University of Glasgow

School of Social and Political Sciences

# Role of Cybersecurity Strategy on Citizens Security: Approaches to Improve Public Awareness on Mobile Internet Threats

# in Kenya.

**Word Count: 14999.**

**August, 2014.**

**2079164O**

**Presented in partial fulfilment of the requirements for the Degree of**

**MSc Global Security [Politics, Information and Security].**

*This page is left intentionally blank*

## DECLARATION

I am aware of and understand the University’s policy on plagiarism and l certify that this dissertation is my own work, except where indicated by referencing, and that l have followed the good academic practices prescribed by the University.

Signed: AAO

Approved by: Dr. Karen Renaud

Dissertation Supervisor.

# DEDICATION

I dedicate this dissertation to my loving husband Paul Magacha whose support, commitment and sacrifice were instrumental in completing this programme. My dedication is also extended to my incredibly brave children Angel, Fidel and Alicia who allowed me to pursue my dream far away from them; my wonderful late mother Alice, my siblings Christopher, Yvonne and nephew Pharell.

# ACKNOWLEGDEMENTS

I would like to express my sincere gratitude to the Almighty God for His grace, favour and spiritual support throughout my programme at the University of Glasgow. I am also indebted to the prestigious Chevening UK Government Scholarships for sponsoring my Master's degree at an international university. Without Chevening, this dream would not have been possible. My experience has been gratifying both academically and culturally. The knowledge gained will be beneficial to my country and future engagements.

To my dissertation supervisor, Dr. Karen Renaud, I am filled with gratitude for your direction, guidance and suggestions. You were very resourceful in critical issues that came up in the course of the research. Your prompt responses on my progress were very significant in writing this report and enabled me to complete it in ample time.

I deeply thank my husband Paul Magacha for his love, support and belief in me which without, it would have been a struggle to complete this programme. Finally, I acknowledge the support of my Directors, Major Rtd. Raphael Kosen and Mr. Isaac Ochieng, and Manager, Mr. Mark Ogonji in pursuit of my master's degree.

# ABSTRACT

Cybersecurity has become a global phenomenon. As governments in the developing world harness ICTs and the Internet to provide better services, meet millennium development goals, liberate human and technical capacity, so does the threat to individual citizens increase accordingly. It is distinctly interesting for Kenya whose Internet growth has been supported by high mobile proliferation and adoption. This places Kenya in a unique position as a case study in the area of cybersecurity in Africa and in particular mobile Internet security. It motivated this study to investigate the role of cybersecurity strategy on citizens security and to explore approaches to improving public awareness of mobile Internet threats that undermine the aim of the strategy.

Participants for the study were drawn from the KICTANet listserv who were surveyed over a four week period through an online survey tool. 58 responses were received forming the sample for analysis through stratified sampling. Thematic analyses were carried out on the data and findings presented using a mixed method approach.

The study confirmed the prevalence of mobile Internet threats with participants suggesting awareness drives to empower the public to improve on detection and enhance coping skills. Easily accessible security-related technology and law enforcement were also proposed as ways to reinforce the awareness drives targeting different sectors of society.

It was concluded that rather than targeting one sector of society with cybersecurity awareness training, it is incumbent on the government to sustain national awareness drives to target all users on mobile Internet.  This may be achieved through media and public campaigns, carrying out national surveys on cybersecurity awareness to identify the gaps that would inform the awareness drives, supporting the public with information on threats through institutions such as the CID, KE-CIRT/CC and Huduma Centres and the government taking the lead role in partnering with mobile network providers to support the public to adapt to the evolving mobile Internet threats.

## TABLE OF CONTENTS

# TABLE OF FIGURES

# LIST OF ABBREVIATIONS AND ACRONYMS

AU – African Union

BYOD – Bring Your Own Device

CAK – Communications Authority of Kenya

CID – Criminal Investigation Department

CSIRT – Computer Security Incident Response Team

COE – Council of Europe

CyberSAT – Cyber Security Awareness Toolkit

DFID – Department of International Development

EASSy – Eastern Africa Submarine Cables

ENISA – European Union Agency for Network and Information Security

ERM – Enterprise Risk Management

IBM – International Business Machines

ICT – Information Communication Technology

ICTA – Information Communication Technology Authority

IDG Connect – International Data Group Connect

ISP – Internet Service Provider

ITU – International Telecommunication Union

KE-CERT – Kenya Computer Emergency Response Team

KE-CIRT/CC – Kenya Computer Incidence Response Team/Co-ordination Centre

KICTANet – Kenya ICT Action Network

KNBS – Kenya National Bureau of Standards

MIT- Mobile Internet Threats

LION – Lower Indian Network

MitB – Man-in-the-Browser

MitM - Man-in-the-Middle

NIST – National Institute of Standards and Technology

OECD – Organisation for Economic Co-operation and Development

OWASP – Open Web Application Security Project

RIA – Research ICT Africa

SD – Secure Digital

UK – United Kingdom

UN – United Nations

UNDOC – United Nations Office on Drugs and Crime

VOIP – Voice over Internet Protocol

*This page is left intentionally blank*

# CHAPTER ONE

## INTRODUCTION

The International Telecommunications Union[1] (ITU) posits that enhancing cybersecurity and protecting critical information infrastructures are essential to each nation's security and economic well-being (2009, p.10). It acknowledges that the influence of information communication technology (ICT) on society goes beyond establishing basic information infrastructure to developing, availing and using networked services such as Internet-based communication, online banking and shopping, Mobile Data Services and Voice over Internet Protocol (VoIP) telephony (ibid). The availability of networked services and ICTs offer a variety of benefits for society in general and especially the developing world, including ICT applications, such as e-Government, e-Commerce, e-Education, e-Health and e-Environment (ibid).

As governments in the developing world harness ICTs and the Internet to provide better services, meet millennium development goals, liberate human and technical capacity, so does the threat to individual citizens on all platforms increase accordingly. ITU observes that attacks against information infrastructure and Internet services now have the potential to harm society in critically new ways (2009, p.11). Making the Internet safer and protecting Internet users has become crucial to the development of new services as well as to governmental policy (ibid).

Therefore, this study finds it useful to focus on one particular area in a phenomenon as huge as this one, and learning lessons from developing countries in this respect. Kenya has undergone an ICT revolution following the laying of undersea cables in 2009 creating high demand for the Internet (Souter and Kerrets-Makau 2012, Demombynes and Thegeya 2012). In addition to Demombynes and Thegeya's recognition of the ICT revolution's influence on the proliferation of mobile money that was launched in 2007 by Safaricom Kenya, a leading mobile network provider (2012, p.1,3) it also important to note that these mobile phones are used to access the Internet according to Research ICT Africa-RIA (RIA, 2012). Statistically, of all the Internet/data users in Kenya, about 98% access Internet/data via mobile broadband (Waema and Ndungu 2012, p.12). Other scholars also adduce that the third wave of mobile

[1] http://www.itu.int/en/about/Pages/default.aspx ITU is UN's specialized agency for ICTs that develops technical standards to ensure networks and technologies interconnect while striving to improve ICTs access to underserved communities worldwide.

for development (M4D) is emerging and focuses on mobile Internet associated with smartphones offering fast data connections, diverse applications, mostly used by business people to complement traditional personal computer Internet access (Gitau et al 2010, p.2603).

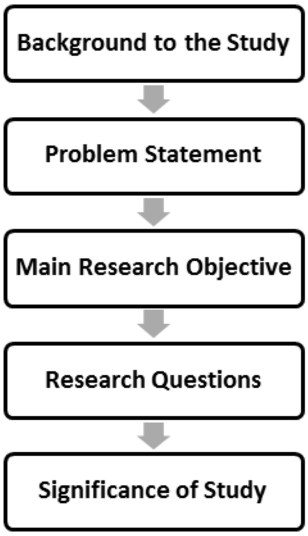
Certainly, these views underpin the importance, for African governments of developing cybersecurity strategies to protect their citizens and information infrastructure from cyber threats, particularly on mobile Internet. Phahlamohlaka et al posits that developing nations have no option but to be part of the cyber citizenry and join the race in developing cybersecurity policies that will support their economic wellbeing and national security (2011, p.2). Mobile phones are also becoming one of the primary communication tools in the developing world and increasingly being used to access the Internet (Andjelkovic 2010, p122).

Notably, with the exception of South Africa, a few African states such as Kenya are launching their newly developed cybersecurity strategies in response to threats emanating from Internet usage. This places Kenya in a unique position as a case study in the area of cybersecurity in Africa and, in particular, mobile Internet security as Kenya can set a benchmark for other African nations with vibrant mobile sectors yet to develop cybersecurity strategies. It further motivates this study to investigate the role of Kenya’s Cybersecurity strategy[2] on citizens security and in particular to explore the approaches that will be used to improve public awareness of mobile Internet threats (abbreviated as MIT hereafter), that undermine the measures aimed at improving citizens’ security.

The remaining section of this chapter places Kenya’s MIT predicament into context. It begins with a background to the study where Kenya’s Internet history and mobile proliferation are discussed. This is followed by the problem statement that gives a concise description of Kenya’s MIT prevalence and a conceptual framework developed from the theoretical framework, which proposes ways to address the MIT. Three research questions derived from the main research objective are outlined in the subsequent sub-section with the chapter ending with a succinct discussion of the study’s significance academically, nationally and regionally. This is illustrated in Figure 1.

[2] http://www.icta.go.ke/wp-content/uploads/2014/03/GOK-national-cybersecurity-strategy.pdf

**Figure 1**. Chapter One Overview



*Source: Author, 2014.*

### A. Background to the study

Cybersecurity is at the core of our understanding the digital age in which we live today. Practically all spheres of life are undertaken on the Internet using virtual technologies. Therefore, as cybersecurity is interwoven with all areas of life for all people, the differential outcome between good and bad cybersecurity policies broadens, while the ease of finding answers falls (Geer, 2014). ITU observes that cybersecurity being a global phenomenon that has increased threats to all spheres of life, requires effective strategies to reduce cyber-attacks (2009, p.8).

In this regard, countries from different regions in the world have developed their national cybersecurity strategies in response to increased cyber-attacks against their critical infrastructure, economy and society. Internationally, the Organisation for Economic Co-operation and Development's (OECD) comparison of new generation cybersecurity strategies of Australia, Canada, France, Germany, Japan, the Netherlands, the United Kingdom and United States points to an elevation of cyber threats among top priority national security matters (2012, p.9). Regionally, the African Union (AU) endorsed a declaration to develop jointly with United Nations Economic Commission for Africa, a Convention on cyber legislation based on Africa's needs (2009). African states are consulting on AU's Draft Convention on Cybersecurity aiming to strengthen existing national cybersecurity legislations (ibid). However, in Africa, only South Africa's Cyber Security Policy has been published by the European Union Agency for Network and Information Security[3] (ENISA) with Rwanda, Namibia, Uganda and Kenya's awaiting publication (2013).

Economically and socially, developing countries like Kenya are less equipped to take advantage of the potential in ICT to stimulate growth and are likely to fall behind advanced economies (National ICT Master Plan[4] 2014, p.3). The number of Internet users in Kenya has rapidly grown following the laying of submarine cables in 2009 consequently increasing her available bandwidth (Serianu 2012, p.4). Similarly, the growing Internet dependence by the government, public and private sector through use of computers, mobile phones, tablets has certainly increased cyber threats against information systems used in Kenya. Lack of cybersecurity awareness by the public exacerbates the situation. Coupled with poor security measures and a lack of a legal framework to develop policies that would protect information infrastructure, the threat posed by cyber is extant (ibid).

Moreover, Magutu et al argue that the realm of cyberspace has provided a range of opportunities for criminal activities, posing a challenge on how to tackle them due to a lack of cyber awareness (2011, p.2). Their study underpins the gap left by lack of proper cyber-legislation to prosecute cyber-crimes including spamming, phishing, malware and hacking, which are increasing in Kenya. Additionally, the study found that lack of security online is a serious threat to the economy following the laying of the national fibre optic that increased Internet dependence and subsequently Internet threats (ibid).

Serianu's first study of Kenya's cybersecurity threat status reports that MIT was growing in tandem with mobile money business (2012, p.22). The report points to an increasing number of scams and fraud targeting mobile phone users. Likewise, it indicates that Symantec reported that mobile vulnerabilities increased by 93% in 2011 with new mobile-specific malware geared to the unique mobile opportunities (ibid). In its 2014 Cybersecurity Threat Study, Serianu affirms that mobile banking threats and mobile money fraud were on an upward trajectory targeting individuals and organisations (Serianu 2014, p.12). It posits that 2011 was the first year that mobile malware presented a tangible threat to businesses and consumers where these malware were designed for data collection, sending content and user tracking (ibid).

[3] http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-in-the-world

[4] http://www.icta.go.ke/national-ict-masterplan/

Against this backdrop, the Kenyan government through the Information Communication Technology Authority (ICTA) developed the national Cybersecurity Strategy to address gaps in information security (ICTA, 2013). ICTA acknowledges that there are numerous security gaps that have not been factored in as risks when developing systems despite huge investments made by government, banking and telecommunication sectors (ibid).

It is important to note at this point that the study acknowledges South Africa's Cybersecurity Policy[5] that highlights a strategy in creating cybersecurity awareness, which sets a benchmark for Kenya. However, this study proposes that Kenya's unique mobile Internet society and its high mobile proliferation requires her to develop a tailored strategy meeting its technical, legal and societal needs as mentioned in this sub-section. The following sub-section describes the key concepts that will be referred to in this study hereinafter.

### *Description of related concepts*

As with every contested concept, related concepts of cybersecurity and cybercrime have no universally acceptable definition since governments, international institutions and IT organizations define them differently. The concept of *cybersecurity* is sometimes defined as a single word, 'cybersecurity' and other times as two words 'cyber security' both generally implying the protection of information systems and users from cyber-attacks.

For instance, ITU adopts the term as one word and defines it as;

> Cybersecurity is the collection of tools, policies, security, concepts, security safeguard, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment, organisations and users' needs.

The definition encompasses both technical and non-technical efforts to protect different aspects of cyber and its users. It also takes into account the objective of the concept to cyber space.

ENISA (2010, p.4) on the other hand adopts the term as two words 'cyber security' and defines it as;

[5] http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/southafricancss.pdf

> The protection of information, information systems and infrastructure from those threats that are associated with using ICT systems in a globally connected environment.

As both definitions inherently imply the protection of information systems, ICTs and their users from attacks in the cyberspace, this study proposes to adopt ITU's definition of cybersecurity. The study notes that Kenya's Cybersecurity strategy does not offer a definition of the term but only refers to its goal to protect Kenya's national cyberspace.

*Cybercrime* is an equally contested term as international institutions and nations approach the concept by way of describing the acts that constitute it rather than by defining it. ITU posits that there are difficulties in defining the term 'cybercrime' as no single definition could include a range of offences from traditional computer crimes, and network crimes (2009, p.18). Nevertheless, the Council of Europe[6] (COE, 2001) which established the Budapest Convention of Cybercrime (standards: CETS 185) recognised today as an important international instrument in combatting cybercrime describes it in the following categories;

- Offences against the confidentiality, integrity and availability of computer data and systems. This includes illegal access, interception of data, misuse of devices and system interference;
- Computer-related offences including forgery and fraud;
- Content-related offences including offences related to child pornography;
- Copyright-related offences.

Similarly, in a study commissioned by the United Nations Office on Drugs and Crime (UNDOC) on cybercrime, UNDOC describes cybercrime by the inherent acts because of the difficulties arising in defining it (2013, p.5). It argues that very few international conventions or regional legal instruments including the COE's Cybercrime Convention, League of Arab States Convention, AU Draft Convention and Shanghai Cooperation Organization Agreement define cybercrime (p.12). The acts include;

[6] http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm

- Acts against the confidentiality, integrity and availability of computer data or computer systems including unauthorised access, interceptions of computer systems or data;
- Computer related acts for personal or financial gain or harm such as fraud, identity offenses, child exploitation;
- Computer content-related acts- such as hate speech.

It is clear that the COE and UNDOC descriptions of cybercrime have similar contexts of the phenomenon despite COE including a fourth category to cover offenses related to intellectual property. Therefore, instructively, this study adopts the categories of cybercrime as listed by COE to refer to mobile Internet threats - MIT.

It is also proposed in this study to include the threats of malware, phishing attacks and spam in the description of MIT as provided by the ENISA's list of major mobile threats (ENISA, 2010).

The study further adopts the definition of a *computer system* as given by COE's Cybercrime Convention; "any device or a group of interconnected of related devices, one or more of which, pursuant to a program performs automatic processing of data" (2001). According to UNDOC, this definition encompasses devices such as mainframe and computer servers, desktops, laptops, smart phones, tablet devices and on-board computers on transit, multimedia devices such as printers, MP3 Players and digital cameras and gaming machines (2013, p.14). It also precludes the need to revise the definition to incorporate more devices every time a new technology is introduced in ICT.

### *History of Internet in Kenya*

The Communications Authority of Kenya[7] (CAK) formerly Communications Commission of Kenya (CCK) dates the introduction of Internet in Kenya back to the early 1990s, where its development was primarily driven by Kenyans returning from overseas studies, Western expatriates and personnel in non-governmental organizations (NGO) who demanded access (CAK 2007, p.34). With a few Internet service providers (ISP) in Kenya, coupled with high costs of personal computers and modems, Internet access was very

[7] http://www.ca.go.ke/ regulatory authority for Kenya's communications sector

expensive. CAK indicates that the early adopters of the Internet were mainly industries with overseas operations, the import/export sector and a few universities.

Prior to former CCK's establishment in 1999 by the Kenya Communications Act 1998, the Kenya Posts and Telecommunications Corporation (KPTC, later renamed Telkom) retained a monopoly in operating the Internet gateway and backbone till mid-2004 (CAK 2007, p.36). However, the liberalisation of the telecommunications industry by the Act allowed more scope for private sector innovation and market with CCK regulating it and issuing more commercial ISP's with licences (ibid). Telkom's monopoly ended with CCK adding two more Internet Backbone Gateway Operators and allowed telecommunication businesses including Telkom Kenya Limited, Safaricom Kenya Limited and Celtel Kenya (now named Airtel Networks Limited), to offer mobile Internet services in competition with stand-alone ISPs (Souter and Kerrets-Makau 2012, p.7). The fourth mobile network provider that offers Internet services is Essar Telecom Kenya Limited.

This development led to a high demand for Internet access among Kenyans although Kenya depended on expensive satellite uplinks for international telecommunication and Internet connections. In 2009, the government spearheaded the laying of East African Marine System (TEAMS) and SEACOM cables under the sea bed of Kenya's coastal town, Mombasa, increasing available international bandwidth in Kenya and other East African nations (Souter and Kerrets-Makau 2012, p.9). Two other cables, Eastern African Submarine Cables (EASSy) funded by World Bank and Lower Indian Network (LION) built by France Telecom and Telkom Kenya, connected Mombasa with the island states of Southern Africa (ibid). With the laying of fibre optic cables, Internet speeds in Kenya matched those in the first world with increased traffic resulting.

### *Mobile Internet penetration in Kenya*

The aforementioned four national mobile network operators offer mobile Internet to their subscribers with the latest CAK's ICT Sector Quarter Statistics in the financial year ending 2013/4 reporting an increase of 13.1% of mobile Internet subscriptions up from 11.6% in 2012/3 (2014, p.22). Out of the 13.1 million Internet subscribers, 13.0 million are mobile Internet subscribers representing 99.0% of the total Internet subscriptions. CAK also reports that the number of Internet users in Kenya had grown to 21.2 million by the end of 2013 up from 16.2 million in 2012 as shown in Table 1 (ibid).

Table 1: Internet Subscriptions and Internet Users

| **Internet/data subscription** | **Dec 2013** | **Sept 2013** | **Quarterly change (%)** | **Dec 2012** |
|---|---|---|---|---|
| **Total Internet subscription** | 13,186,968 | 11,671,337 | 13.0 | 9,496,575 |
| **Mobile** | 13,090,348 | 11,580,065 | 13.0 | 9,406,843 |
| **Fixed wireless** | 16,429 | 17,169 | -4.3 | 23,814 |
| **Satellite** | 682 | 749 | -8.9 | 684 |
| **Fixed DSL** | 12,014 | 11,537 | 4.1 | 10,807 |
| **Fixed Fibre optic** | 67,470 | 61,739 | 9.3 | 54,400 |
| **Fixed cable modem** | 25 | 25 | 0.0 | 25 |
| **Total Internet users** | **21,273,738** | **19,162,055** | **11.0** | **16,236,583** |

*Source: CAK, 2014.*

The RIA 2011 Survey that investigated Internet usage of 11 African countries reported that 23.5% Kenyans accessed the Internet through their mobile phones (RIA, 2012). It further revealed that 77.8% Kenyans aged 15 years and above accessed the Internet using their mobile phones in the twelve months preceding the survey compared to 72.4% who accessed it through a cyber cafe (ibid). These statistics are a clear indication of the high penetration rate of mobile Internet in Kenya where CAK (2014, p.22) reports it grew by 13%.

It should be remembered that at the time of RIA's survey, the Kenya National Bureau of Statistics (KNBS) had reported Kenya's population to be 38.6 million with 58% being above 15 years (KNBS, 2013), depicting mobile penetration was reaching saturation. As the level of mobile Internet subscription is lower than that of mobile penetration, 13 million against 31.3 million (CAK 2014, p.9), it is expected that the aforesaid mobile network providers would focus their marketing strategies to providing mobile Internet services to remain competitive. For instance Safaricom, the largest mobile Internet provider, has an application store where its subscribers can download applications ranging from games, communication, and business to entertainment on their Android mobile phones (Safaricom, 2014).

Moreover, the Kenyan market is saturated with a variety of Internet-enabled mobile phones and competitive data bundles offered at affordable prices (CAK 2014, p.22). However, despite the National Institute of Standards and Technology (NIST) acknowledging the new capabilities of modern mobile phones, it cautions that they lack strong roots of trust to perform critical security functions like those built in computers (NIST, 2014). For instance, mobile phones are incapable to measure and verify software, protect cryptographic keys or even perform device authentication (ibid).

It is worthy to note that the Kenyan public is not security-savvy to detect and prevent cybercrime perpetrated through their mobile phones (Serianu 2012, p.4). Internet-enabled mobile phones are designed in such a way that they do not require high IT skills to operate them but are needed to prevent fraud. Needful to say, the roles of Kenya's Computer Emergency Response Team (KE-CERT) and Kenya Computer Incident Response and Coordination Centre (KE-CIRT/CC) in increasing citizens cybersecurity awareness with respect to MIT, need to be highlighted. This underscores the need for a government strategy that prioritises increasing public awareness on the extant MIT, how to report them and explaining how public can protect itself.

This brief background clearly depicts that Kenya's Internet usage, which has been amplified by high mobile proliferation, is facing cyber threats that require awareness to improve citizens' security. This guides the identification of themes underscored in the following sub-section.

### *Theoretical Framework*

The study identified key themes that form a theoretical framework in understanding the problem of mobile Internet insecurity as follows;

- Increased Internet dependence and mobile Internet use
- Poor security measures for Internet use
- Increased cybercrime against mobile phones users
- Lack of cybersecurity awareness by the public
- Lack of legal framework to develop and enforce Internet security policies

These themes highlight the need to raise public cybersecurity awareness on MIT following Kenya's ICT revolution and proliferation of mobile phones used to access the Internet. To place them into context, the study's problem statement presents an incisive description of MIT prevalence signifying the importance of public awareness. Through the conceptual framework, proposals to address MIT are highlighted citing approaches used in South Africa. It also informed the development of the main research objective and research questions that subsequently guided the study's methodology.

### B. The Problem

The increased use and dependence on the Internet has exposed the Kenyan public to unprecedented individual security threats, and of particular interest to this study, cyber threats perpetrated through mobile Internet including mobile malware, identity theft, fraud, data theft (Serianu 2012, p.22). Most of these MIT are premeditated so that if users were aware of how to protect themselves, they would improve their security. The threats bear both financial and social implications on the victims who may not even know where to report the incidents.

Additionally, Kenya has not had a legislative framework to protect its Internet users legally. Therefore, cybercrimes have gone unprosecuted since the introduction of Internet and emergence of cyber threats against Internet users in Kenya (ibid). This is against the backdrop of the provisions to fight cybercrime through the Kenya Information Communication Amendment Act 2009 (ICTA, 2013).

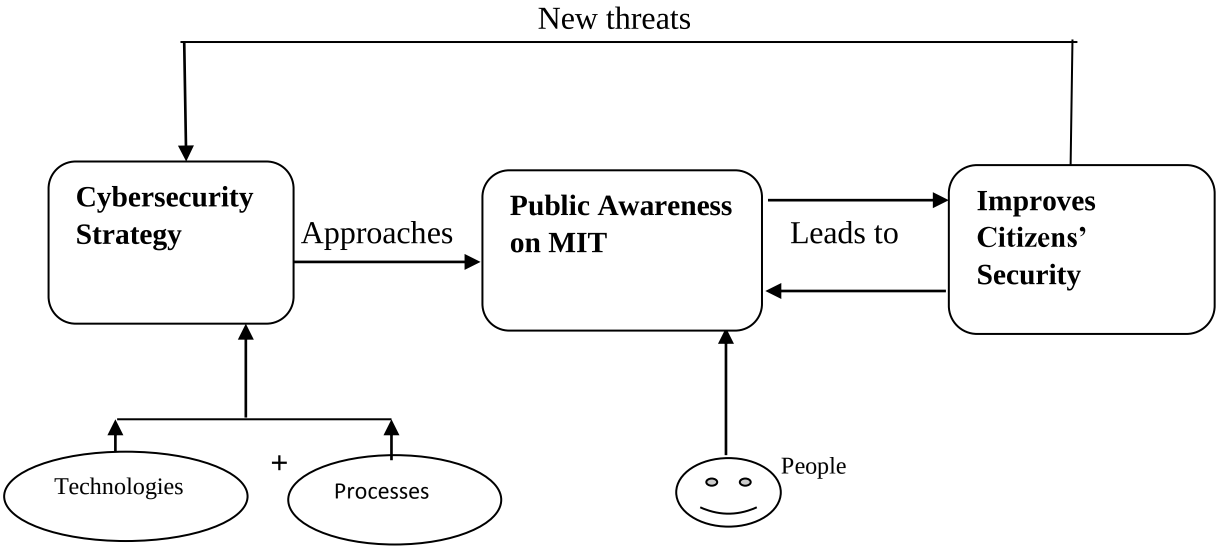
In line with the government's aim to facilitate socio-economic growth through the ICT Master Plan 2007, it is imperative that Kenya's information infrastructure is reasonably secure for her citizens to take advantage of the benefits and opportunities that technology provides. The Cybersecurity strategy, aimed at facilitating socio-economic growth through increased Internet usage, is inconclusive on how government will address mobile Internet insecurity that undermines citizens' security. The strategy is equally silent on the approaches the government will use to raise public awareness on cyber threats when using mobile Internet. It specifically does not state how it will handle prevalent MIT including phishing, malware attacks, identity theft, lack of user awareness, surveillance or user tracking raised in other studies (ENISA 2010, UNDOC 2013, OWASP 2013, Serianu 2012 & 2014, Magutu et al 2011, WolfPack 2012). NIST equally acknowledges that mobile devices such as smartphones and tablets ought to support security objectives including confidentiality, integrity and availability, and therefore need to be secured against threats (2014).

Therefore, against the highlighted evidence of cyber threat growth on the mobile platform, it is incumbent on government to institute continuous awareness campaigns for all sectors of society in its strategy to secure Kenya's cyberspace. This instructed the study to conceptualise a framework that guided the exploration of approaches government could use to raise citizens' cybersecurity awareness on MIT.

**Conceptual Framework**

Mobile Internet use in Kenya is theoretically projected to grow according to CAK's statistics, therefore this study's conceptual framework focused on the cybersecurity awareness approaches that will improve mobile Internet security as illustrated in figure 2;

Figure 2: Conceptual Framework



*Source: Author, 2014.*

The upward trajectory of mobile Internet subscription and the evolving nature of MIT calls for a national cybersecurity strategy that will address threats bedevilling the mobile Internet platform. Andjelkovic argues that Internet policy cannot be separated from the future of mobile communications where the combination of mobile telephony and mobile Internet already comprise the largest communication and distribution network worldwide (2010, p.122). This resonates with Kenya which has high proliferation of mobile Internet-enabled phones and has only just begun implementing a newly developed national security strategy for its cyberspace. With few studies having being conducted on specifically MIT in Kenya, the current study began from the point of exploring the prevalent threats facing users of mobile Internet. Strategy formulation begins from a point of knowledge of the current position of a situation it seeks to address.

Verily, studies have continually suggested that the human factor is the weakest link in the security of information systems, and public awareness and training are primary ways of addressing this problem (Bresz 2004, p.57). Bresz suggests that raising user awareness of various types of malicious software would enable users detect anomalies in normal operations of a system (ibid). Key to this research is Reid and Van Niekerk's study on annual cybersecurity educational campaigns aimed at fostering a cybersecurity culture amongst the youth in South Africa's Nelson Mandela Metropolis (2014, p.174). Their argument that the effectiveness of security solutions consisting of technologies, processes and people depend on whether people use the technologies securely and/or follow the secure procedures (ibid), holds true for Kenya's case as shown in Figure 2. Indisputably, the public is inherently an unconscious threat to security if it lacks knowledge of security practices or is unable to properly apply security knowledge (ibid) exemplifying the significance of fostering a culture of security through awareness initiatives.

Similarly, von Solms and von Solms acknowledge the failure by most African governments to providing any governmental support in attempting to raise the levels of cybersecurity amongst school children which they note is becoming a growing problem (2014, p.186,188). Kenya is mentioned among African nations that lack national cybersecurity awareness and education (ibid). Going by RIA's statistics that revealed 77.8% Kenyans aged 15 years and above access the Internet using their mobile phones (2012), the government should be compelled to adopt an approach that will target different sectors of the Kenyan society in cybersecurity awareness.

Certainly, compared to South Africa which has not yet established its national CERT or CIRT but has national awareness campaigns on cybersecurity (WolfPack 2012, Grobler et al 2010, Reid and Van Niekerk 2014), the Kenyan public needs awareness on the roles of the national KE-CERT and KE-CIRT/CC in mitigating cyber threats and specifically MIT. It is incumbent on the government to educate the public on the importance of continuous reporting of cyber incidents to KE-CIRT/CC as well as to provide information portals publishing up to date cybersecurity guidelines for mobile Internet security.

Therefore through this framework, I argue that there is need to continuously create public awareness on the evolving MIT in a bid to deal with the human factor to improve citizens' security. I predict that if the Cybersecurity strategy does not address how a significant part of the public should be protected while using mobile Internet technology, it undermines the overall aim of the strategy to improve citizens' security.

### C. Main Research Objective

To investigate the approaches the Kenyan government will use, through the new Cybersecurity Strategy, to increase awareness of MIT and consequently improve citizens' security.

### D. Research questions

The study pursued to answer the following research questions derived from the main research objective;

- Has the government considered public awareness drives on cyber threats when using mobile Internet?
- With the emergent and ever evolving nature of threats, which threats does the government envisage to address through public awareness drives and perhaps technologically?
- What measures will the government use to assist the public adapt to the evolving nature of the threats to mobile Internet usage?

### E. Significance of Study

***Academically***

Cyber threat is an emerging global threat and many nations in the international community have developed cybersecurity strategies to counter it and protect their citizens. However, there is currently very scarce data on cybersecurity in Kenya and Africa as a region in the Social and Political Science department, and the Computing Science department. The findings of this study will contribute to this knowledge base. The results of the study can be used in future comparative analyses by countries developing their cybersecurity strategies and have vibrant mobile Internet societies.

***Nationally***

This study is being conducted at a significant time in Kenya when she is launching her Cybersecurity strategy. Its findings will contribute to bridging the identified awareness gap and present its implications and recommendations. CAK statistics on the growth of mobile Internet usage underpins the significance of improving citizens' security on this platform.

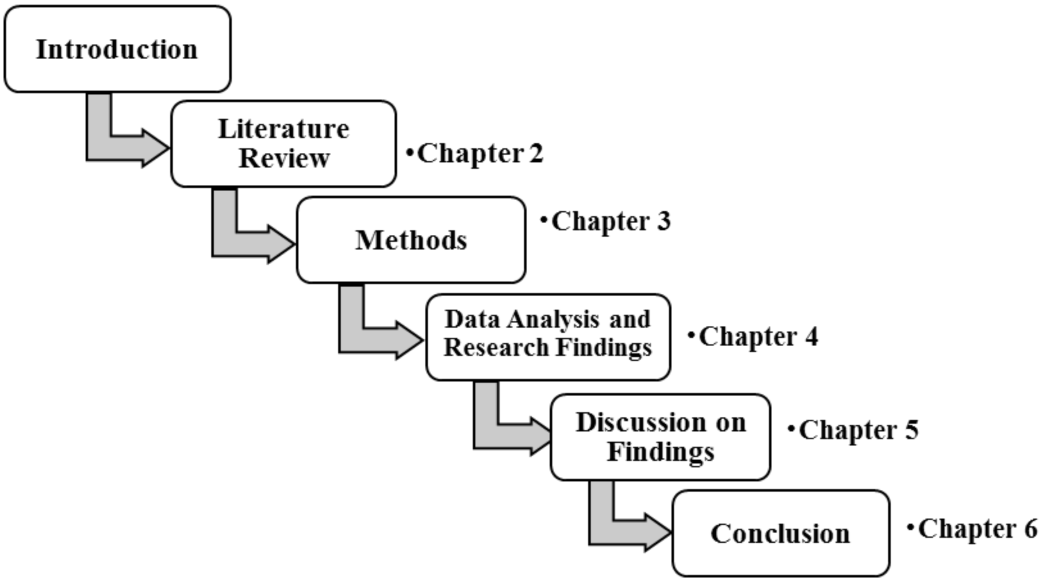
***Regionally***

Results from the study will inform other African nations that are developing their strategies. The study can be used as a comparative analysis for other nations worldwide that have a vibrant mobile Internet sector and are formulating strategies to increase their cyber awareness. This research will also complement the ongoing research and consultative work on AU's Draft Convention on Cybersecurity.

### F. Overview of subsequent chapters

The literature review presents an analysis of global MIT, a comparative analysis of Kenya and South Africa's MIT and approaches used to create awareness on these threats. Data collection, sampling, analysis are discussed in the Methods chapter. A presentation of the survey findings is given in the fourth chapter where an integration approach of analysing both qualitative and quantitative data was used. The discussion reflects on the data collected and compares it to the literature review in view to answering the research questions. Implications, recommendations, suggestions for future research and the limitations of the study are finally presented in the report's conclusion. Figure 3 illustrates the overview;

Figure 3. Overview of Chapters



*Source: Author, 2014.*

# CHAPTER TWO

# LITERATURE REVIEW

## A. Introduction

The legal, technical and institutional challenges posed by cybersecurity are global and far-reaching and can only be addressed through a coherent strategy taking into account the role of different stakeholders and existing initiatives, within a framework of international cooperation. (ITU 2009, p.11). This chapter takes into account ITU's premise and analyses the global threats to mobile Internet in the first section. It further presents a comparative analysis on South Africa and Kenya's MIT and the respective approaches used to create public awareness.

## B. Analysis on global MIT

The number of global mobile Internet subscriptions was reported to stand at 1.2 billion by UNDOC's survey on cybercrime in 2013, a figure that was twice that of fixed lines and projected to grow (2013, p.2). This follows Symantec's 2011 analysis of mobile threats that had noted the growing uptake in smartphones and tables and their increasing connectivity and capability, had a corresponding increase in attention from threat developers and security researchers (2011). According to this report, there was a significant number of vulnerabilities reported by mobile vendors and Symantec's security products that affected mobile devices in 2011.

However, despite the number of immediate MIT being low compared to threats targeting computers, there were new developments in the field (Symantec, 2011). It was projected that as long as malicious code for mobile devices generated revenue for malware developers, there would be more threats created targeting devices used for online transactions such as banking and online shopping (ibid). Symantec's 2014 Internet Security Threat Report confirmed this projection where it reported a significant growth of scams and malware in 2013 (2014, p.6). It states that most malicious codes for mobile devices consist of Trojans posing as legitimate applications that users would download and install from the mobile application marketplaces (2014, p.16).

Further, Symantec posits that when Android allowed smartphone users more freedom to install software from outside their official marketplace, it opened the doors to malware authors and traditional desktop malware began to appear on the mobile platform (2014, p.69).

Phishing pages are being developed for mobile devices with designs that lend themselves to mobile devices such as smaller images and texts (ibid).

The latest ITU's Trend Lab 1Q Security Roundup echoes Symantec's MIT growth projection. It confirms the growing pace of mobile malware and high risk applications that reached two million in the first quarter of 2014 (ITU 2014, p.10). It attributes this growth to the increasing demand for malicious tools and services that can be used to create and distribute mobile malware underground (ibid). Further a vulnerability detected on the Android platform that traps devices in an endless cycle of reboots, rendering them unusable, marked the maturity of current mobile threat landscape (ibid).

Symantec and ITU's findings are resonated by Barlow of IBM who observes that the current trend of security mechanisms of firewalls and intrusion prevention systems are inadequate as the security risk lies in mobile phones applications rather than their operating systems (2014). Mobile phone security should be inbuilt following recent hacking incidents of 100 percent of the top 100 Android apps and just over 50 percent of Apple (ibid).

Barlow's assertions are reinforced by NIST's caution that mobile devices are designed to make it easy to find, acquire, install and use third-party applications thereby posing security risks, especially for mobile device platforms that do not place security restrictions or other limitations on third-party applications (2014). Mobile devices with these features have proliferated mobile markets especially in Kenya that lead to counterfeit phones being shut down (Standard Digital 2013, All Africa 2012).

Likewise, ENISA's Emerging Threat Landscape posits that cyber threats that targeted computers a few years ago have now migrated to mobile computing which has enabled digital convergence and caused a revolution in IT architecture (2013, p.42). It cautions that apart from threats moving to the mobile ecosystem which consists of mobile devices, mobile sensors, mobile security devices, and now part of the Internet architecture and services; cyber criminals are projected to invest heavily in identifying and exploiting new vulnerabilities (ibid).

The top ten threats ENISA reckons as increasingly and specifically targeting mobile computing include; drive-by downloads, worms or Trojans, code injection, exploit kits, botnets, physical damage or theft, identity theft or fraud, phishing, data breach and information leakage (ibid). ENISA cautions that vulnerabilities can be introduced in the applications after bypassing the vetting process of application store vending operators increasing mobile security risks as mentioned in the ITU and Symantecs' analyses.

Despite the Bring Your Own Device (BYOD) trend enhancing employee productivity and maintaining their focus on business activities by allowing them to access their organizations' information assets over privately owned mobile devices, it increases cyber threats such as data loss and information leakage (Renaud and Goucher 2013, p.3). The information leakage occurs through various ways including information being captured on screens using mobile phone cameras without the employees' knowledge (ibid). It can also be leaked through file sharing from web mail where data is stolen by malware application designed to access the secure digital (SD) card on mobiles (Morrow 2012, p.5).

ENISA observes that this developing threat will pave way for cyber criminals to access companies' networks through insecure mobile devices (2014, p.46). Organisations' inability to verify the authenticity of applications on mobile devices that are not under their control but continuously access company data resources, constitute threat to mobile Internet (ENISA 2014, Renaud and Goucher 2013). It is important to note that BYOD will continue to be used as organisations benefit from the trend and are saved money by employees who finance the mobile devices (Renaud and Goucher 2013).

With their significant contribution to big data, mobile devices are capable of revealing useful data such as geo-location, user media behaviour and contact lists which makes them very attractive to cyber criminals (ENISA 2014, p.48). It is prudent to note ENISA's caution of big data in mobile devices being at risk to application developers, operators and wireless providers who can manipulate it without users' consent, a threat echoed by Symantec (2014).

Ruggiero and Foot likewise acknowledge that smartphones and mobile phones with computer capabilities have not kept pace with traditional computer security (2011, p.1). Mobile phones lack technical security measures like firewalls, antivirus, encryption yet their operating systems are not updated as frequently as those in computers (ibid). These shortcomings, which users fail to recognise, make mobile devices highly vulnerable to Internet threats.

Malware written for mobile devices is an increasing threat, mainly for Android and jailbroken iPhones (Morrow 2012, p.6). Malware such as man-in-the-browser (MitB) installed in the Internet browser between websites and users, modifies/alters communication between the two parties without their knowledge. The mobile version of MitB, Man-in-the-Mobile (MitM), works in a similar manner and not only steals online banking information like MitB but also user login and password credentials (p.7).

The threat of mobile malware is also highlighted in McAfee's *2013 Lab Threat Report.* It highlights a significant increase in mobile malware especially on Android platform compared to Apple (2013, p.4). These observations resonate with Symantec and ITU's findings that attributed mobile malware threats to Android malicious applications. McAfee further reveals that a vulnerability known as MasterKey, that allows an attacker to bypass the signature checking of installed applications on nearly all Android devices, had been discovered by computer security researchers (ibid). This vulnerability explains Android's high rate of compromised mobile devices.

Similarly, mobile malware authors continue to concentrate on Android platform due to its high market share of 79.3% of mobile phones and tablets than iOS, Blackberry and Windows platforms (F-Secure Lab 2013, p.4). F-Secure Lab reckons that since mobile platform and tablets have become the more preferred media consumption for most users, mobile malware follows this trend. The deployment of mobile malware to intercept security checks for user credentials and online banking during two factor authentication marks new threat landscape as mobile malware is capable of circumventing extra levels of protection by subverting text messages used for validation (p.7).

Certainly, rogue anti-spyware programs in computers have found their way to mobile devices, for instance *FakeDefender* which does not remove any malware as claimed (F-Secure 2013, p.9). Other MIT reported by F-Secure include backdoors, Trojan, worms, trackware and Adware, as highlighted in Symantec and ENISA mobile threat reports.

Additionally, the growth of virtual currencies market used in cybercrime is attributed to the proliferation of mobile devices (Yankee Group 2013, p.3). This is achieved through mobile owners' fast rate of downloading applications, paying for applications and upgrades, willingness to engage in advertising for free paid applications and digital content (p.6). Arguably, users with more security ready systems irrespective of whether they safeguard themselves or administrators act for them, are more likely to engage in risky behaviours such as downloading undocumented code that increases their perceived utility from experience (Christin et al 2013, p.13). This behaviour is particularly significant because malware developers not only carefully conceal their code from users, but also limit the adverse impact on hosts' systems (ibid).

Finally, UNDOC's global study on cybercrime that underpinned computer technology and Internet as having security risks such as use in criminal activity, acknowledged that the growth of connectivity is inherent to contemporary cybercrime with transnational reach (2013, p.7). The study's findings indicate that African countries reported cybercrime acts to be strongly increasing especially in fraud, forgery, and identity offences (2013, p.7).

The above analysis evidently illustrates the inherent worldwide MIT. There is a clear need for future studies to concentrate on MIT landscape for specific countries where the mobile platform has revolutionised the use of ICTs and is being used to conduct daily online activities.

### C. Comparative Analysis on Kenya and South Africa's MIT Landscape

South Africa, being the only African nation to have published its cybersecurity policy, provides a good benchmark and comparison to Kenya regarding cybersecurity awareness and MIT. The two nations have had similar ICT revolutions and mobile proliferation where mobile network companies provide both data and voice services to citizens with increased Internet bandwidth (IDG Connect 2013, RIA 2012, CAK 2013). In fact, South Africa has been used as a benchmark by OECD in mobile proliferation studies (RIA, 2010) although IDG Connect reports that its Internet penetration remains low at only 14% due to poor information infrastructure. Nevertheless, compared with other polled African nations, Kenya and South Africa reported high mobile Internet usage of 77.8% and 70% respectively (RIA 2012, p.2). Furthermore, being the strongest economies in their respective regions, with GDP's of $350.6 billion and $44.10 billion respectively (World Bank, 2014) South Africa and Kenya therefore offer a good comparison for this study.

World Internet Statistics ranks Kenya fourth in Africa with 12 million Internet users compared to South Africa's 8.5 million Internet users against a population of 43 million and 48.8 million respectively (2012). The statistics point to a high growth of Internet penetration in both countries that experienced IT revolution since the laying of undersea cables. However, with the growing Internet penetration, WolfPack acknowledges that Internet users in Africa are not security-savvy. It attributes this to lack of knowledge, understanding, expertise and awareness that exacerbates the cybercrime predicament (2011, p.24).

Table 2: Kenya and South Africa Internet Statistics

| INTERNET USERS, POPULATION AND FACEBOOK STATISTICS FOR AFRICA 2012 Q2 | | | | | | |
|---|---|---|---|---|---|---|
| AFRICA | Population (2012 Est.) | Internet Users Dec/2000 | Internet Users 30-June-2012 | Penetration (% Population) | Internet % Africa | Facebook 31-Dec-2012 |
| Kenya | 43,013,341 | 200,000 | **12,043,735** | **28.0** | **7.2** | 2,045,900 |
| South Africa | 48,810,427 | 2,400,000 | **8,500,000** | **17.4** | **5.1** | 6,269,600 |

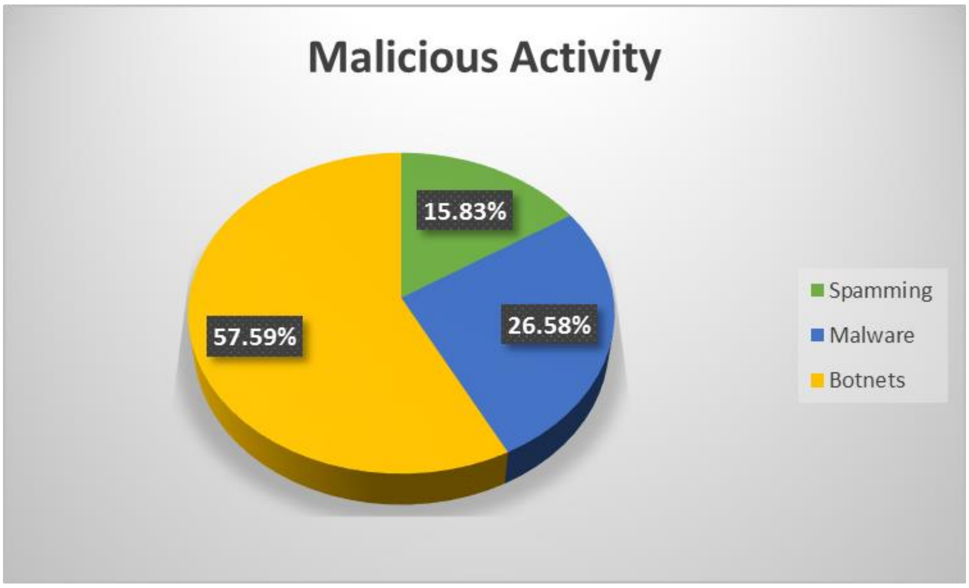
*Source: http://www.internetworldstats.com*

IDG Connect puts Kenya’s MIT landscape into perspective. It brings to the fore the problem of increased public vulnerability to cyber threats attributing it to lack of knowledge, skills and protection to the population accessing the Internet (2013). Projecting Kenya’s development into a wholly mobile Internet structure following IT revolution, availability of affordable smartphones and growth of Internet and social media, IDG Connect affirms that cybercrime poses the greatest challenge to the police and organisations, costing Kenya $36 million per year (ibid). It is worthy to note that 103 Kenyan government websites were hacked by an amateur Indonesian student for fun and practice depicting the ineffective state of security of information systems even at government level (ibid).

On another front, Serianu’s 2012 Kenya Cyber Security report indicates that the threat to mobile phone users has increased with malware authors re-inventing existing malware for mobile devices and also creating mobile-specific malware targeted to distinctive mobile opportunities such as mobile banking (2012, p.22). Its latest study lists eight threats to Kenya’s cyber space including mobile money fraud, online and mobile banking threat, cyber espionage, VOIP PBX fraud, denial of service attacks, social media, insider threats and botnet attacks that target individuals, organisations and critical infrastructure (Serianu 2014, p.12).

The growing threat on mobile money fraud and mobile banking depicts an upward trajectory which Serianu attributes to financial institutions’ trend of introducing vulnerable web and mobile applications that lack strong encryption and are susceptible to phishing attacks (2014, p.12). From its sample of thirty-three online banking applications, only two banking portals had adequate online security deployed on their web application (ibid).

Figure 4: Malicious Activity in Kenya



*Source: Serianu, 2014.*

Botnet is the greatest threat on Kenya's cyber space reported to have increased by 100% from 900,000 events for the period ending December 2012 to 1,800,000 events in 2013 (Serianu 2014, p.12) depicted by Figure 5. Kenya's lack of cybercrime legislation to prosecute and deter cyber criminals calls our attention to Christin et al's study that explored the perspective of botnet operators who the authors argue associate risks of hosting bot operations to countries that have ambiguous or non-existent cybercrime laws (2011, p.3).

Statistics from Serianu further indicate that Kenya ranks second after Germany for top attacking IP addresses in the world where these IPs not only perform regular wide spread host scans of popular ports but also other malicious activity including brute force attacks and exploit attempts (2014, p.15). At this point, it is important to remember that mobile network providers have the highest Internet subscribers according to CAK statistics as shown in Table 3 (2014, p.23).

Table 3: Mobile Internet Market Share

| **Name of Operator** | **December 2013** | **% Market Share** |
|---|---|---|
| **Safaricom Limited Kenya** | 9,637,828 | 73.6 |
| **Airtel Networks Kenya Limited** | 1,945,152 | 14.9 |
| **Telkom Kenya Limited (Orange)** | 904,739 | 6.9 |
| **Essar Telcom Kenya Limited** | 602,629 | 4.6 |

*Source: CAK, 2014.*

Serianu's detection of high botnet activity and spamming in Kenya's ISP's (2013, p.20) calls our attention to CAK's statistics that one of the mobile network providers Safaricom Limited, is the 5th largest ISP in the country controlling a 7.2% market share of fixed line and wireless Internet subscriptions (2013, p.24). Certainly, the Internet threat landscape cuts across all Internet users.

Similarly, Symantec Internet Threat report ranked malicious code and phishing as Kenya's most common cyber threats (2013). For the threat of malicious code, Kenya ranked 70th in the world and 10th in Africa, while for hosting phishing websites she is ranked 5th in Africa (ibid). This is besides the fact that Kenya has an established KE-CIRT, which the national cybersecurity strategy is indistinct on its role in mitigating MIT.

Comparatively, South Africa has high mobile penetration of 84.2% and 70.6% mobile Internet access (RIA 2012, p.1-2) but lacks proper communication infrastructure and communication speeds even with the presence of undersea broadband cables (IDG Connect 2013). Interestingly, South Africa has a low number of Internet users, 14% of total population, but ranks 7th in the world for cybercrime (ibid). Symantec ranks South Africa 1st in top ten African nations for cybercrime, phishing and virus, 3rd in spamming (2013, p.10). There also is a skills shortage and exposure to IT among a large portion of the population which is likely to pose a cyber risk when accessing the Internet (IDG Connect, 2013).

Likewise, WolfPack's security report on South Africa adduce that the most common cybercrime act in South Africa is online fraud, including economic fraud and theft of confidential information (2013, p.7). Its investigation puts South Africa's cyber threat landscape into perspective analysing it in four dimensions including cyber threats against

South Africa as a country, government, finance and telecommunication sectors. Of particular interest to the current study are the findings of the telecommunications sector where data theft, loss and falsification of documents are of critical concern.

The propagation of malware through mobile devices, social networks and web navigation has increased the rate of cybercrime following the increased use of mobile phones. (WolfPack 2012, p.35). Further, the combination of social networks and mobile devices plays a significant role in aiding Internet related fraud through mobile malware that have been detected in information theft or espionage attacks (ibid). WolfPack reports that SIM cloning, where cyber criminals attempt to intercept communications between online bank and the target are on the increase. Identity theft is also reported to be an increasing threat in this sector where abuse of identity forms the basis of occupational fraud and cybercrime (ibid). Finally, it was noted that there is a huge shortage of skilled resources for the development of secure applications with most applications being developed without security features (ibid).

Therefore, the comparative analysis clearly delineates the gap existing in documenting MIT in Kenya as WolfPack reports for South Africa. Contextually, CAK reports Kenya's fast growth in mobile penetration and mobile Internet subscription but it does not provide information on the threats inherent this platform that can inform awareness initiatives and security policy making. Although Serianu's latest report acts as a pointer it lacks adequate information on specific MIT for instance the mobile malware type affecting mobile banking, fraud mobile applications for social networks it acknowledges as threats.

### D. Thoughts on Awareness Approaches for MIT

ITU observes deterring cybercrime as an integral component of a national cybersecurity and critical information infrastructure protection strategy (2009, p.12) and this exemplifies the role of cybersecurity strategies to citizens' security. It posits that specific strategies of cybersecurity such as development of technical protection systems or educating users to prevent them from falling victim to cybercrime can help to reduce the risk of cybercrime (ibid).

In this regard, ITU advocates for the protection of customers, firms and Internet-based services but warns that weak protection measures in developing countries increase difficulties in promoting e-business and participation in online service industries (2009, p.16).

### *ITU on Capacity Building and User Education*

ITU affirms certain cybercrimes such as those related to fraud for instance phishing and spoofing, are not attributed to lack of technical protection but rather to lack of awareness by victims (2009, p.86). It further cautions that a user protection strategy that focuses only on the software products has limited ability to protect users. The continuous development and updates of technical protection measures are arguably insufficient substitutes to other approaches such as user education (ibid). For instance, ITU posits that when users are aware that their financial institutions would never contact them by e-mail requesting passwords or bank account details, their chances of falling victim to phishing or identity fraud attacks would be minimal. Therefore, ITU suggests ways through which user awareness can be raised to reduce the number of potential targets including;

- Public campaigns
- Lessons in schools, libraries, IT centres and universities
- Through public private partnerships (PPP).

Additionally, one of the key requirements of an efficient education and information strategy is open communication of the latest cybercrime threats (ibid). ITU recommends the collection and publication of relevant information to determine threat levels as a way to informing users. However, some states and private businesses refuse to acknowledge that their citizens and clients respectively are affected by cybercrime threats, so as to protect themselves from losing trust in online communication services (2009, p.87).

### *South Africa's Awareness Approaches*

Through its Cybersecurity Policy, the South African government affirms its commitment to raise awareness on cyber threats but it does not explicitly state the approaches it will use to meet this objective (Cybersecurity Policy, 2010).

However, in a proposal for a Cyber Security Awareness Toolkit for national security (CyberSAT), Phalomolakha et al argue from a philosophical position that the fundamental premise on which cyber security policies are developed is an absolute necessity (2011, p.9). They posit that since cyberspace is a socially constructed, man-made space, crosscutting social dimension of national power any cybersecurity awareness initiative must acknowledge that no full-proof technological protection is possible in a socially constructed space (ibid). They theorize that the holistic approach to cybersecurity policy that South Africa is looking for, is likely to be enhanced by this philosophical position and understanding confined to the economic, political, military, psychological and informational dimensions.

The establishment of a functional national Computer Security Incident Response Team (CSIRT) in South Africa was identified as a major concern in the WolfPack report where the business industry is reported to be planning to institute a private CSIRT if the South African government fails to establish the national CSIRT (2012, p.7). The report proposes the need to establish sector CSIRTs that are not duplicated but are sustainable (2012, p.47). It further urges the South African government to initiate continuous cybersecurity awareness all year round and the department of education to include it in the education curriculum.

This call was heeded by Reid and Van Niekerk's annual education campaigns since 2011, that aim to effectively and measurably educate South Africa's youth about cyber issues (2014 p.177). Topics such as online activities, cyber citizenship, cybercrime, social networking, password and hardware security, viruses, malware, cyber bullying, cyber identity management among others are covered through the education part of the campaign (ibid). A poster contest follows thereafter to measure the campaign's impact on the involved youth's awareness levels. They voluntarily create and submit hand-crafted or digitally-created posters promoting awareness of the campaign's covered security issues (ibid). Needful to say, the campaigns have recorded improved youth participation, cybersecurity awareness and inclusion of teachers who positively impacted on the study. Reid and Van Niekerk also recommend an interdisciplinary approach where cybersecurity experts determine what users are taught and other experts such as teachers craft how the message will be delivered (p.183).

Meanwhile, in an attempt to empower African school teachers to educate children on cybersecurity, von Solms and von Solms created a video-based syllabus to teach children how to protect themselves when exploring the Internet subsequently developing a cybersecurity culture (2014, p.186). They propose utilisation of open education resources on cyber topics to empower teachers to educate children on using cyber space safely (ibid). Through a search of e-safety children videos on YouTube, the authors liaised with teachers to analyse the most suitable videos and made three distinct video-based cybersecurity syllabuses for African children in three different age groups between ages 7 and 13 (ibid). Clearly, it highlights the importance of developing a national cybersecurity culture and involving teachers in creating awareness messages for the youth and children.

Additionally, privately run initiatives such as Cellphone Safety managed by independent non-commercial institutions, support cybersecurity awareness drives in South Africa. The initiative runs cellphonesafety.co.za that helps parents to keep their children's mobile phones and tablets safer by giving safety tips ranging from usage, to how to block pornographic content from their children's devices. Cybercrime.co.za equally serves as an awareness portal aimed at educating individuals on criminal exploitation of ICTs in South Africa and the rest of Africa (2014).

Similarly, scholars indicate that there are a number of cybersecurity awareness programmes aimed at educating users groups in different geographical parts of South Africa necessitated by increased rate of bandwidth consumption in the country (Grobler et al 2012, p.4). Research studies that have been conducted in parts of South Africa have indicated the level of awareness and user online behaviour as having increased among the citizens (ibid).

### *Kenya's ICTA's Awareness Initiative*

This study recognises the new partnership between ICTA and the University of Nairobi's C4DLab in offering quarterly training to IT professionals in government and private sector interested to learn more about information security (ICTA 2014, C4DLab 2014). The institutions aim to develop a community of experts who will understand and counter cyber threats, and prepare cyber strategies for their organisations. This initiative is promising being the first of its kind in Kenya albeit a high training fee of Kenyan shillings 50,000 (£335) for each self-sponsoring participant (ibid). It is important to note that as the training is targeting IT professionals only, it is insufficient in creating a comprehensive public awareness required for MIT. This study therefore instructively argues for the requirement of a national awareness program targeting all sectors of society on MIT to sustain ICTA's initiative.

### *Role of KE-CIRT/CC on Mobile Internet Security*

CAK is mandated by the Kenya Communications Act 1998 to establish a national cyber security management framework that creates the National Kenya Computer Incident Response Team Coordination Centre[8] (KE-CIRT) to coordinate response and manage cyber security incidents nationally (CAK, 2014). Aside from acting as Kenya's national cybersecurity trusted point of contact for information security matters, KE-CIRT/CC's other functions include;

[8] http://www.ke-cirt.go.ke/index.php/about-us/

- Offering advisories on Cybersecurity matters and coordinating cyber incident response in collaboration with relevant actors locally, regionally and internationally.
- Gathering and disseminating technical information on computer security incidents.
- Carrying out research and analysis on computer security.
- Capacity building in information security and creating and maintaining awareness on cybersecurity-related activities (ibid).

The study acknowledges CAK's action features for cyber incident handling including reporting of incidents and vulnerabilities. Its resources on security tips for non-technical computer users range from child bullying, safe use of social networks to general cyber security guidelines are welcome. However, there is a gap for guidelines on mobile Internet safety use or threats.

Nonetheless, it is prudent to appreciate the efforts of ICTA and CAK through KE-CIRT/CC's resources to improve cybersecurity. It is however incumbent on the government to create a comprehensive national awareness campaign through continuous drives targeting all sectors of society on MIT to help in improving overall cybersecurity.

Evidently, both governments of South Africa and Kenya need to respond directly to the mobile Internet security challenge in their cyberspaces. However, despite having a vibrant mobile Internet society and a resourceful KE-CIRT/CC, Kenya's elements of awareness on MIT and general cyber threats do not compare favourably with South Africa's various approaches. There are various aspects Kenya can learn from South Africa's cybersecurity education campaigns that focus on the youth and the information portals. It is also expected that the findings from the survey will inform the government of the threats considered prevalent to Kenyan mobile Internet users to guide approaches it may deploy to create awareness on MIT.

# CHAPTER THREE

# METHODS

## A. Introduction

This study explored the approaches the Kenyan government would use to create public awareness on MIT. This section discusses the study design, setting of study, sampling, response rate, research instruments and analysis procedure used in the data collection for the research.

## B. Study Design

It was proposed to use case study and cross-sectional research designs to give an in-depth examination of approaches the Kenya government should use to raise public awareness of MIT. Comparative analyses were conducted on South Africa and Kenya's MIT landscape as well as approaches used in both nations to create awareness of these threats.

The cross-sectional research design was to primarily collect survey data from a cross-section of key stakeholders of ICT in Kenya. These stakeholders were enlisted to a listserv; the Kenya ICT Action Network (KICTANet) and initial contact was made to the administrator seeking consent of the members' participation.

## C. Setting of study

KICTANet is a multi-stakeholder ICT policy discussion forum comprised of 758 members representing 38 ICT stakeholder groups from the civil society, public and private sectors, academia, development partners and media (KICTANet, 2007). It was established as a project funded by the UK Department of International Development (DFID) to speed up development of an ICT policy in Kenya. KICTANet's main goal is to act as a catalyst for reform in the ICT sector in support of the government's mission to enable Kenyans gain maximum benefit from the opportunity offered by ICTs (ibid).

Its roles include acting as a platform for information exchange, catalyst for change, policy shaper and development, ICT standardisation, monitoring and evaluating ICT initiatives (ibid). The forum is administered by three members who manage the discussions and membership subscriptions.

### D. Sampling

The study targeted KICTANet's population of 758 members whose response was stratified into six groups forming the study's sample size. The six strata included public sector, private sector, media, academia, development partners and civil society. Bryman argues that stratifying the population of a study by criterion ensures that members are equally represented in terms of their groups (2012, p.192). Since the researcher was not aware of the distribution of each strata that make up the 758 total membership, six sets of different numbers randomly generated by Research Randomizer were selected to represent the sample that was analysed. This reduced the sampling bias as all the members had an equal chance to be selected for analysis.

### E. Research Instruments

An online social survey method was used, and in particular, web survey. Bryman acknowledges that there has been a considerable growth in the number of surveys administered online (2012). He argues that they tend to have faster response than postal questionnaires and are not constrained to geographic coverage. Additionally, Bryman asserts that online surveys offer better response to open questions with more details and accuracy due to automated data entry. However, they suffer from low response rate compared to postal questionnaires and participants need to be motivated as they need to be online to answer the questionnaire especially if they have to pay for Internet connection (ibid).

The Survey Monkey tool was used to develop, administer questionnaires and collect the responses. The filled questionnaires were stored in Survey Monkey's database which the researcher retrieved for analysis. Survey Monkey does not allow changes of responses by researchers which guaranteed reliability and validity of the data collected.

### F. Ethical Issues

The study argues that the Internet is in the realm of public sphere; however, the researcher contacted participants through the forum's administrator seeking their participation. As the link was sent to the listserv where the participants could access if they wished to participate, their confidentiality and anonymity was upheld. A plain language statement was attached to the questionnaire link and participants consent was by way of return of the survey. Respondents did not indicate their names or any personal data that would identify them and they were at liberty to withdraw from the survey at any point.

## G. Analysis of data

A mixed method approach was used to analyse the data. Survey Monkey tool has an analysis feature which the researcher used to statistically analyse the demographic data. NVivo was used to code and analyse the textual data through themes that were identified. Bryman suggests NVivo is an effective tool to analyse qualitative data thematically (2012, p.581). In a bid to reduce sampling bias, the data was grouped into six strata representing all the responses received. Six sets of distinct numbers were created by Research Randomizer with a range of 1-17. Responses were picked according to the numbers in each set forming the sample for analysis.

## H. Presentation of Findings

The results are presented using an integrated approach of quantitative and qualitative analyses through charts, tables and textual analysis in the findings chapter.

# CHAPTER FOUR

# DATA ANALYSIS AND RESEARCH FINDINGS

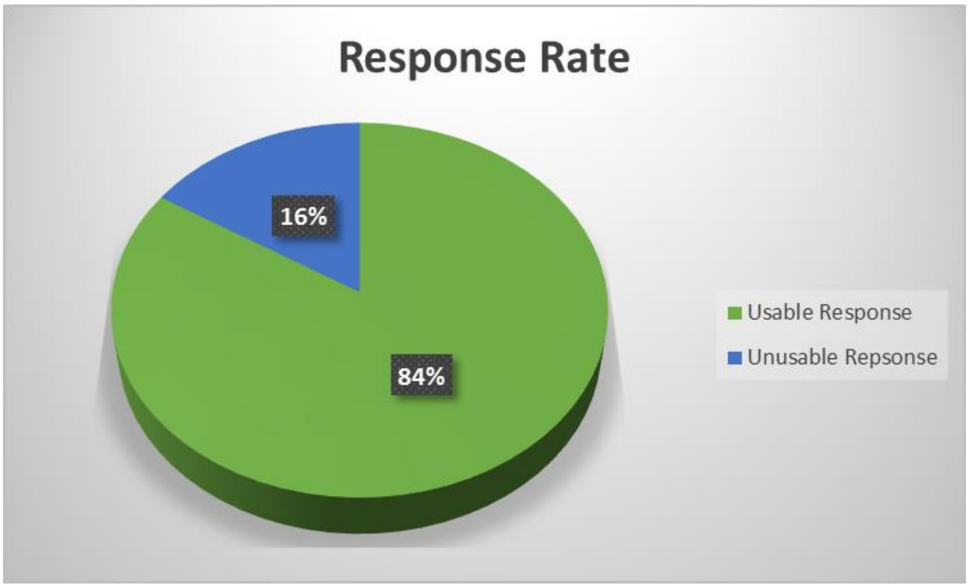
## A. Introduction

The study aimed at investigating the approaches the Kenyan government would use to create public awareness on MIT through the Cybersecurity strategy. This chapter presents the findings of a survey conducted to find out these approaches. An integrated approach of both quantitative and qualitative methods was used to analyse the data. Charts, tables and figures were used to graphically illustrate the data while a thematic analysis was employed on the textual data, and the themes are presented here.

## B. Response Rate

The study's sample size for analysis consisted of 58 responses drawn from KICTANet's listserv from which a response rate was calculated using Bryman's formula (2014, p.199) as illustrated below:

Figure 5: Response Rate



*Source: Author, 2014.*

The 58 responses were categorised into six strata but 5 respondents skipped the question requiring them to indicate the sector which they belonged to. Therefore, as the 5 responses could not be grouped in any stratum, they were added to the unusable questionnaires that totalled to 8 responses. The unusable questionnaires included those that participants only filled their demographic data. The remaining 49 stratified responses represent 84% of the study's sample size with the highest participation coming from the public sector. This was considered representative of the sample size. Table 3 illustrates this further;

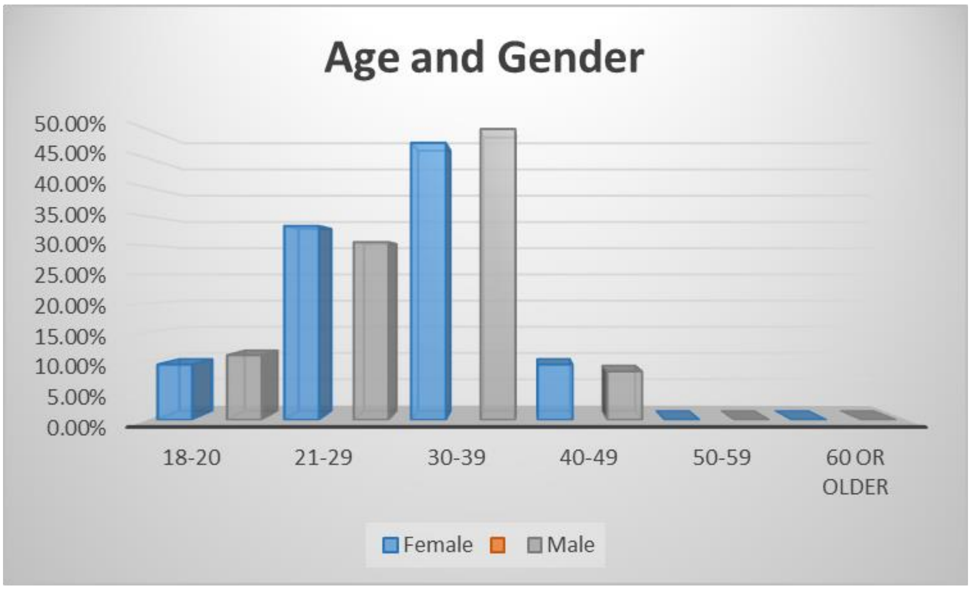
Table 3: Stratified Response

| Strata | Stratified Sample | Stratified Response |
|---|---|---|
| **Public service** | 19 | 17 |
| **Private sector** | 10 | 9 |
| **Civil society** | 4 | 4 |
| **Academia** | 14 | 13 |
| **Development partner** | 1 | 1 |
| **Media** | 5 | 5 |
| **Total stratified sample analysed** | **53** | **49** |

*Source: Author, 2014.*

There were more male participants in the valid responses of the sample with a 54% rate in the 30-39 age bracket, while females in the same category represented 40% as shown in Figure 7. The participants were at liberty to withdraw from the survey at any point and it is important to highlight that this affected responses from both gender whose responses were incomplete.

Figure 6: Age and Gender Distribution of Valid Response



*Source: Author, 2014.*

In a bid to investigate the participants' awareness of the cybersecurity strategy, the survey required them to state if they had access to and had read the strategy document. More participants with high school, tertiary college and graduate education had low access to the strategy compared to the postgraduates as shown in table 4. It suggests that Kenya's public access to documents is likely to be influenced by level of education.

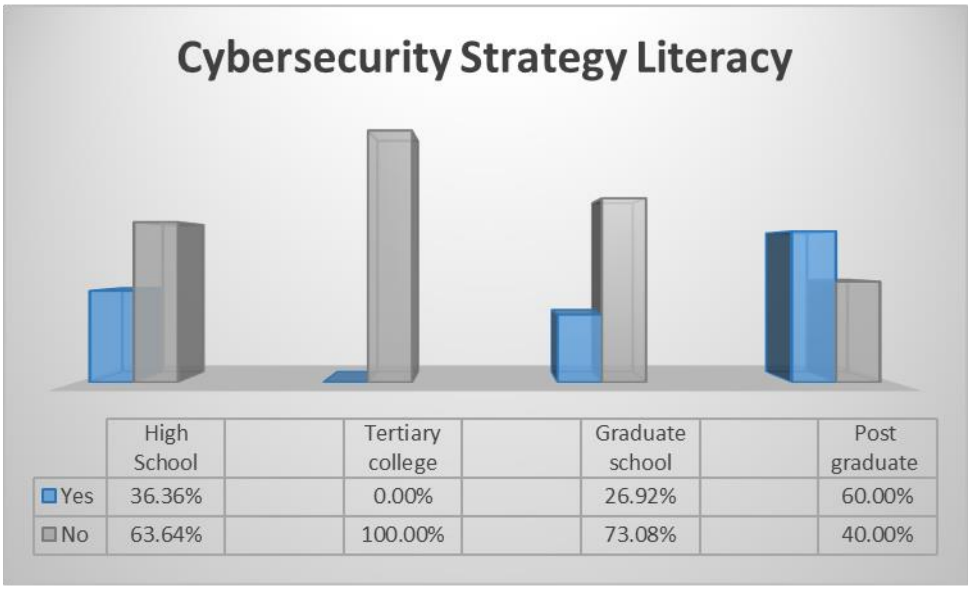
Table 4: Access to Cybersecurity Strategy document

| Education level | Access to Strategy | No access to Strategy |
|---|---|---|
| **High school** | 36% | 64% |
| **Tertiary college** | 25% | 75% |
| **Graduate** | 38% | 62% |
| **Postgraduate** | 70% | 30% |

*Source: Author, 2014.*

A closer analysis of the data reveals that more postgraduate participants had read the strategy document with none of the tertiary college participants having read it as indicated in Figure 8. It is instructive to state that access to the strategy and level of education influence literacy of the strategy document, signifying the need to target all Kenyans through national awareness drives.

Figure 7: Participants who have read the strategy document



*Source: Author, 2014.*

Worthy to note from the data, 98% of the respondents indicated that they have an Internet-enabled mobile phone of which 75% use it to access the Internet very often as shown in Table 5. Only 1.92% reported not to own an Internet-enabled mobile phone and therefore do not use it all to access the Internet. The data confirms the high mobile Internet proliferation among the Kenyan public which requires awareness drives for MIT**.**

**Table 5: Mobile Internet Usage**

| **Internet Mobile Phone** | **Use very often** | **Use often** | **Not often** | **Not at all** |
|---|---|---|---|---|
| **Yes (98.0%)** | 75% | 25% | 0 | 0 |
| **No (1.92%)** | 0 | 0 | 0 | 100% |

*Source: Author, 2014*

### C. MIT Data Analysis

It is informative for the study to present an analysis of the findings of MIT that participants indicated as prevalent when using mobile Internet in a bid to justify the significance of the approaches suggested to create awareness on threats. In exploring the results, Table 6 illustrates the two major themes of MIT that were identified; technical and non-technical.

Table 6: MIT Analysis

| MIT Type | Number of Entries | Percentage Response |
|---|---|---|
| **Technical** | 28 | 57% |
| **Non-technical** | 21 | 43% |

*Source: Author, 2014.*

The findings suggest that technical MIT are the most commonly experienced by participants, rated at 57%. These threats include hacking, mobile banking fraud, malware attacks, adware, spam, phishing, identity theft, fake third-party applications, cybercrime, botnet attacks, cyber espionage and insider threats. The non-technical MIT that rated 43% include use of mobile Internet to spread hate messages, cyber bullying, negligence of mobile network providers to register Internet subscribers, limited capacity of police force to combat cybercrime, terrorism threats, obscene content, inadequate legislation to fight cybercrime and hackers, infringement of privacy, low IT literacy, social engineering attacks, social network attacks and personal data breaches.

Upon analysing the two themes further, there was evidence indicating lack of public awareness on how to detect and avert both technical and non-technical MIT amplifying their success rate. Verily, there was a suggestion that the public is unaware on how to protect itself while using mobile Internet technology. Moreover, accusations against mobile network providers' negligence to monitoring their networks and applications were raised. Some participants submitted that mobile network providers need to provide mobile Internet users with updates to detect and manage MIT. This demonstrates that users do not know how to detect threats and protect themselves.

By the same token, the civil society participants posited that the government has not invested adequately on data protection thus allowing advancements in technology to augment public unawareness on security measures. Additionally, a cross section of participants from the public and private sectors argued that incapacity of law enforcement and inability to prosecute cyber criminals contribute to the success rate of MIT. There were concerns from the academia and development partners that legal loopholes and the ever evolving nature of new attacks contribute to MIT with the public lacking protection and coping skills. Participants from the media and development partners posited that mobile Internet users did not understand the link between cybersecurity and access to the Internet using their mobile phones, subsequently heightening the vulnerability. The themes underscore the apparent lack of and requirement for public awareness on prevalent MIT to help improve users' security.

### D. Suggestions on Addressing MIT

***With the emergent and ever evolving nature of threats, which threats does the government envisage to address through public awareness drives and perhaps technologically?***

In exploring the research question on MIT the government envisages to address through public awareness drives and perhaps technologically, three main themes were identified including public awareness, technology and law enforcement. As aforementioned, MIT were thematically grouped into technical and non-technical. Table 7 suggests that public awareness drives is the preferred approach to addressing both technical and non-technical MIT however, a body of evidence indicates that technical means cannot be disregarded.

Table 7: Approaches to Address MIT

| **Approach** | **Responses** |
|---|---|
| **Public awareness** | 62.79% |
| **Technologically** | 20.93% |
| **Law enforcement** | 16.28% |
| **Total** | 100% |

*Source: Author, 2014.*

The proponents of public awareness particularly from private sector, media and academia posited that empowering people with knowledge and basic skills such as password design and social networking safety practices would support users in improving mobile Internet security. This confirms that users do not understand what is required to protect themselves while using mobile Internet. Likewise, their disclosure of public lacking understanding of the dangers of insecure Internet practices such as downloading third-party applications, logging onto dangerous sites and releasing personal information through social engineering tactics confirms the awareness requirement.

Verily, the suggestion of using technical means to address MIT was accompanied by calls for government to invest in technology that would support public awareness programs. Specifically, the civil society and private sector proposed that government should protect information infrastructure through technical means to ensure Kenya’s cyber space is reasonably secure for both communication and business transactions. They further adduced the need for government to engage mobile network providers when implementing tailored technologies to protect mobile Internet users without infringing on their privacy rights. However, the public sector countered that technology alone would neither increase awareness nor reduce MIT if there is low public IT knowledge on the very technology. They proposed the need for public education and training on reasonably secure technology.

The third theme of using law enforcement was proposed by all participants as a way to reinforce public awareness initiatives and address MIT. The participants argued that the public lacked awareness not only on measures to protect itself from MIT but also the laws that fight the threats. The private sector participants were particular to propose government initiatives to educate both the public and police on laws that fight cybercrime and consequences of violating extant laws on cybercrime, mobile money fraud and spreading of hate speech using mobile Internet. The three themes clearly delineate the requirement of an interwoven yet tailored approach that addresses different societal needs on MIT.

### E. Thoughts on Public Awareness Drives on MIT

***Has the government considered public awareness drives on cyber threats when using mobile Internet?***

Results on the questions that sought participants’ thoughts on public awareness drives when using mobile Internet discerned four themes of awareness drives that the government should use to sensitize the public on MIT.

Table 8: Public Awareness Drives on MIT

| **Public Awareness Drives** | **Response** |
|---|---|
| **Media campaigns** | 52% |
| **Public forums** | 24% |
| **Education curriculum** | 13% |
| **Mobile Network Providers** | 11% |
| **Total** | 100% |

*Source: Author, 2014.*

As Table 8 illustrates, media campaigns were the most preferred public awareness drives that the government should use to create awareness on MIT with 52% of the participants proposing them. The media campaigns recommended include print, electronic and social media networks. Specifically, the participants suggested public communication on the threats through radio and television shows and documentaries, newspapers supplements and social media platforms such as Twitter and Facebook. They also proposed using promotional advertisements through radio and television to teach the public MIT detection and coping skills.

Public forums such as community gatherings, public conferences, road shows and use of Provincial Administration to educate the public on MIT were suggested by 24% of the respondents. Educating the police force on specifically MIT and the laws that fight them was mentioned as critical in reinforcing public awareness drives on the threats.

Another 13% response proposed introducing cybersecurity lessons in the education curriculum of primary schools through to universities where threats on mobile and computer Internet would be taught to the youth. The development partner participant particularly argued that as the youth are increasingly owning mobile Internet-enabled phones, educating them on threats like cyber bullying would develop effective online security practices from an early age.

The use of text alert system where mobile network providers would send information on threats to their subscribers was proposed by an 11% response. There was suggestion that the government should be the link between education institutions and mobile network providers to ensure provision of reasonably secure mobile Internet networks for the online-active youth.

### F. Government's Public Support Programs to Adapt to MIT

***What measures will the government use to assist the public adapt to the evolving nature of the threats to mobile internet?***

In exploring the research question on how the government should assist the public to adapt to the evolving nature of MIT, three themes were identified namely; training and education, information portal and help desk. They were exemplified through respondents' submissions on programs the government should develop to support the public in adapting to the evolving nature of MIT, reporting MIT and accessing information to MIT.

Table 9: Public Support Programs on MIT

| **Public Support Program** | **Response** |
|---|---|
| **Training and education** | 51% |
| **Information Portal** | 27% |
| **Help Desk** | 22% |
| **Total** | 100% |

*Source: Author, 2014.*

As Table 9 illustrates, majority of participants require the government to establish training and education programs to support the public adapt to the evolving nature of MIT. They specifically proposed national awareness drives through media campaigns such as radio, television, newspapers, billboards and pamphlets. Use of expert groups on cybersecurity and liaisons with the academia to educate the public on MIT were also indicated as efforts that would increase public awareness. Additionally, the participants reiterated the need to include lessons on MIT and safety practices in the education curriculum to teach the youth on overall cybersecurity.

The establishment of information portals was a theme identified from participants' proposals to develop platforms where the public can access information on MIT. The private and public sectors principally suggested publicising KE-CIRT/CC's role as an information portal. They argued that as public is not aware of KE-CIRT/CC's role, it would not know where to access threat information. CAK and the police's Criminal Investigation Department (CID) were also mentioned as important government bodies that need to establish information portals on MIT and avail them online for the public. Similarly, the civil society required the government to conduct surveys on cyber threats including MIT, publish quarterly threat reports and avail them to the public. The participants also submitted the development of information portals on MIT in Huduma Centres[9] across the country to avail threat information to all users of mobile Internet that access these centres for government services.

The theme of help desks was exemplified in suggestions of establishing toll free lines available at all times for the public to report incidences of MIT. The participants require that the police should create help desks to deal with MIT especially at the CID.  While participants submitted the requirement of KE-CIRT/CC to establish a help line for reporting computer threat incidences that would inform appropriate response on the threats, the study confirms that there is a help line for this purpose. This demonstrates the need to publicise KE-CIRT/CC's functions. Moreover, participants highlighted the requirement of ISPs and mobile network providers to alert mobile Internet users on any threats on their networks, how to detect and prevent/manage them. They indicated the use of text message alerts on mobile phones would be fast and convenient. It was also proposed that CAK, should create its own help desk where the public would access information to assist in detection and prevention of MIT.

The study went further to inquire how the aforementioned government roles in addressing MIT through public awareness can be reflected in the Cybersecurity strategy. Succinctly, there was requirement for the government to take the lead role in public education and training programs and have an action plan in the strategy. The government was required to reflect the following in its strategy;

- Information on major MIT, public access to this information and government proposals to deal with them;
- Establishment of private-public sector engagement to increase awareness on MIT;
- Police empowerment on MIT and specific laws on MIT;

[9] http://www.hudumakenya.go.ke/?about-us.php

- Cybersecurity response team to offer MIT intelligence analyses to the public.

Finally, the participants pointed out the need for the government to create awareness on the importance of the cybersecurity strategy in securing Kenya's cyber space.

It is instructive to mention that the themes identified in the findings confirm the requirement of public awareness on various aspects that would support the public to detect, prevent and/or manage MIT. A more incisive discussion of the findings is presented in the next chapter.

# CHAPTER FIVE

# DISCUSSION ON FINDINGS

## A. Introduction

This research study pursued to investigate approaches the Kenyan government would use to improve public awareness on MIT. The discussion presented here reflects on the study's key findings with reference to the literature review in a bid to answering the research questions.

## B. Response Rate

The striking finding in this section was that education level influenced public access and literacy of the strategy document with postgraduates reporting the highest rate in both instances. This calls the study's attention to ICTA and C4DLab's partnership that trains IT professionals on cybersecurity and is echoed by Schneier's argument that training security developers expertise in a fast-changing environment increases a system's overall security (2014, p.152). Reid and Van Niekerk's study however proposes a different approach (2014).

The results on respondents' mobile Internet usage that confirmed statistics by RIA 2012 Survey, IDG Connect (2013) and CAK (2014) on Kenya's mobile Internet penetration, support the study's requirement to institute measures to support the growing number of mobile Internet users adapt to threats targeting this platform.

## C. Analysis of Kenya's MIT

It was informative for the study to begin from a point of knowledge on threats prevalent on mobile Internet platform where the identified themes confirmed the MIT analyses reviewed in the literature. The technical threats including malware attacks, identity theft, phishing, botnet attacks, mobile banking fraud, malicious third-party applications, were posited as growing MIT by Symantec's 2014 Internet Security Threat Report, McAfee's 2013 Lab Threat Report, ENISA's 2013 top ten mobile threats, NIST 2014, F-Secure's 2013 Lab Report, and Serianu's 2014 Kenya Cybersecurity Report. Equally so, the non-technical threats including low IT literacy, data breaches, legal loopholes, limited police capacity to fight cybercrime were highlighted by IDG Connect (2013), Serianu (2012, 2014) and Magutu et al (2011) as prevalent in Kenya.

Evidently, Kenya's MIT analysis confirms ENISA's 2013 and Symantec's 2014 reports that computer threats have moved to the mobile platform. It also confirms that these studies can be usefully employed to extend our understanding of Kenya's MIT landscape. The analysis would therefore be useful to government when designing the approaches to improve public awareness on threat detection and coping skills.

### D. Suggestions on Addressing MIT

*With the emergent and ever evolving nature of threats, which threats does the government envisage to address through public awareness drives and perhaps technologically?*

The thematic analysis derived from exploring the survey results on suggestions to address MIT helped to explain the correlation of three approaches that were identified. Public awareness was the most favoured where participants proposed empowering the public with knowledge and basic cybersecurity skills in a bid to improve MIT detection and coping skills. IDG Connect specifically attributes cyber threats in Kenya to lack of knowledge, skills and protection of the public exemplifying the requirement for public awareness drives to empower users. While one of KE-CIRT/CC's role is capacity building in information security, cybersecurity awareness creation and maintenance, the results indicate that majority of the public is unaware of this role. This strengthens the study's findings on public awareness and make publication of KE-CIRT/CC's cybersecurity awareness mandate critical.

Additionally, the ICTA and C4DLab's partnership on cybersecurity training albeit targeting only a specific sector, reinforces the public awareness theme. While the initiative is useful, it excludes an important segment of Kenya's population, the youth; which RIA's statistics indicate 77.8% mobile Internet users begin from 15 years. To underscore the importance of targeting the public including youth, the study reflects on the positive impact achieved by cybersecurity awareness approaches employed in South Africa targeting the youth from primary schools. Specifically, Reid and Van Niekerk's annual education campaigns that aim to educate South Africa's youth on cyber issues through an interdisciplinary approach, supports the study's findings requiring targeting all sectors of society using mobile Internet. Additionally, von Solms and von Solms video-based syllabus that teaches children how to protect themselves when exploring the Internet also supports the study's findings.

Recognising that cybercrime deterrence is an integral component of national cybersecurity strategies, ITU's endorsement of public awareness campaigns strengthens the study's awareness argument. Furthermore, Phalomolakha et al's 2011 CyberSAT proposal for

South Africa’s national security supports the public awareness campaigns evidenced in this study’s results.

It was interesting to note the themes of technology and law enforcement were identified as ways to reinforce public awareness drives and coping skills of MIT. Serianu’s 2012 Report on Kenya’s Cybersecurity highlighted Kenya’s legal gap in cybersecurity where cybercrimes go unprosecuted leaving the victims vulnerable. Law enforcement is also supported by Magutu et al’s 2011 study on mitigations of cybercrime which underpins the gap left by lack of proper cyber-legislation to prosecute cybercrimes including spamming, phishing, malware and hacking, prevalent in Kenya. Botnet attacks in Kenya and legal loopholes certainly confirms Christin et al’s 2011 study, that explored the perspective of botnet operators who associate risks of hosting bot operations in countries that have ambiguous or non-existent cybercrime laws. The current study’s results endorse the law and the importance of public awareness as a deterrent for perpetrating mobile Internet crimes.

Strong support for technical means to dealing with MIT was clearly evident in the results. In fact Schneier argues for the design of better security systems that assume uneducated users and prevent them from changing security settings that expose them to risk (2014, p.123). However, research on security awareness recommends for effective training for users to operate securely since a purely technical approach is insufficient (Renaud and Goucher 2012, p.301, Phalomalakha et al 2011). Essentially, this confirms that user awareness and education on MIT is important in efforts to improve citizens’ security.

As discussed above, the correlation between the three themes exemplifies the requirement of public awareness strengthened by concerted efforts of technology and law enforcement to sensitize the public on MIT. It is also evident that different sectors of society require tailored awareness approaches to make them aware of MIT.

### E. Thoughts on Public Awareness Drives to Address MIT

*Has the government considered public awareness drives on cyber threats when using mobile Internet?*

In exploring this research question, it was important for the study to acknowledge the awareness efforts already underway spearheaded by ICTA and C4DLab. As training is the first of its kind in Kenya, this study’s findings argue for the requirement of government to roll out more awareness campaigns targeting all sectors of society using mobile Internet.

Four main themes emerged which have an implication for the investigation of awareness drives the government should deploy. The media campaigns theme was favoured by majority of participants who suggested using print, electronic and social media networks to publicise MIT, as supported by ITU's public campaigns.

Certainly, the themes of public forums and engagement with mobile network providers are reinforced by ITU's advocacy for public-private partnerships in creating awareness to fight cyber threats. It is conscionable for participants to require the government to take the lead role in ensuring mobile network providers take responsibility in protecting Internet subscribers especially since they control the largest Internet market share in Kenya.

Principally, the introduction of cybersecurity lessons in schools evidenced in the results is noted in South Africa's awareness drives by Reid and Van Niekerk's annual education campaign and von Solms and von Solms' video-based syllabus for primary schools. ITU also recommends for the introduction of cyber threats lessons in schools and universities. This confirms that in so far as the requirement to develop a cybersecurity awareness culture in society is concerned, it is prudent to begin with the youth in society who are increasingly using mobile Internet as confirmed by the RIA Survey.

The four themes confirm that despite the Kenyan government having only just begun quarterly awareness drives in one sector, there is a requirement for awareness drives targeting different sectors of society using mobile Internet to be sustained.

### F. Government's Role in Supporting the Public through Cybersecurity Strategy

*What measures will the government use to assist the public adapt to the evolving nature of the threats to mobile Internet?*

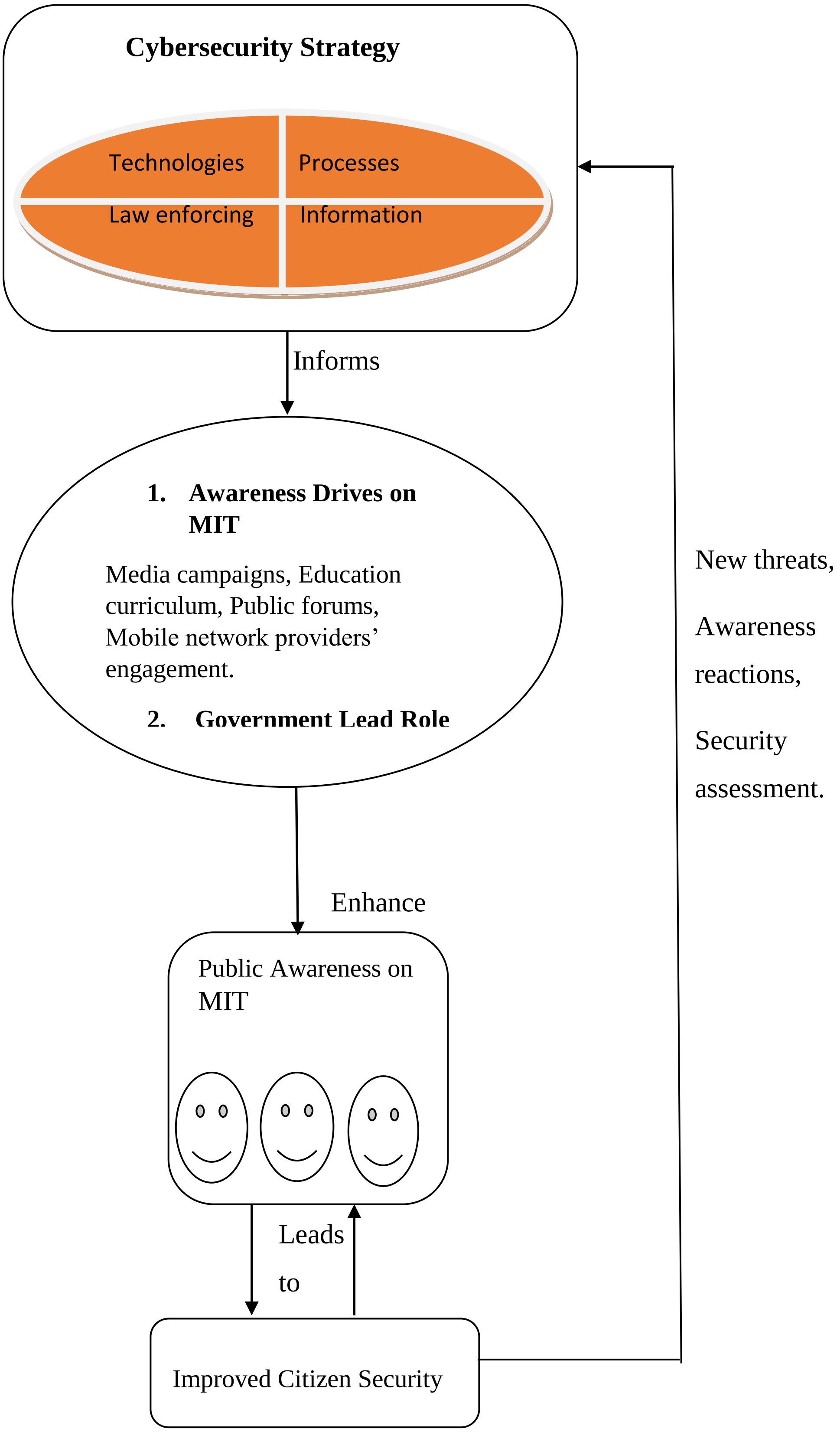
The thematic analysis exploring the research question on government measures to assist the public adapt to the evolving nature of MIT confirms that the themes of training and education, information portals and help desks are significant in our understanding of how the public can be supported. The ITU, Reid and Van Niekerk and von Solms and von Solms studies strongly support the training and education theme, and underscore the impact of including cybersecurity lessons in schools to teach the youth the latest cyber threats and how to protect themselves. Enterprise Risk Management (ERM) suggests that when using awareness and training programs, awareness tools should be deployed to make the learning process more interesting and engaging (2009). The study's results confirm that such support is required to be extended to other sectors of society using mobile Internet who are not currently included in ICTA's cybersecurity training program.

The findings provide evidence that the themes of information portals and help desks can be useful in extending our understanding of the role of KE-CIRT/CC and dedicated toll free lines at the CID to help the public report threat incidents and access threat information. Geer advocates for mandatory reporting of cyber incidents based on thresholds set by the law (2014). WolfPack's 2013 security report on South Africa that proposed establishment of a national and sector CSIRTs to coordinate incidence reporting and response to threats, also support these findings.

The information portal theme also suggested conducting surveys on threat awareness and prevalence, and publishing results for the public to access from CAK's website. Upon reviewing KE-CIRT/CC's functions, the study found out that it is mandated to carry out research on computer threats and, now on MIT, and to publish results. Indeed, ITU proposes the collection and publication of relevant information to determine threat levels as a way to informing users. Articles and newsletters about security are one way of spreading awareness (ERM, 2009) as evidenced in South Africa's Cybercrime.co.za awareness portal on cybersecurity issues and Cellphone Safety program on children's mobiles.

Overall, by answering the research questions, these findings confirm the support for the requirement of public awareness on MIT to help improve citizens' security. Therefore, the study proposes an improved conceptual framework that incorporates the suggestions from the findings and literature review as shown in Figure 9 to help creating public awareness on MIT. The strategy is required to incorporate the law, facilitate public access to usable technology, processes and information on MIT. These would inform tailored awareness drives targeting all sectors of society using mobile Internet, provide security assessments, and support government's role on reducing MIT.

Figure 8. Proposed Conceptual Framework



*Source: Author, 2014.*

# CHAPTER SIX

# CONCLUSION

## A. Introduction

The study aimed to investigate approaches the Kenyan government should use to improve public awareness on MIT through the Cybersecurity strategy. Projected growth of Kenya's mobile Internet requires awareness drives that will improve cybersecurity detection and coping skills of different sectors of society using mobile Internet. The findings have confirmed the importance of considering the concept of human factor in the security link by delineating the requirement of public awareness on MIT to improve citizen's security.

## B. Thoughts on Implication of Findings

Taking a mixed methods approach proved beneficial to the main contributions of this research because the researcher was able to use comparative analyses on South Africa and Kenya's MIT and awareness approaches as well as survey data, to answer the research questions. The main contribution of this research is the demonstration of the requirement for awareness drives to be sustained in all sectors of society to improve mobile Internet security in Kenya. The study suggests that awareness drives would be strengthened by widespread, easily accessible technology and a good legal framework.

On the basis of the MIT analyses, the findings of MIT prevalent in Kenya can be a useful springboard for designing awareness drives that the government may deploy to meet varying technical levels of society. Evidence also requires the government's lead role to support the public adapt to the evolving nature of MIT.

It is informative to mention that the implication of this research main finding for Phalomolakha et al's theory that proposes a Cyber Security Awareness Toolkit for South Africa's national security, and Reid and Van Niekerk's concept of youth education campaign confirms that different sectors of society require tailored cybersecurity awareness approaches.

The findings lead to the conclusion that governments that have vibrant mobile Internet societies require to improve the cybersecurity awareness of their mobile Internet users within the context of secure technology and robust legal framework or stringent cybercrime laws. Consequently, the development of cybersecurity strategies that endorse public awareness campaigns of MIT exemplifies the integral component and role of cybersecurity strategies to citizens' security as evidenced in this study.

### C. Proposed recommendations

Creating MIT awareness for all sectors of society is not effortless in a society with disparate IT skills. However, it is incumbent on government as a key stakeholder in security to take the lead role in the campaign. The study has devised some recommendations to support the government's role;

*Tailor specific awareness programs:* to support the ICTA's cybersecurity professional training, specific and measurable awareness programs must target different technical levels of all sectors of society. The effectiveness of training and awareness programs need to be measured to evaluate their impact (Reid and van Neikerk, Renaud and Goucher 2014).

*Information portals:* availability of, and access to threat information on CAK, CID, KE-CIRT/CC websites and Huduma Centres would spread awareness and provide support to the public in more decentralised ways helping them adapt to the evolving MIT. Use of awareness tools through different media and public campaigns are successful ways of spreading awareness to reach audiences of different technical levels (ERM 2009, ITU 2009).

*Surveys:* national surveys on cybersecurity awareness, usable and reasonably secure mobile technology drawing participants from different sectors of society, would be useful in identifying gaps and trends which can inform awareness programs. ITU recommends the collection and publication of relevant information to determine threat levels as a way to inform users (2009), and surveys are a way to achieving this.

*Government regulation:* mobile network providers' use of insecure mobile technologies rendering users vulnerable to MIT should be met with serious government penalties. Herley et al advocate for more government regulation to address the difference in power that allows service providers to shift losses to users when security breaches occur (2009, p.8).

### D. Limitations and challenges of the study

The research used web-based survey to collect data from key stakeholders of ICT in Kenya. The main limitation faced was lacking direct access to the respondents to ask further questions as they could only be reached through the listserv. There was also time constraint to collect the data and learn different features of NVivo that was used to code and thematically analyse the textual data.

Key challenges faced were the difficulty in accessing vital information especially from government sources without due authorisation and cost of paying for the online tools.

### E. Areas of further research

In conclusion, it is proposed that future research in this area be carried out to specifically measure the effectiveness of cybersecurity awareness approaches in countries with vibrant mobile Internet societies that have implemented awareness drives. This would set a benchmark for those developing or yet to develop their cybersecurity strategies.

Additionally, more research concentrating on MIT landscape in countries with vibrant mobile Internet societies would be useful as this study confirms these threats are on an upward trajectory.

## BIBLIOGRAPHY

African Union Website. 'African Union Draft Legislation for cybersecurity in Africa', available at http://www.itu.int/ITU-<D/projects/ITU_EC_ACP/hipssa/events/2011/WDOcs/CA_5/Draft%20Convention%20on%20Cyberlegislation%20in%20Africa%20Draft0.pdf 9/04/2014aa>, accessed on 15th June 2014.

Andjelkovic, M. (2012) 'The future is Mobile: why developing country entrepreneurs can drive internet innovation, SAIS Review of International Affairs, Volume 30 Number 2, available at

<http://muse.jhu.edu/journals/sais_review/v030/30.2.andjelkovic.pdf>, accessed on 12th April 2014.

Barlow, C. (2014) 'Highlights and Insights' RSA 2014 Conference, available at <http://www.inforisktoday.com/interviews/how-mobile-hacks-threaten-enterprise-i-2199> and http://6dbf9d0f8046b8d5551a-7164cafcaac68bfd3318486ab257f999.r57.cf1.rackcdn.com//rsa-conference-2014-highlights-insights-pdf-10-h-52.pdf, accessed 11/06/2014.

Bresz, F. (2004) 'People - Often The Weakest Link in Security, But One of The Best Places To Start', Journal of Healthcare Compliance , p.57-62, available at <http://web.b.ebscohost.com/ehost/pdfviewer/pdfviewer?sid=10dfe60d-662c-4d8c-bf41-3b8e91971848%40sessionmgr113&vid=2&hid=122>, accessed on 7th July 2014.

Bryman, A. (2012) Social Research Methods, New York: Oxford University Press.

Christin, N., Egelman, S., Vidas, T. and Grossklags, T. (2011) 'Its all about the Benjamins: an empirical study on incentivizing users to ignore security advice', available at https://www.andrew.cmu.edu/user/nicolasc/publications/CEVG-FC11.pdf, accessed on 7th July 2014.

Demombynes, G. and Thegeya, A. (2012) 'Kenya's Mobile Revolution and the Promise of Mobile Savings', Poverty Reduction and Economic Management Unit, Africa Region World Bank, available at <http://elibrary.worldbank.org/doi/pdf/10.1596/1813-9450-5988>, accessed on 20th June 2014.

CAK. (2014) 'ICT Sector Quarterly Statistics Report 2013/4: Second Quarter of Financial Years 2013/4', available at <http://www.ca.go.ke/images/downloads/STATISTICS/Sector%20Statistics%20Report%20Q2%202013-14.pdf>, accessed on 12th May 2014.

CAK. (2007) 'Internet Market Analysis Study', available at <http://www.ca.go.ke/images/downloads/RESEARCH/Internet%20Market%20Analysis%20Study%20Final%20Report.pdf>, accessed on 9th June 2014.

CCK and KNBS. (2011) 'National ICT Survey Report', available at

http://www.ca.go.ke/images/downloads/RESEARCH/Report%20on%20National%20ICT%20Survey.pdf>, accessed on 13th May 2014.

Cell phone safety website, available at< http://www.cellphonesafety.co.za/, accessed on 5th July 2014.

Council of Europe. (2001) 'Convention on Cybercrime', available at <http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm> , accessed on 29th June 2014.

Cybercrime. 'Local Resources on Cybercrime' available at http://cybercrime.org.za/local-resources/>, accessed on 5th July 2014.

ENISA. 'Cybersecurity Policy of South Africa 2010', National Cyber Security Strategies. http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-in-the-world>, accessed on 17th May 2014.

ENISA. (2010) 'ENISA and Cybersecurity', available at <http://www.europarl.europa.eu/document/activities/cont/201010/20101026ATT90288/20101026ATT90288EN.pdf>accessed>, accessed on 6th July 2014.

ENISA. (2013) 'ENISA threat Landscape 2013-Overview of Current and Emerging Cyber Threats', available at https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape-2013-overview-of-current-and-emerging-cyber-threats>, accessed on 8th July 2014.

Enterprise Risk Management. (2009) 'Social Engineering: People Hacking', Control Essentials, available at <www.emrisk.com>, accessed on 1st August 2014.

Grobler, M., Van Vuuren, J. J. and Leenen, L. (2012) 'Implementation of a Cyber Security Policy in South Africa: Reflection on Progress and the Way Forward', Council for Scientific and Industrial Research, available at http://krr.meraka.org.za/~lleenen/Grobler_Final.pdf >, accessed on 7th July 2014.

F-Secure Lab. (2013) 'Mobile Threat Report', available at <http://www.f-secure.com/static/doc/labs_global/Research/Mobile_Threat_Report_Q3_2013.pdf>, accessed on 5th July 2014.

Herley C., van Oorscht, P.C. and Patrick A. S. (2009) 'Passwords: If we're so smart, why are we still using them?' Springer, available at <http://moodle2.gla.ac.uk/pluginfile.php/99603/mod_resource/content/1/fc09.pdf>, accessed on 14th August 2014.

Geer, D. 2014. 'Cybersecurity as Realpolitik', Black Hat USA 2014 Conference, available at <https://www.youtube.com/watch?v=nT-TGvYOBpI>, accessed on 23th August 2014.

ICT Authority and C4DLab (2014). 'Cybersecurity training', available at <http://www.c4dlab.ac.ke/training/cybersecurity/>, accessed on 24th July 2014.

ICT Authority (2014) 'Cybersecurity capacity building', available at <http://www.icta.go.ke/ict-authority-university-nairobi-building-capacity-cyber-security/>, accessed on 24th July 2014.

ICT Authority. (2013) 'Kenya's ICT Master Plan 2014-2017', available at http://www.ict.go.ke/docs/MasterPlan2017.pdf Kenya's master plan 2017>, accessed on 13th March 2014.

ICT Authority. (2013) 'Kenya Cybersecurity Strategy', available at <http://www.information.go.ke/wp-content/uploads/2014/03/GOKCSMP.pdf>, accessed on 10th March 2014.

IDG Connect. (2013) 'Cybercrime, Hacking and Malware', available at <http://www.slideshare.net/IDGConnect/africa-2013-cybercrime-hacking-malware>, accessed on 11th June 2014.

ITU. (2009) 'Understanding Cybercrime: A guide for developing countries', ITU Telecommunication Development Centre, available at < http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-understanding-cybercrime-guide.pdf>, accessed on 2nd June 2014.

ITU TrendMicro. (2014) 'Cybercrime Hits the Unexpected,' Trend Labs 1Q Security Roundups, available at <http://www.itu.int/en/ITU-D/Cybersecurity/Documents/rpt-cybercrime-hits-the-unexpected.pdf>, accessed on 8th July 2014.

Kamau, M. (2013) 'Kenya Wants EAC States to Hasten Fake Phone Switch Off', Standard Digital, 28th June, available at http://www.standardmedia.co.ke/business/article/2000086969/kenya-wants-eac-states-to-hasten-fake-phone-switch-off 7/07/2013, accessed on 17th June 2014.

KE-CIRT website. Available at <http://www.ke-cirt.go.ke/index.php/services/national-cirt-services/>, accessed on 18th June 2014.

KICTANet. (2007) 'KICTANet 28-29 September 2007 Workshop Report' available at http://www.kictanet.or.ke/documents/instassessment/KICTANet-28-29-September-2007-Workshop-Report.pdf>, accessed on 5th May 2014.

Kigwe, W. (2012) 'Kenya: 1.9 million Fake Phones Shut' All Africa, available at http://allafrica.com/stories/201210020512.html, accessed on 17th June 2014.

Magutu. P. O., Ondimu G. M. and Ipu C. J. (2011) 'Effects of Cybercrime on State Security: Types, Impact and Mitigations with Fibre Optic Deployment in Kenya', University of Nairobi.

McAfee. (2013) 'McAfee Lab Threat Report: Third Quarter 2013', available at <http://www.mcafee.com/uk/resources/reports/rp-quarterly-threat-q3-2013.pdf>, accessed on 5th July 2014.

Morrow, B. (2012) 'BYOD Security challenges: control and protect your most sensitive data', available at < http://ac.els-cdn.com/S1353485812701113/1-s2.0-S1353485812701113-main.pdf?_tid=a05489f0-e011-11e3-abae-00000aab0f27&acdnat=1400585386_9e1d3946ba69cb424cb1e43161b9e51a>, accessed on 7th June 2014.

Ndung'u, T. M and Waema, M. N. (2010) 'Development outcome of internet and mobile phone use in Kenya: the household perspectives', Emerald Insight, Volume 13, Number 3, p.110-124, available at <http://www.emeraldinsight.com.ezproxy.lib.gla.ac.uk/journals.htm?articleid=1923886>, accessed 18th June 2014.

NIST website. (2014) 'The role of NIST and Technology in Mobile Security', available at <http://csrc.nist.gov/documents/nist-mobile-security-report.pdf>, accessed on 5th June 2014.

OECD. (2012) 'Cybersecurity Policy making at a turning point. Analysing a new generation of national cybersecurity strategies for the Internet economy' OECD Cyber Policy Comparison, available at <http://oe.cd/security>, accessed on 7th May 2014.

OWASP. (2013) 'Mobile Top 10 Risks', available at <https://www.owasp.org/index.php/OWASP_Mobile_Security_Project#tab=Top_Ten_Mobile_Risks>, accessed on 18th June 2014.

Phahlamohlaka L.J., Van Vuuren, J.J. and Coetzee, A. C. (2011) 'Cyber Security Awareness Toolkit for National Security: an Approach to South Africa's Cyber Security Policy Implementation', available at <http://researchspace.csir.co.za/dspace/bitstream/10204/5162/1/Phahlamohlaka_2011.pdf>, accessed on 7th July 2014.

Research ICT Africa. (2012) 'Internet going mobile: Internet access and usage in 11 African countries', available at <http://www.researchictafrica.net/publications/Country_Specific_Policy_Briefs/Internet_going_mobile_-_Internet_access_and_usage_in_11_African_countries.pdf>, accessed on 2nd April 2014.

Reid, R. and J. Van Niekerk. 2014. 'Towards an Education Campaign for Fostering a Societal Cyber Security Culture', HAISA, available at <http://www.cscan.org/default.asp?page=openaccess&eid=15&id=249>, accessed on 20th July 2014.

Renaud, K. and Goucher, W. (2013) 'Monkey See -Money Take Photo: The Risk of Mobile Information Leakage' International Journal of Cyber Warfare and Terrorism, Volume 3, Number 4, available at <http://www.irma-international.org/article/monkey-see-monkey-take-photo/105191/>, accessed on 20th August 2014.

Renaud. K., and Goucher, W. (2012) 'Health Service employees and Information Security Policies: an Uneasy Partnership?', Information Management & Computer Security, Volume 20, Number 4, pp.296 – 311, available at <http://www.emeraldinsight.com/journals.htm?articleid=17058066>, accessed on 9th August 2014.

Ruggeiro, P. and Foote, J. (2011) 'Cyber Threats to Mobile Phones' US-CERT, available at <https://www.us-cert.gov/sites/default/files/publications/cyber_threats-to_mobile_phones.pdf> , accessed on 15/05/2014.

Safaricom App Store (2014). Available at <http://appstore.safaricom.com/Web/shop/index.aspx>, accessed on 17th June 2014.

Schneier, B. (2014) Carry On. Sound Advice from Schneier on Security, Indiana: John Wiley & Sons Inc.

Serianu. (2014) 'Kenya Cybersecurity Report 2014. Rethinking cyber security "An Integrated Approach: Process, Intelligence and Monitoring"', available at <http://www.cyberusalama.co.ke/reports/2014/Kenya%20Cyber%20Security%20Report%20 2014.pdf>, accessed on 20th May 2014.

Serianu. (2012) 'Kenya Cyber Security Report', available at <http://aitec.usp.net/AITEC%20East%20Africa%20ICT%20Summit,%20Nariobi,%202-25%20October%202012/William%20Makatiani%20Director%20Serianu%20LTD%20Kenya %20Cyber%20Security%20Report.pdf>, accessed on 13 June 2014.

Shikoh, G., Mardsen, G. and Donner, J. (2010) 'After Access: Challenges facing mobile-internet users in developing world', H.5 Information Interfaces and Presentations, available at

<http://delivery.acm.org.ezproxy.lib.gla.ac.uk/10.1145/1760000/1753720/p2603-gitau.pdf?ip=130.209.6.50&id=1753720&acc=ACTIVE%20SERVICE&key=C2D842D97AC95F7A.C612DDE1DA0E84ED.4D4702B0C3E38B35.4D4702B0C3E38B35&CFID=434969168&CFTOKEN=62885201&__acm__=1396997471_d3ed470865d1d2d70f08169cbb97f3b8>, accessed on 18th June 2014.

Souter, D. and Kerrets-Makau, M. (2012) 'Internet Governance in Kenya: An Assessment' ICT Development Associates Ltd, available at <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 on 23rd May 2014.

Symantec. (2014) 'Internet Security Threat Report', available at http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf>, accessed on 5th July 2014.

Symantec. (2014) 'Analysis of mobile threats', available at <http://www.symantec.com/en/uk/threatreport/topic.jsp?id=threat_activity_trends&aid=analysis_of_mobile_threats>, accessed on 6th July 2014.

The Yankee Group. (2013) 'Redefining Virtual Currency', available at <http://info.tapjoy.com/wpcontent/uploads/sites/4/2013/05/RedefiningVirtualCurrency_WhitePaper-1MAY2013-v1.pdf>, accessed on 6th July 2014.

Von Solms, S., and Von Solms, R. (2014) 'Towards Cyber Safety Education in Primary Schools in Africa', HAISA, available at <http://www.cscan.org/default.asp?page=openaccess&eid=15&id=247>, accessed on 20th July 2014.

WolfPack. (2012/3) 'The South African Cyber Threat Barometer', available at <http://www.bic-trust.eu/files/2012/10/SA-2012-Cyber-Threat-Barometer_Medium_res.pdf>, accessed on 10th June 2014.

World Bank website. 'South Africa', available at <http://data.worldbank.org/country/south-africa>, accessed on 18th June 2014

World Bank website. 'Kenya', available at <http://data.worldbank.org/country/kenya>, accessed on 18th June 2014.

World Internet statistics. (2012) 'Internet Usage Statistics for Africa' available at <http://www.internetworldstats.com/stats1.htm> accessed on 28th June 2014.

# APPENDICES

## APPENDIX I

### Coding Frame

| Theme | Code | Item |
|---|---|---|
| **Mobile Internet threats** | MIT | MIT-technical<br>MIT-non-technical |
| **Threat Approach** | MIT-Apr | Public awareness<br>Technologically<br>Law enforcement |
| **Awareness Drives** | MIT-AwrDr | Media campaigns<br>Public forums<br>Education curriculum<br>Mobile network providers |
| **Threat Support** | MIT-Supt | Training and education<br>Information portals<br>Help desks |
| **Government Role** | MIT-Govt | Awareness and info access<br>Public-private partnership<br>Law creation<br>Cybersecurity response team |

## APPENDIX II

## Plain Language Statement

University of Glasgow | College of Social Sciences

**Role of Cybersecurity Strategy on National Security: Approaches to Increase Public Awareness on Mobile Internet Security in Kenya.**

Dear participant,

You are kindly invited to take part in the above mentioned research study which is being conducted by Ms. Angela Atieno Okuku (MSc Global Security student) in the College of Social Sciences, University of Glasgow, UK. However, before you decide it is important for you to understand why the research is being done and what it will involve.

This study is aimed at investigating the role of cybersecurity strategy on national security. It will specifically examine how Kenya's newly developed Cybersecurity strategy would address mobile internet security threats that undermine the overall efforts of national security. The results of this study will form part of my dissertation project for the award of a Master's degree. The study has been reviewed by Ms Karen Renaud, a senior lecturer in the School of Computing Science whose main research interest is usable security.

As a key stakeholder of the Cybersecurity strategy, a public policy in Kenya, your views on the approaches the government should use to increase public awareness on mobile internet security will help in answering the research questions of this study. The link provided below will direct you to a five minutes questionnaire at a time convenient to you. With your permission, the researcher would like to clarify further questions that may arise from the analysis of the survey through an email based questionnaire. Your decision to participate or not or to withdraw at some point of the study will be completely voluntarily. Your consent will be implied by return of the survey. The data will be kept securely in the College of Social Sciences for ten years from the date of publication before being destroyed.

The researcher intends to distribute a final copy of the study to the Kenya ICT Authority to support its ongoing efforts in developing the national cybersecurity strategy. It is also possible that the results will be published in academic journals.

Should you have any concerns regarding the conduct of this research project or require further information, please contact either: College of Social Sciences Ethics Officer via; http://www.gla.ac.uk/colleges/socialsciences/info/students/ethics/committee/; the supervisor of this research Ms Renaud on Karen.Renaud@glasgow.ac.uk; or the researcher at 20791640@gla.ac.uk; chachaangelou@yahoo.com, mobile +44 7466134569.

Thank you for your participation.

Yours faithfully,

Angela Atieno Okuku.

## APPENDIX III

## Questionnaire

### Section A

### Demographics

1. What is your gender? a) Male b) Female

2. Which category below includes your age?

a) 18-23 b) 24-29 c) 30-35 d) 36- 41 e) 42 and above

3. Which sector do you belong to?

a) Civil society (NGO's) b) Public service c) Private sector

d) Academia e) Media f) Development partners

4. What is the highest level of education you have completed?

a) High school b) Tertiary college c) University graduate

d) Post graduate e) Other

### Section B: Cybersecurity Strategy Literacy

5. Do you have access to Kenya's new proposed Cybersecurity strategy? a) Yes b) No

6. Have you read the Cybersecurity strategy? A) Yes b) No

7. Do you currently own an Internet-enabled mobile phone? A) Yes b) No

8. How often do you access the Internet using your mobile phone?

a) Often b) Very Often c) Not often d) Not at all

### Section C: Mobile Internet Security

From your perspective:

9. What are the major threats facing mobile Internet security in Kenya?

10. How do you envisage the government should address these threats?

a. Public awareness drives? b. Technologically? C. Law enforcement?

11. Please give reason(s) for your answer in question 10 above.

**Section D: Public Awareness Drives**

13. What awareness drives should the government use to create public awareness on mobile Internet security?

14. What plans should the government put in place to assist the public adopt to the evolving nature of threats to mobile Internet?

15. How should the government's role in mitigating mobile Internet threats mentioned above be reflected in the strategy?

End.

*Thank you.*

## APPENDIX IV

### Archive Permission Form

# Global Security PGT Programmes 2013/4

## Dissertation Archive Permission Form

I give the School of Social and Political Sciences, University of Glasgow permission to archive an e-copy and hard copy of my MSc dissertation in a publicly available folder and to use it for educational purposes in the future.

Student Name: **ANGELA ATIENO OKUKU**

Student Number: **2079164O**

Student Signature: **AAO** Date: **25th August 2014**

## APPENDIX V

### Record of Supervision Form

**School of Social and Political Sciences**

**MSc in Global Security**

**Record of Supervision**

Student: Angela Okuku

Supervisor: Karen Renaud

Date of Meeting: 4th June 2014

---

Main Issues Discussed:

Topic of study and the research objective, type of participants to include in the study, various online data collection tools and their limitations, and the survey questions to include.

---

Guidance/ Advice Received:

Karen advised to focus on mobile Internet platform as cybersecurity is a huge subject area. Kenya was best placed as a case study due to its mobile proliferation and past successes on mobile banking. She further guided me on my survey questions and ensured they were suitable to answer the research questions. We settled on KICTANet as opposed to including the general public participants to the study.

Additionally, I took on her suggestion of using Survey Monkey as an online tool to collect my data. She also submitted my ethics form for approval to conduct the survey.

---

Course of Action to Next Meeting:

To work on the literature review as we waited for ethical approval to carry out the survey.

---

Date/Time of Next Meeting: We were to meet over Skype as Karen had travelled overseas for a conference.

**Signed**

Supervisor: Karen Renaud Student: AAO

*This page has been left intentionally blank*