ministries and agencies whose roles relate to national security and reports to the National Security Council (NSC), which is led by the President of the Republic of Kenya (Kenya 2014d).

- ***The National Cyber Security Committee (NCSC);***

"The NCSC provides policy oversight and advice on cyber security issues. The NCSC reports to the NSAC and it consists of the principal cabinet secretaries and directors of relevant government ministries, agencies and parastatals. The NCSC is chaired by the permanent secretary of the Ministry of ICT" (Kenya 2014d).

- ***The National Kenya Computer Incident Response Team- Coordination Centre KE-CIRT/CC Cyber security Committee (NKCC);***

"The National KE-CIRT/CC (NKCC) was established in October 2012 with the assistance of the International Telecommunication Union (ITU) through the International Multilateral Partnership against Cyber Threats (IMPACT) program" (KE-CIRT 2014). "The NKCC's main purpose is to participate in the implementation of the National KE-CIRT/CC and facilitate coordination and collaboration in the response to cyber security incidents, among other cyber-crime management activities" (Kenya 2014c: 14). The NKCC reports to the NCSC and is "chaired by CAK and draws its membership from the Ministry of ICT, ICTA, law enforcement, the Directorate of Public Prosecutions (DPP), public utility service providers, internet Service Providers (ISPs), telecommunication operators, academia, the banking/financial sector, among others" (Kenya 2014c: 14).

- ***Kenya Computer Incident Response team- Coordination Centre (KE-CIRT/CC)***

The Kenya Computer Response Team- Coordination Centre (KE-CIRT/CC) derives its mandate from the Kenya Information and Communications Act CAP 411A which directed the CAK to develop a national cyber security management framework through the establishment of a national Computer Incident Response Team (CIRT) (CCK 2013). In addition, KE-CIRT is receives financial support from the CAK and the ITU for capacity-building (KHRC 2014: 43).KE-CIRT brings together government agencies, the Central Bank and internet expertise drawn from the Kenya Network Information Centre (KENIC), the Telecommunication Service Providers Association of Kenya (TESPOK) and the Kenya Education Network (KENET) to address cyber-attacks as and when they occur (KE-CIRT 2014).

KE-CIRT/CC is Kenya's national cyber security "trusted point of contact and is mandated with offering advice on cyber security matters nationally and coordinating responses to cyber incidents in collaboration with relevant stakeholders locally, regionally and globally" (KE-CIRT 2014). "The functions of KE-CIRT/CC include: offering advisories on cyber security matters and coordinating cyber incidents responses, in collaboration with relevant actors locally, regionally and internationally; acting as the national trusted point of contact for information security matters; gathering and disseminating technical information on computer security incidents; carrying out research and analysis on computer security; capacity building in information security in creating and maintaining awareness on cyber security related activities" (KE-CIRT 2014).

Kenya's cyber security framework and strategy is intended to provide a backbone for cyber security efforts and initiatives in Kenya, as well as play a critical role in shaping cyber security in the country (Serianu 2014: 42). Kenya's National Cyber Security Strategy and Master Plan will assist in drafting cyber security legislation that will help manage and protect individuals and organisations in cyberspace. In addition, Kenya's National Cyber Security Strategy and Master Plan seeks to address the wide range of cyber security threats posed by the expansive and dynamic nature of ICT. It is therefore imperative for the Kenyan government to speed up the implementation process of its cyber security frameworks and strategies it has formulated, to prevent a catastrophic cyber-attack which may potentially threaten Kenya's national security. However, successful implementation will require more public awareness and the full cooperation of the public and private sector when dealing with cyber security issues in Kenya. This will determine Kenya's resilience in building a strong cyber security posture.

5.3. Summary of the Study

The main objective of this study was to explore current trends and emerging challenges within the cyber security environment that may pose a significant threat to Kenya's national security. To achieve this, the study analysed the traditional and modern conceptions of national security; described the evolution of cyber security; and assessed the state of cyber security as an emerging threat to Kenya's national security.

Chapter 2 of the study presented a conceptual overview of national security by tracing how the concept evolved from a traditional realist state-centric approach to security, to a more broadened and deepened approach that considered non-military and individual threats. In addition, the concepts of national security, national interest, the revolution in military affairs (RMA), securitisation theory, and human security were discussed in order to explain the meaning and understanding of security in the 21st century. The chapter also gave a historical overview of Kenya's national security and the important role it plays in East African regional security in order to determine the key actors and policies responsible for national security. Terrorism in Kenya was addressed as it currently poses the biggest external threat to Kenya's national security in terms of physical loss and damage. The study also revealed that terror and traditional security overlap with regards to cyber security and the broadened view of national security. This was essential in contextualising cyber security within the discourse of national security, as cyber threats and attacks are transnational in nature and affect both the individual and nation-states.

Chapter 3 of the study provided a conceptual overview of cyber security, with the aim of tracing the evolution of cyberspace through the development of the personal computer and the internet. The manifestations of cyber insecurity were also explored in order to analyse the threats posed by cyber-attacks, as well as their evolution and sophistication over time. The analysis revealed that cyber-attacks today are increasingly becoming more advanced and dangerous, with the capability of causing serious damage to a country's critical information infrastructure. In addition, cyberspace has opened up new vulnerabilities for nation-states as non-state actors are becoming increasingly powerful in cyberspace. Moreover, the absence of a single sovereign authority in cyberspace has created an enabling environment for the development of cyber weapons by both state and non-state actors. With the on-going trends occurring in cyber security, the future of cyberspace will have an even greater impact on national security.

Chapter 4 presented a case study analysis of Kenya's cyber security environment. The chapter then addressed Kenya's cyber security as an emerging threat to national security. An overview of Kenya's ICT environment was provided to establish how the growing use and dependence on ICT systems in Kenya may be a potential threat to its national security. The chapter revealed that Kenya is a victim of numerous cyber-attacks targeting individuals as well as private and public organisations. With the growing sophistication of cyber-attacks and the increase of ICT usage in Kenya, cyber security is of real importance to Kenya, especially in light of the rising number of terror attacks in the country.

Chapter 5 discussed Kenya's cyber security legal policy framework and strategy, to determine whether the government is taking sufficient action in addressing the emerging cyber security threats and challenges that Kenya is vulnerable to. In this regard, Kenya acknowledges its vulnerability in cyberspace and has devised a National Cyber Security Strategy and Master Plan that seeks to address the wide range of cyber security threats posed by the expansive and dynamic nature of ICT. However, the implementation process will determine Kenya's resilience in building a strong cyber security posture.

5.4. Conclusion and Recommendations

Cyber security is a complex issue and is of real importance to Kenya with regard to its biggest physical threat, terrorism. Al Shabaab and other transnational terrorist organisations are increasingly using social media in furthering their strategic interests by spreading propaganda, recruiting members, and obtaining funding. It is therefore only a matter of time before terrorist organisations adapt sophisticated cyber offensive capabilities, with the potential of causing significant damage to any target.

Based on the findings of this study, the best way forward for the Kenyan government would be to securitise cyber security in the country as a way of prioritising the issue for individuals and organisations in the private sector. On paper, Kenya's National Cyber Security Strategy is a well-thought out and well-written document, but in practice more needs to be done for the implementation process to succeed. For the Strategy to be fully effective, cyber security can be declared an existential threat to Kenya's national security by senior government officials in order to gain the required acceptance from the Kenyan people.

Additionally, the Kenyan government should prioritise and invest in cyber offensive capabilities as a way of enhancing its cyber security posture. Cyber power can be a very useful strategic tool for the Kenyan government in achieving its national interests. For example, Kenya's national security institutions can improve their efficiency when pursuing various strategic objectives by setting up a cyber-military command centre capable of coordinating various cyber-attacks on specific targets that pose a significant threat to Kenya's national security. However, such an undertaking would require sufficient funding and training of highly skilled computer experts and hackers who would eventually form part of Kenya's 'cyber army'. By utilising cyber offensive capabilities, Kenya will be able to develop a strong cyber security posture in relation to other nation-states globally.

Lastly, the Kenyan government through its legislative branch should advocate for a constitutional amendment that will incorporate cyber security laws in the Kenyan constitution. On the other hand, a separate cyber security law based on the existing constitution can be formulated. This will ensure that any forms of cyber insecurity are dealt with accordingly. Furthermore, by having a cyber-security law, law enforcement agencies will have the necessary powers to effectively pursue and prosecute cyber criminals. This will also improve the accountability of those responsible for protecting Kenya's cyber security. However, it is crucial for the government to achieve this without infringing on the individual human rights of citizens in regard to violation of privacy and freedom of expression in cyberspace.

In conclusion, the study finds that cyber security is a real threat to the national security interests of Kenya as it seeks to enhance its ICT capabilities and critical infrastructure. In this regard, the threat of cyber-attacks will continue to grow in terms of scale and sophistication. It is therefore essential for the Kenyan government to securitise the issue of cyber security in order to direct more attention and funding to address the growing threat of cyber insecurity in the country. However, the securitisation process must be done carefully so as to avoid the obstruction of accountable democratic governance by the state.

5.5. Recommendations for further research

Beyond the analysis given, some issues were not addressed in the course of the research due to time constraints as well as the analytical scope available for a mini-dissertation. Some of the issues include;

- Firstly, considering that majority of developed states are developing defensive and offensive cyber power capabilities, could cyber security represent a new strategic political tool that can be used to achieve specific national security interests?
- Secondly, as some states already possess powerful cyber weapons (such as Stuxnet), could cyber security represent a new dimension in the revolution of military affairs?
- Thirdly, the growing importance of cyber insecurity requires governments to actively engage in improving cyber security. However, the challenge is that improving cyber security requires more government monitoring and surveillance by state security organs. In this regard, to what extent does improving cyber security encroach on the privacy and freedoms of individuals online? Can we have both cybersecurity and the protection of individual rights and freedoms in cyberspace?

6. BIBLIOGRAPHY

Abrahamsen, R. 2005. ‘Blair’s Africa: The Politics of Securitisation and Fear.’ *Alternatives: Global, Local, Political*, 30: 55-80

Adan, H. H. 2005.*Combating Transnational Terrorism in Kenya*. Faculty of the U.S. Army Command and General Staff College. Internet: http://www.dtic.mil/get-tr-doc/pdf?AD=ADA436675 Accessed: 28 October 2014

Al Jazeera. *2014. Kenya Police Find Explosives in Mosque Raids.* 20 November. Internet: http://www.aljazeera.com/news/africa/2014/11/kenya-police-find-explosives-mosque-raids-2014112095511530664.html Accessed 22 November 2014.

Aligula, E. and Florence, E. E. 2006.*“Making Sense of Information and Communication Technology Investments” in Mainstreaming ICT: Research Perspectives from Kenya*. Outa, Etta and Aligulaeds, Nairobi.

Andress, J. and Winterfeld, S. 2011.*Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners*. Syngress: Elsevier Science.

Apps, P. 2014. *DDoS Cyber-attacks get bigger, smarter, more damaging*. Wednesday March 5, 2014. Reuters. Internet: http://www.reuters.com/article/2014/03/05/us-cyber-ddos-idUSBREA240XZ20140305 Accessed: 20 September 2014.

Aronson, S. 2013. ‘Kenya and the Global War on Terror: Neglecting History and Geopolitics in Approaches to Counterterrorism’. *African Journal of Criminology and Justice Studies*. Volume 7. Internet: http://www.umes.edu/cms300uploadedfiles/ajcjs/volume_7_issue_1_and_2/vol7.1%20aronson%20final.pdf Accessed 22 July 2014.

Associated Press. 2009. *A Look at Estonia’s Cyber Attack in 2007*. Internet: http://www.nbcnews.com/id/31801246/ns/technology_and_science-security/t/look-estonias-cyber-attack/#.VDaIKvmSzh4 Accessed: 20 September 2014.

Bachmann, J. 2012. *Kenya and International Security: Enabling Globalisation, Stabilising ‘Stateness’, and Deploying Enforcement.* Globalizations, 9 (1): 125-143. London: Routledge.

Bajaj, K. 2010. *The Cyber Security Agenda – Mobilizing for International Action*. New York, East West Institute.

Baldwin, D.A. 1997. 'The Concept of Security'. *Review of International Studies*. 23(1): 5-26.

Baylis, J. and Smith, S. 2001. *The Globalization of World Politics: An Introduction to International Relations*. Oxford. Oxford University Press.

BBC. 2014. *Kenya Bus Killings Claimed By Somali Group Al-Shabab*. 22 November. Internet: http://www.bbc.com/news/world-africa-30157581 Accessed: 29 November 2014

BBC. 2015. *US Centcom Twitter account hacked by pro-IS group*. 12 January. Internet: http://www.bbc.com/news/world-us-canada-30785232 Accessed: 13 January 2015

Blanchard, L. P. 2013. *U.S.-Kenya Relations: Current Political and Security Issues.* Congressional Research Service. Internet: http://www.fas.org/sgp/crs/row/R42967.pdf Accessed: 1 October 2014

Boulanin, V. 2013.*Cybersecurity and the Arms Industry*. Stockholm International Peace Research Institute (SIPRI). An offprint of section II of chapter 4 of SIPRI Yearbook 2013: Armaments, Disarmament and International Security Oxford University Press, 2013,

Bourne, M. 2014.*Understanding Security*. London. Palgrave Macmillan.

Brechbhl, H. Bruce, R. Dynes, S. & Johnson, E. M. 2010. 'Protecting Critical Information Infrastructure: Developing Cybersecurity Policy'. *Information Technology for Development.* 16 (1): 83- 91.

Briard. 2008. *A Brief History of Personal Computers*. Internet: http://www.techsupportalert.com/history-of-personal-computers.htm Accessed 22 October 2014.

Brickey, J. 2012. *Defining Cyberterrorism: Capturing a Broad Range of Activities in Cyberspace.* August 23, 2012. Internet: https://www.ctc.usma.edu/posts/defining-cyberterrorism-capturing-a-broad-range-of-activities-in-cyberspace Accessed: 20 September 2014.

Britannica. 2014. *World Wibe Web (WWW)*. Internet: http://global.britannica.com/EBchecked/topic/649051/World-Wide-Web-WWW Accessed: 26 June 2014.

Burgess, J. P. 2008. Non-Military Security Challenges. In *Contemporary Security and Strategy*. 2nd edition, edited by Snyder, C.A. Houndmills: Palgrave Macmillan.

Buzan, B. 1991.*People, States, and Fear: An Agenda for International Security Studies in the Post-Cold War Era*. 2nd edition. New York: L. Rienner Publishers. London

Buzan, B. 1998. Security: *A New Framework for Analysis*. Lynne Riennar Publishers

Caulderwood, K. 2014. *Nearly $1.7 Trillion Passed Through Kenyan Mobile Phones Last Year*. IB Times. January 10. Internet: http://www.ibtimes.com/nearly-17-trillion-passed-through-kenyan-mobile-phones-last-year-1535426 Accessed: 28 October 2014.

CERN. 2014. *The Birth of the Web*. Internet: http://home.web.cern.ch/topics/birth-web Accessed: 26 June 2014.

Choo, K. R. 2011. 'The Cyber Threat Landscape: Challenges and Future Research Directions.' *Computers & Security*.30: 719- 731.

CNN. 2014. "*Kenyatta: Terror in Africa a Global Issue*". 5 August. Internet: http://edition.cnn.com/video/data/2.0/video/business/2014/08/05/qmb-africa-terrorism-uhuru-kenyatta-intv.cnn.html Accessed: 6 August 2014.

Communications Authority of Kenya (CAK). 2014. *Quarterly Sector Statistics Report (January – March 2014).* Internet: http://ca.go.ke/images/downloads/STATISTICS/Sector%20Statistics%20Report%20Q3%202013-2014.pdf Accessed: 23 April 2014.

Communications Authority of Kenya (CAK). 2015. *Quarterly Sector Statistics Report: First Quarter of the Financial Year 2014/15 (July – September 2014).* Internet: http://ca.go.ke/images/downloads/STATISTICS/Sector%20Statistics%20Report%20Q1%202014-2015.pdf Accessed: 5 March 2015.

Communications Commission of Kenya (CCK). 2013. *All Statistics, CCK, Quarterly report, January 2013*

Communications Commission of Kenya (CCK). 2013. *Quarterly Sector Statistics Report (Jan-Mar 2013)*. Internet: http://cck.go.ke/resc/downloads/Sector_Statistics_Report_for_3rd_Quarter_2012-2013.pdf Accessed: November 13, 2013.

Cooperative Cyber Defence Centre of Excellence (CCDCOE). 2014. *History*. NATO. Internet: https://www.ccdcoe.org/history.html Accessed: 12 June 2014.

Council of Europe. 2014. *Convention on Cybercrime (ETS No. 185).* Internet: http://conventions.coe.int/Treaty/en/Summaries/Html/185.htm Accessed: 4 June 2014.

Daily Nation. 2012. *Massive Cyber-attack Hits 100 State Websites.* 17 January Internet:http://www.nation.co.ke/business/Tech/Massive+cyber+attack+hits+100+State+websites+/-/1017288/1309316/-/13shwd7z/-/index.html Accessed: 25 March 2014

Daily Nation. 2013. *How Safe is the Kenyan Cyberspace?* August 13, 2013 Internet: http://www.nation.co.ke/oped/blogs/Kenyan+cyberspace+is+not+safe/-/634/1945962/-/view/asBlogPost/-/1g2sx1/-/index.html Accessed: 23 April 2014.

Dalby, S. 2000. *Geopolitical Change and Contemporary Security Studies: Contextualizing the Human Security Agenda*. Institute for International Relations. The University of British Columbia. Working Paper No.30.

Demchak, C. C. 2011. *Wars of Disruption and Resilience: Cyber led Conflict, Power, and National Security*. The University of Georgia Press. Athens.

Dilanian, K. 2013. *Cyber-attacks a bigger threat than Al Qaeda, officials say*. Los Angeles Times, March 12, 2013. Internet: http://articles.latimes.com/2013/mar/12/world/la-fg-worldwide-threats-20130313 Accessed: 20 September 2014.

Dunn, C. M. 2008.*Cyber-Security and Threat Politics: US Efforts to Secure the Information Age*. Routledge: London.

Eneken Tikk, E. Kaska, K. & Vihul, L. 2010. *International Cyber Incidents: Legal Considerations, Cooperative Cyber Defence Centre of Excellence.* Tallinn: Estonia.

Eriksson, J. Giacomello, G. 2006. 'The Information Revolution, Security, and International Relations: (IR) relevant Theory?' *International Political Science Review*, 27: 221-244.

Ernst & Young. 2014. *Get Ahead of Cybercrime: EY's Global Information Security Survey 2014*. Internet: http://www.ey.com/Publication/vwLUAssets/EY-global-information-security-survey-2014/$FILE/EY-global-information-security-survey-2014.pdf Accessed: 5 November 2014

European Commission. 2013. *Cyber Security Strategy of the European Union: An Open, Safe and Secure Cyberspace*. Brussels. Internet: http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf Accessed: June 2014.

Evans, C. T. and Mack, H. 1999. *The PC Revolution*. Internet: http://novaonline.nvcc.edu/eli/evans/his135/events/pcrevolution76/revolution_text.htmlAccessed: 26 June 2014.

Fortinet. 2009. *Inquiry into Cyber Crime*. Internet: http://www.aph.gov.au/parliamentary_business/committees/house_of_representatives_committees?url=coms/cybercrime/subs/sub29.pdf Accessed: 20 September 2014.

Freeman, C. W. 1997. *Arts of Power: Statecraft and Diplomacy*. Washington. US Institute of Peace.

Gardner, H. 2005. *American Global Strategy and the "War on Terrorism"*. Aldershot: Ashgate.

Garnett, J.C. 1996. European Security after the Cold War, in Davis, M.J. (ed.) *Security Issues in the Post-Cold War World*. Cheltenham: Edward Elgar.

Geers, K. 2011. *Strategic Cyber Security*. NATO Cooperative Cyber Defence Centre of Excellence. Tallinn, Estonia.

Gercke, M. 2011. *Understanding Cybercrime: A Guide for Developing Countries*. Geneva: International Telecommunications Union (ITU). Internet: www.itu.int/ITU-D/cyb/cybersecurity/legislation.html. Accessed: 3 March 2014

Gilbert, D. 2014a. *DDoS Attacks Rise by 240% in 2014, Says Security Watchdog*. April 1 2014. International Business Times. Internet: http://www.ibtimes.co.uk/ddos-attacks-rises-by-240-2014-1442813 Accessed: 20 September 2014.

Gilbert, D. 2014b. *Hacktivists Hit Back at Israel After Death of Anonymous Member in West Bank*. July 28 2014. International Business Times. Internet: http://www.ibtimes.co.uk/hacktivists-hits-back-israel-after-death-anonymous-member-west-bank-1458623 Accessed: 20 September 2014.

Graham, J. Howard, R. and Olson, R. 2011. *Cyber Security Essentials*. Auerbach Publications: Taylor and Francis Group.

Guilmartin, J. F. 2013. *Reflections on the Revolution in Military Affairs*. *The RMA Debate*. Internet: http://www.comw.org/rma/fulltext/reflect.html#versus. Accessed: 10 April 2013.

Guzman, D. 2014. *National Intelligence Agencies Wary of Cyberterrorism as ISIS Builds a 'Digital Caliphate'*. September 25. Association of Certified Financial Crime Specialists (ACFCS). Internet: http://www.acfcs.org/national-intelligence-agencies-wary-of-cyberterrorism-as-isis-rises-as-a-digital-caliphate/ Accessed: 20 September 2014.

Haftendorn, H. 1991. *The Security Puzzle: Theory-Building and Discipline-Building in International Security*. International Studies Quarterly, 35 (1): 3-17

Hansen, L. and Nissenbaum, H. 2009. *Digital disaster, cyber security, and the Copenhagen School*. International Studies Quarterly, vol. 53 (4): 1155–75.

History Learning Site. 2006. *The Personal Computer*. Internet: http://www.historylearningsite.co.uk/personal_computer.htm Accessed: 26 June 2014.

History. 2014. *Invention of the Internet*. http://www.history.com/topics/inventions/invention-of-the-internet Accessed: 26 June 2014.

Hold Security. 2014. *You Have Been Hacked*! August 5. Internet: http://www.holdsecurity.com/news/cybervor-breach/ Accessed: 20 September 2014.

Howe, W. 2012.*A Brief History of the Internet*. Internet: http://www.walthowe.com/navnet/history.html Accessed: 27 June 2014.

Institute for Security Studies (ISS). 2012. *ISS and HSF Seminar Report: Kenya`s Foreign Policy and Geostrategic interests*. ISS. 10 May. Internet: http://www.issafrica.org/events/iss-and-hsf-seminar-report-kenyas-foreign-policy-and-geostrategic-interests Accessed: 29 October 2014

International Crisis Group (ICG). 2014. *Kenya: Al-Shabaab – Closer to Home. Africa Briefing: Number 102*. Internet: http://www.crisisgroup.org/~/media/files/africa/horn-of-africa/kenya/b102-kenya-al-shabaab-closer-to-home.pdf Accessed: 28 October 2014

International Data Corporation (IDC) Government Insights. 2014. *White Paper: Breaking the Barriers with Technology: A Special Report on the Kenyan ICT Market*. IDC. Internet: http://www.connected.go.ke/wp-content/uploads/2014/04/ICTA-Whitepaper_Final-100414.pdf Accessed: 23 June 2014.

International Telecommunications Union (ITU). 2008. *Data Networks, Open System Communications and Security: Telecommunication Security: Overview of Cyber Security*. ITU-TX.1205: series X: Geneva: ITU.

Internet World Stats. 2013. *Internet Usage Statistics for Africa*. Internet: www.internetworldstats.com/stats1.htm.Accessed: 3 March 2014

Itosno, S. 2014. *Kenya's Cyber Security Strategy Enters Homestretch*. March 17 2014. Internet: http://www.biztechafrica.com/article/kenyas-cyber-security-strategy-enters-homestretch/7862/#.U4tFcvmSwrU Accessed: 25March 2014.

Jourdan, A. 2014.*China-U.S. Cyber Spying Row Turns Spotlight back on Shadowy Unit 61398*. Tuesday May 20. Reuters. Internet: http://uk.reuters.com/article/2014/05/20/us-cybercrime-usa-china-unit-idUKBREA4J08M20140520 Accessed: 20 September 2014.

Jubilee Coalition. 2012. Transforming Kenya: *Securing Kenya's Prosperity 2013-2017*. Internet: http://www.scribd.com/document_downloads/123569244?extension=pdf&from=embed&source=embed Accessed: November 13, 2013.

Julisch, K. 2013. 'Understanding and Overcoming Cyber Security Anti-patterns.' *Computer Networks*, 57: 2206-2211.

Kaspersky. 2012. *Kaspersky Lab and ITU Research Reveals New Advanced Cyber Threat*. 28 May 2012. Internet: http://www.kaspersky.com/about/news/virus/2012/Kaspersky_Lab_and_ITU_Research_Reveals_New_Advanced_Cyber_Threat Accessed: 12 June 2014.

KE-CIRT. 2014. *About Us*. Internet: http://www.ke-cirt.go.ke/index.php/about-us/ Accessed: 15 June 2014.

Kenya Human Rights Commission (KHRC). 2014. *The Internet Legislative and Policy Environment in Kenya*. Nairobi. KHRC.

Kenya Revenue Authority (KRA). 2014. Internet: http://www.revenue.go.ke/ Accessed: 23 April 2014.

Kenya. 2007. *Vision 2030*. Nairobi. Government Printers. Internet: http://www.vision2030.go.ke/cms/vds/Popular_Version.pdf Accessed: 17 November 2013.

Kenya. 2010. *The Constitution of Kenya, Revised Edition*. National Council for Law Reporting. Government Printers. Nairobi. Internet: https://www.kenyaembassy.com/pdfs/The%20Constitution%20of%20Kenya.pdf Accessed: 15 April 2014.

Kenya. 2012. *National Security Intelligence Service Act: No. 11 of 1998*. National Council for Law Reporting. Government Printers. Nairobi

Kenya. 2013. *The National Broadband Strategy: A Vision 2030 Flagship Project*. Nairobi. Government Printers.

Kenya. ICT Authority. 2014b. *About ICT Authority*. Internet: http://www.icta.go.ke/ict-authority/ Accessed: 12 November 2014

Kenya. Ministry of Information, Communication and Technology. 2014a. *The Kenya National ICT Masterplan: 2014-2017*. Nairobi. Government Printers.

Kenya. Ministry of Information, Communication and Technology. 2014c. *National Cybersecurity Strategy 2014*. Nairobi. Government Printers.

Kenya. Ministry of Information, Communication and Technology. 2014d. *National Cybersecurity Framework 2014*. Government printers, Nairobi.

Kenya. State House. 2009. *The East African Marine Systems Cable Officially Launched*. Internet: http://www.statehousekenya.go.ke/news/june09/2009120601.htm Accessed: November 13, 2013.

Kenyatta, U. 2013. *President Uhuru Kenyatta's Speech during the 6th Extraordinary Summit of the Heads of State and Government on ICGLR*, 31 July. Internet: https://www.scribd.com/doc/157179276/President-Uhuru-Kenyatta-s-Speech-During-the-6th-Extraordinary-Summit-of-the-Heads-of-State-and-Government-on-ICGLR Access: 28 October 2014.

Kenyatta, U. 2014a. H.E *President Uhuru Kenyatta Speech During Jamhuri Day celebrations*, 12th December. Internet: http://www.president.go.ke/h-e-president-uhuru-kenyatta-speech-during-jamhuri-day-celebrations-12th-december-2014/ Access: 13 December 2014.

Kenyatta, U. 2014b. *President Uhuru Kenyatta's Speech during the Official Launch of the Communications Authority of Kenya, Westlands, Nairobi*, 24th June. Internet: http://www.president.go.ke/speech-by-his-excellency-hon-uhuru-kenyatta-c-g-h-president-and-commander-in-chief-of-the-defence-forces-of-the-republic-of-kenya-on-official-launch-of-the-communications-authority-of-kenya-commun/ Access: 10 August 2014.

Kesan, J. P. and Hayes, C. M. 2012. ‘Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace.’ *Harvard Journal of Law and Technology*, 25 (2): 417-527.

Kimani, M. 2013. *Gone in 12 months: How Fraudsters Stole $17m from Kenya’s Banks*. The East African. May 18. Internet: http://www.theeastafrican.co.ke/news/How-fraudsters-stole--17m-from-Kenya-s-banks/-/2558/1856364/-/fe3jd3/-/index.html Accessed: 20 July 2014.

Kiplagat, S. 2014. *Sh14.9bn Safaricom CCTV deal is signed*. The Star. 26 November. Internet: http://www.the-star.co.ke/article/sh149bn-safaricom-cctv-deal-signed Accessed: 2 January 2015.

Kisiangani, E. 2014.*Kenya’s Regional Relations: Between Principle and Practice*. South African Foreign Policy and African Drivers Programme. Policy Briefing 113.

Kizza, J. M. 2014. *Computer Network Security and Cyber Ethics, Fourth Edition*. Jefferson, NC: McFarland &Co Inc.

Klare, M. T. and Chandrani, Y. eds. 1998.*World Security: Challenges for a New Century*. Third Edition. New York: St. Martin's Press.

Klimburg, A. (Ed.) 2012. *National Cyber Security Framework Manual*. NATO CCD COE. Talinn, Estonia.

Landler, M. and Markoff, J. 2007. *In Estonia, What may be the First War in Cyberspace*. The New York Times, May 28, 2007. Internet: http://www.nytimes.com/2007/05/28/business/worldbusiness/28iht-cyberwar.4.5901141.html?pagewanted=all&_r=0 Accessed: 20 September 2014.

Leiner, B. M. Cerf, V. G. Clark, D. D. Kahn, R. E. Kleinrock, L. Lynch, D. C. Postel, J. Roberts, L. G. & Wolff, S. S. 2009. 'A Brief History of the Internet.' *ACM SIGCOMM Computer Communication Review*. 39 (5): 22- 31.

Lewis, J. A. 2014. 'National Perceptions of Cyber Threats'. *Strategic Analysis*. 38 (4): 566-576. Internet: http://dx.doi.org/10.1080/09700161.2014.918445 Accessed 20 September 2014.

Limnell, J. 2014. *Isis Propaganda War on the Front Line of Cyberspace*. September 15. International Business Times. Internet: http://www.ibtimes.co.uk/isis-propaganda-war-front-line-cyberspace-1465459 Accessed; 20 September 2014.

Lin, H. 2012. 'Some Modest Steps Towards Greater Cyber Security.' *Bulletin of the Atomic Scientists*, 68 (5): 2012.

Lumsden, A. 2012.*A Brief History of the World Wide Web*. Internet: http://webdesign.tutsplus.com/articles/a-brief-history-of-the-world-wide-web--webdesign-8710 Accessed: 26 June 2014.

Macharia, J. and Potter, M. 2014. *Safaricom Signs Security Contract with Kenya's Government*. Reuters. 25 November. Internet: http://www.reuters.com/article/2014/11/25/kenya-security-safaricom-idUSL6N0TF1A520141125 Accessed: 2 January 2015.

Malalo, H. 2011. *Kenya says Kidnapping Provocation by Al Shabaab*. Reuters, 3 October. Internet: http://www.reuters.com/article/2011/10/03/us-kenya-kidnap-idUSTRE7924OK20111003

Malingha, D. D. 2014.*Kenya Overtakes Ghana, Tunisia as Data Revision Boosts GDP*. Bloomberg. 30 September. Internet: http://www.bloomberg.com/news/2014-09-30/kenya-overtakes-ghana-tunisia-as-size-of-economy-climbs-by-25-.html Accessed: 28 October 2014.

Matinde, V. 2014. *High Data Costs a Factor in Mobile Insecurity in Africa*. IDG Connect. 14 October. Internet: http://www.idgconnect.com/abstract/8941/high-data-costs-factor-mobile-insecurity-africa Accessed: 28 October 2014.

McAfee. 2011. *McAfee Threat Report: Fourth Quarter 2010*, February 2011. Internet: https://personalmacgeniuses.com/wp-content/uploads/rp-quarterly-threat-q4-2010.pdf Accessed: 15 July 2013.

Mcafee. 2014. *McAfee Labs Threat Report: June 2014*. Internet: http://www.mcafee.com/hk/resources/reports/rp-quarterly-threat-q1-2014.pdf Accessed: 15 September 2014.

McEvoy, C. 2013. *Shifting Priorities: Kenya's Changing Approach to Peace Building and Peace-Making.* Norwegian Peace building Resource Centre (NOREF), Oslo, Norway. Internet: http://www.peacebuilding.no/var/ezflow_site/storage/original/application/bca199817c66f0d0f91212128181c024.pdf Accessed: 28 September 2014.

McSweeney, B. 1999. *Security, Identity and Interests: A Sociology of International Relations*. Cambridge: Cambridge University Press.

Merriam-Webster Dictionary. 2012. *Definition of Cyber*. Intenet: http://www.merriam-webster.com/dictionary/cyber. Accessed: 4 January 2014.

Merriam-Webster Dictionary. 2014a. *Definition of Personal Computer*. Internet: http://www.merriam-webster.com/dictionary/personal%20computer. Accessed 26 June 2014.

Merriam-Webster Dictionary. 2014b. *Definition of the Internet*. Internet: http://www.merriam-webster.com/dictionary/internet. Accessed: 26 June 2014

Meyers, C. Powers, S. and Faissol, D. 2009.*Taxonomies of Cyber Adversaries and Attacks: A Survey of Incidents and Approaches*. Lawrence Livermore National Laboratory.

Miller, E. K. 1989. *The Computer Revolution: A review of the continuing battle to increase our computational abilities*. IEEE: 27-31.

Misiko, H. 2014. *How Anonymous and other Hacktivists are Waging War on Kenya*. The Washington Post. 30 July. Internet: http://www.washingtonpost.com/blogs/worldviews/wp/2014/07/30/how-anonymous-and-other-hacktivists-are-waging-war-on-kenya/ Accessed: 28 October 2014.

Moeng, B. 2011. *9 Reasons to Invest in African ICT*. IT News Africa, 14 September. Internet: http://www.itnewsafrica.com/2011/08/9-tech-investment-opportunities-in-africa/ Accessed: 4 April 2013.

Mohamed, H. 2013. *Q&A: Al-Shabab defends Nairobi attack*. Al Jazeera, 25 September. Internet: http://www.aljazeera.com/indepth/features/2013/09/2013923628350977.html Accessed: 29 October 2014.

Munster, R. van. 2005. *Logics of Security: The Copenhagen School, Risk Management and the War on Terror*. Political Science Publications 10/2005, Odense: University of Southern Denmark.

Murithi, T. 2009. 'Inter-Governmental Authority on Development on the Ground: Comparing Interventions in Sudan and Somalia.' *African Security*, 2 (2-3): 136-157.

Mutegi, L. 2014. *KDF Twitter Accounts Hacked By #anonymous*. All Africa, 21 July. Internet: http://allafrica.com/stories/201407210683.html Accessed: 15 September 2014.

Mwenesi, S. 2014. *Kenyan ICT Giants come together to Launch @iLab Africa*. *Human IPO*. 20 June. Internet: http://www.humanipo.com/news/45324/kenyan-ict-giants-come-together-to-launch-ilab-africa/ Accessed: 30 October 2014

Nailab. 2014. *About Nailab*. Internet: http://www.nailab.co.ke/ Accessed: 30 October 2014

National Cohesion and Integration Commission (NCIC). 2014. *About NCIC*. Internet: http://www.cohesion.or.ke/index.php/about-us Accessed: 23 April 2014.

National Society for the Prevention of Cruelty to Children (NSPCC). 2014. *Bullying and Cyberbullying; What is*. Internet: http://www.nspcc.org.uk/preventing-abuse/child-abuse-andneglect/bullying-and-cyberbullying/what-is-bullying-cyberbullying/ Accessed: 28 October 2014.

Ndung'u, M. N. and Waema, T. M. 2012. *Understanding what is happening in ICT in Kenya: A Supply-and- Demand Side Analysis of the ICT Sector*. Internet: http://www.researchictafrica.net/publications/Evidence_for_ICT_Policy_Action/Policy_Paper_9_-_Understanding_what_is_happening_in_ICT_in_Kenya.pdf. Accessed: 16 June 2014

Neuneck, G. & Alwardt, C. 2008.*The Revolution in Military Affairs, its Driving Forces, Elements and Complexity: Interdisciplinary Research Group on Disarmament, Arms Control and Risk Technologies*: Institute for Peace Research and Security Policy: University of Hamburg.

Newman, E. 2010. 'Critical human security studies.' *Review of International Studies*. 36: 77–94.

Nuechterlein, D. E. 1976. 'National Interests and Foreign Policy: A Conceptual Framework for Analysis and Decision-Making.' *British Journal of International Studies*. 2(3): 246-266.

Nyange. H. 2014. *Kenya's National Cyber Security Framework*. Internet: http://www.cafrad.org/Workshops/Tanger23-25_06_14/Hans_KENYA.pdf Accessed: 15 September 2014.

oldcomputers.net. 2014.*MITS Altair 8800*. Internet: http://oldcomputers.net/altair-8800.html Accessed: 26 September 2014.

Open Briefing. 2015. *Remote-control warfare briefing #09*. 24 February. Internet: http://www.oxfordresearchgroup.org.uk/sites/default/files/Open-Briefing-remote-control-warfare-briefing-9-240215-5.pdf Accessed: 3 March 2015.

Otieno, J. 2014. *Worries over New Avenues of Cyber-Crime*. The East African. 22 September. Internet: http://www.theeastafrican.co.ke/news/Worries-over-new-avenues-of-cyber-crime/-/2558/2461630/-/vsn7k0z/-/index.html Accessed: 28 October 2014.

Owili, R. 2014. *Govt Launches Phase Two of National Optic Fibre Backbone Infrastructure*. Smart Kenya. 23 September. Internet: http://www.smartkenya.co.uk/govt-launches-phase-two-of-national-optic-fibre-backbone-infrastructure/Accesseded: 28 October 2014.

Peoples, C. and Vaughan-Williams, N. 2010. *Critical security studies: An introduction*. London: Routledge.

Perloth, N. 2012. *Hackers in China Attacked The Times for last 4 months*. New York Times, 30 Jan. 2013. Internet: http://www.nytimes.com/2013/01/31/technology/chinese-hackers-infiltrate-new-york-times-computers.html?pagewanted=all Accessed: 12 June 2014.

Perloth, N. and Gelles, D. 2014. *Russian Hackers Amass Over a Billion Internet Passwords*. August 5 2014. The New York Times. Internet: http://www.nytimes.com/2014/08/06/technology/russian-gang-said-to-amass-more-than-a-billion-stolen-internet-credentials.html?hp&action=click&pgtype=Homepage&version=LedeSum&module=first-column-region&region=top-news&WT.nav=top-news&_r=0 Accessed: 2 October 2014.

Peter, I. 2004. *History of the World Wide Web*. Internet: http://www.nethistory.info/History%20of%20the%20Internet/web.html Accessed: 27 June 2014.

Pfleeger, S. L. & Caputo, D. D. 2012. 'Leveraging Behavioural Science to Mitigate Cyber Security.' *Computers and Security*. 31: 597-611

PR Newswire. 2012. *Global Cyber Security Market worth $120.1 Billion by 2017*. Wall Street Online, 28 June 2012. Internet: http://www.wallstreet-online.de/nachricht/4952697-marketsandmarkets-global-cyber-security-market-worth-120-1-billion-by-2017 Accessed: 20 September 2014.

Price Waterhouse Coopers (PWC) 2011. *Cybersecurity M&A: Decoding Deals in the Global Cybersecurity Industry*. Internet: http://www.pwc.com/gx/en/aerospace-defence-and-security/publications/cyber-security-mergers-and-acquisitions.jhtml Accessed: 5 October 2014.

Ranger, S. 2014a. *Nearly Half of Companies Hit with DDoS Attacks in the Last Year*. Internet: http://www.zdnet.com/nearly-half-of-companies-hit-with-ddos-attacks-in-the-last-year-7000031073/ Accessed: 20 September 2014.

Ranger, S. 2014b. *Organised Cybercrime Groups are now as Powerful as Nations*. Internet: http://www.zdnet.com/organised-cybercrime-groups-are-now-as-powerful-as-nations-7000030323/ Accessed: 20 September 2014.

Reuters. 2014. *Kenya's Economy Increases by a Quarter to Join Africa's top 10*. 30 September. Internet: http://www.reuters.com/article/2014/09/30/kenya-economy-idUSL6N0RV1Q020140930 Accessed: 28 October 2014.

Reveron, D. S. 2012. *Cyber Challenges and National Security: Threats, Opportunities, and Power in a Virtual World*. Baltimore, MD: Georgetown University Press.

Rezk, D. 2010. *The Revolution in Military Affairs and the Changing Nature of Warfare in the Middle East*. Internet: http://blogs.lse.ac.uk/ideas/2010/04/the-revolution-in-military-affairs-and-the-changing-nature-of-warfare-in-the-middle-east/Accessed. 9 April 2013.

Rid, T. 2012. 'Cyber War Will Not Take Place.' *Journal of Strategic Studies*, 35 (1): 5-32.

Robb, D. 2014. *Sony Hack: A timeline*. Deadline. 22 December. Internet: http://deadline.com/2014/12/sony-hack-timeline-any-pascal-the-interview-north-korea-1201325501/ Accessed: 20 February 2015.

RT News. 2014. *'Israel you're weak': Anonymous hacktivists shut down key Israeli websites*. August 4. Internet: http://rt.com/news/177936-anonymous-gaza-mossad-idf/ Accessed 20 September 2014.

Rudner, M. 2013. 'Cyber-Threats to Critical National Infrastructure: An Intelligence Challenge.' *International Journal of Intelligence and Counterintelligence*, 26 (3): 453-481.

Saleh, A. 2010. 'Broadening the Concept of Security: Identity and Societal Security.' *Geopolitics Quarterly*, 6 (4): 228-241.

Schreier, F. 2012. 'On Cyber Warfare.' *DCAF Horizon 2015 Working Paper*, No. 7.

Schreier, F. Weekes, B. and Winkler, T. H. 2011. 'Cyber Security: The Road Ahead.' *DCAF Horizon 2015 Working Paper Series* (4).

Schultze, C.L. 1973. 'The Economic Content of National Security Policy.' *Foreign Affairs*, 51 (3): 529-530.

Schumann, R. and Kende, M. 2013. *Lifting barriers to internet development in Africa: suggestions for improving connectivity*. ISOC. Internet: http://www.internetsociety.org/sites/default/files/Barriers%20to%20Internet%20in%20Africa%20Internet%20Society.pdf Accessed: 23 April 2014.

Serianu. 2014. *Kenya Cyber Security Report. Rethinking Cyber Security – "An Integrated Approach: Processes, Intelligence and Monitoring."* Nairobi. Serianu. Internet: http://www.Serianu.com/downloads/KenyaCyberSecurityReport2014.pdf Accessed: 22 July 2014.

Sheldon, J. B. 2012. 'State of the Art: Attackers and Targets in Cyberspace.' *Journal of Military and Strategic Studies,* 14 (2): 1-19.

Sheldon, J. B. 2013. The Rise of Cyberpower. In *Strategy in the Contemporary World*, edited by Baylis, J. Wirtz, J. J. & Gray, C. S. Oxford. Oxford University Press.

Sofaer, A. D. Clark, D. Diffie, W. 2010. *Cyber Security and International Agreements. Proceedings of a Workshop on Deterring Cyber Attacks: Informing Strategies and Developing Options for U.S. Policy*. Internet: http://www.nap.edu/catalog/12997.html Accessed: 15 September 2014.

Souter, D. and Kerretts-Makau, M. K. 2012. *Internet Governance in Kenya- An Assessment for the internet Society*. Internet: http://www.internetsociety.org/sites/default/files/ISOC%20study%20of%20IG%20in%20Kenya%20-%20D%20Souter%20%26%20M%20Kerretts-Makau%20-%20final.pdf Accessed: 23 April 2014.

Study of Terrorism And Responses to Terrorism (START). 2013. *Background Report: Al-Shabaab Attack on Westgate Mall in Kenya*. Internet: http://www.start.umd.edu/sites/default/files/publications/local_attachments/STARTBackgroundReport_alShabaabKenya_Sept2013.pdfAccessed: 28 October 2014.

Techi Warehouse. 2010. *History, Origins, and Generations of Computers*. January 13 2010. Internet: http://www.techiwarehouse.com/cms/engine.php?page_id=51c38188. Accessed: 26 June 2014.

Techopedia.2014a. *Definition of Denial of Service (DoS) Attack*. Internet: http://www.techopedia.com/definition/24841/denial-of-service-attack-dos Accessed: 15 September 2014.

Techopedia.2014b. *Definition of Distributed Denial of Service (DDoS) Attack*. Internet: http://www.techopedia.com/definition/10261/distributed-denial-of-service-ddos Accessed: 15 September 2014.

Techopedia.2014c. *Definition of Hacker*. Internet: http://www.techopedia.com/definition/3805/hacker Accessed: 15 September 2014.

Tespok Kenya iCSIRT. 2013. *Cyber Threat Trends Report: Quarter 3, July- September 2013*. Internet: http://www.tespok.or.ke/reports/Q3-2013/Cyber%20Threat%20Trends%20Report_Q3.pdf Accessed: 23 April 2014.

The History of the Personal Computer and other Computers which have had an impact upon Society. 2014. Internet: http://ncehshistorycomputer.tripod.com/index.html. Accessed 26 June 2014.

Think Security Africa. 2014. *A National Security Profile on the Republic of Kenya*. Internet: http://thinksecurityafrica.org/wordpress/wp-content/uploads/National-Security-Profile-Kenya.pdf Accessed: 28 October 2014.

Tikk, K. Kaska, K. Rünnimeri, M. Kert, A. Talihärm& L. Vihul, (2008). *Cyber Attacks Against Georgia: Legal Lessons Identified*. Internet: http://www.carlisle.army.mil/DIME/documents/Georgia%201%200.pdf Accessed 22 July 2014.

Traynor, I. 2007. *Russia Accused of Unleashing Cyberwar to Disable Estonia*. The Guardian. 17 May 2014. Internet: http://www.theguardian.com/world/2007/may/17/topstories3.russia Accessed: 20 September 2014.

UN Office on Drugs and Crime (UNODC). 2013. *Comprehensive Study on Cybercrime*. Internet: www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf. Accessed: 3 March 2014.

United Nations Development Program (UNDP). 1994. *Human Development Report*. New York: Oxford University Press.

United Nations Institute for Disarmament Research (UNIDR). 2013. *The Cyber Index: International Security Trends and Realities*. Geneva, Switzerland.

University System of Georgia (USG). 2014. *A Brief History of the Internet*. Internet: http://www.usg.edu/galileo/skills/unit07/internet07_02.phtml Accessed: 26 June 2014.

US Department of Defence (DoD). 2011. *Department of Defense Strategy for Operating in Cyberspace*. Washington, DC.

Von Solms, R. & van Niekerk, J. 2013. *From Information Security to Cyber Security*. Computers & Security: 1- 6. http://dx.doi.org/10.1016/j.cose.2013.04.004 Accessed: 21 November 2013

Waever, Ole. 1993. *Societal Security: The Concept*. Identity, Migration and the New Security Agenda in Europe. London. Pinter Publishers.

Wangalwa, E. 2014. *Kenya Leads Africa's Internet Access and Connectivity*. CNBC Africa. 9 September. Internet: http://www.cnbcafrica.com/news/east-africa/2014/09/09/kenya-leads-internet/ Accessed: 28 October 2014.

Wanjiku, R. 2014. *Kenya's Cyber Security Concerns on the Rise*. PC Advisor. 17 June. Internet: http://www.pcadvisor.co.uk/news/security/3525420/kenyas-cybersecurity-concerns-on-the-rise/ Accessed: 28 October 2014.

Wanyama, L. 2013. *The Economic Diplomacy of Kenya's Regional Interests*. SAIIA Occasional Paper No 137. Internet: http://www.saiia.org.za/occasional-papers/the-economic-diplomacy-of-kenyas-regional-interests Accessed: 29 October 2014.

Weng Loo, B. F. 2005. 'Transforming the Strategic Landscape of Southeast Asia. Contemporary Southeast Asia.' *A Journal of International and Strategic Affairs*. 27 (3): 388-405.

White House. 2009. *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure*. Internet:

https://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf Accessed: 13 March 2014.

WhoIsHostingThis.com. 2014.*History of the Web*. Internet: http://www.whoishostingthis.com/resources/history-of-web/#ixzz3FRvFWJDR Accessed: 26 June 2014.

Wolfers, A. 1952. “National Security” as an Ambiguous Symbol. *Political Science Quarterly*. 67 (4): 481-502.

World Bank. 2014. Kenya Overview. Internet: http://www.worldbank.org/en/country/kenya/overview Accessed: 28 October 2014.

Wyn Jones, R. 1996. "Travel Without Maps": Thinking About Security After the Cold War, in Davis, M.J. (ed.) *Security Issues in the Post-Cold War World*. Cheltenham: Edward Elgar.

Zelikow, P. 2003. *The Transformation of National Security: Five Redefinitions*. The National Interest- Spring 2003.

Zetter, K. 2010. *Google Hack Attack Was Ultra Sophisticated, New Details Show*. Wired. 14 January. Internet: http://www.wired.com/2010/01/operation-aurora/ Accessed: 26 September 2014.