A Cyber Security Awareness and Education Framework for South Africa

by

Noluxolo Kortjan

2013

A Cyber Security Awareness and Education Framework for South Africa

by

Noluxolo Kortjan

Submitted in fulfilment of the requirements for the degree

MAGISTER TECHNOLOGIAE

in

INFORMATION TECHNOLOGY

in the

FACULTY OF ENGINEERING, THE BUILT ENVIRONMENT AND

INFORMATION TECHNOLOGY

of the

NELSON MANDELA METROPOLITAN UNIVERSITY

Supervisor: Prof R von Solms

November 2013

DECLARATION

NAME:	Noluxolo Kortjan
STUDENT NUMBER:	208045801
QUALIFICATION:	MTech IT
TITLE OF PROJECT:	A cyber security awareness and education framework for South Africa

DECLARATION:

In accordance with Rule G4.6.3, I hereby declare that this treatise/dissertation/thesis is my own work and that it has not previously been submitted for assessment to another University or for another qualification.

SIGNATURE: ____

DATE: ____

ABSTRACT

The Internet is becoming increasingly interwoven in the daily life of many individuals, organisations and nations. It has, to a large extent, had a positive effect on the way people communicate. It has also introduced new avenues for business and has offered nations an opportunity to govern online. Nevertheless, although cyberspace offers an endless list of services and opportunities, it is also accompanied by many risks.

One of these risks is cybercrime. The Internet has given criminals a platform on which to grow and proliferate. As a result of the abstract nature of the Internet, it is easy for these criminals to go unpunished. Moreover, many who use the Internet are not aware of such threats; therefore they may themselves be at risk, together with businesses and governmental assets and infrastructure. In view of this, there is a need for cyber security awareness and education initiatives that will promote users who are well versed in the risks associated with the Internet.

In this context, it is the role of the government to empower all levels of society by providing the necessary knowledge and expertise to act securely online. However, there is currently a definite lack in South Africa (SA) in this regard, as there are currently no government-led cyber security awareness and education initiatives. The primary research objective of this study, therefore, is to propose a cyber security awareness and education framework for SA that will assist in creating a cyber secure culture in SA among all of its users of the Internet.

ACKNOWLEDGEMENTS

I would like to thank the Lord for preparing the way for me to pursue this research. My Lord God has strengthened me throughout the course of this study and has given me the knowledge and understanding I needed to complete this dissertation. Moreover, he has blessed me with all the people who have supported me, as listed below:

- My supervisor, Prof Rossouw von Solms. You are not merely an academic figure in my life; you are a father. You have shaped this study with your guidance and diligence.
- My parents, Nomzamo and Zongezile Kortjan, and the rest of my family and friends. I appreciate your encouragement as well as the hope you vested in me.
- My husband, Bulelani Gcaza, you are utterly amazing! I am forever grateful for carrying me through with your love and support. Uyathandwa ndim Gqu gqu gqu!
- Alexa Barnby, for language editing this dissertation.
- The financial assistance of the National Research Foundation (DAAD-NRF) towards this research is hereby acknowledged. The opinions expressed and the conclusions arrived at are those of the author and are not necessarily to be attributed to the DAAD-NRF.
- The financial assistance by the Vodacom/NMMU scholarship towards this research is also hereby acknowledged. Opinions expressed and conclusions arrived at are those of the author and are not necessarily to be attributed to the sponsors.

"I can do all things through Christ who strengthens me (Philippians 4:13)."

TABLE OF CONTENTS

List of Figures

LIST OF TABLES

CHAPTER 1: INTRODUCTION

1.1 Background

“We are currently living in an age where the use of the Internet has become second nature to millions of people” (Kritzinger & von Solms, 2010).

Of all modern technology, the Internet has become one of the most significant inventions to date (Hunton, 2011). Over the years the Internet has developed immensely, providing billions of individuals and organisations across the globe with digital communication (Livingstone & Helsper, 2007). In the modern way of doing business, organisations use the Internet to meet their aims and to enable business processes (Hunton, 2011). Over and above its communication value, people use the Internet for financial and entertainment purposes (PEW Internet, 2012). As a result, large numbers of people have become dependent on it.

Although the Internet offers numerous advantages, it is constantly threatened by many risks that often have serious adverse effects on those who use the Internet. One of these risks is online crime (Riem, 2001). The Internet has given criminals a platform on which to grow and proliferate (Selwyn, 2008); furthermore, it is easy for criminals to go unpunished because of the abstract nature of the Internet and the difficulties involved in tracing the origins of such crime (Hunton, 2011).

Core to criminal activities on the Internet is the exploitation of private information (De Joode, 2011). Thus, Internet users are at risk of having their private information compromised. According to Thomson, Von Solms, and Louw (2006), many users are unaware of the concept of protecting information. Moreover, users online often behave in an unsecure manner which makes them easy targets for exploitation. Consequently, humans are deemed as “a severe threat to each other’s security” (Mitnick & Simon, 2002). Moreover, users not only pose a threat to each other, but also to national security (Grobler, Dlamini, Ngobeni, & Labuschagne, 2011).

In view of the risks that accompany the ever-increasing reliance on the Internet, certain safety and security measures have been adopted. Many developed countries, such as the United States (US), the United Kingdom (UK) and others, have established and implemented a number of cyber security measures. Part of these measures involves awareness and education initiatives. This is due to the fact that lack of knowledge is viewed as a factor that contributes to insecure online behaviour by Internet users (Thomson et al., 2006). The following subsection provides more detail on the cyber security efforts of some developed countries.

1.1.1 Cyber security efforts in developed countries

In 2007, Estonia was the first country ever to experience a cyber-attack (Mansfield-Devine, 2012). According to Jenik (2009), this cyber-attack relied on the computers of unaware users to form part of numerous botnets. A botnet is a network consisting of private computers that contain malicious software, which are added to the network – botnet – without their owners' knowledge (Lu, Tavallaee, Rammidi, & Ghorbani, 2009). This attack crippled significant national infrastructure such as the banking systems (Mansfield-Devine, 2012).

As a result of the high integration of the Estonian government services on the Internet, this attack called for national attention. Consequently, the Estonian Cyber Security Policy was drafted to avoid future incidents of the same nature (Dlamini, Taute, & Radebe, 2011). Additionally, Estonia identified cyber security awareness and education as a means to instil secure behaviour in the society at large (Mansfield-Devine, 2012).

It was not long after Estonia was attacked that other nations followed suit in promoting cyber security. In May 2009, the President of the United States of America, Barack

Obama, directed an intensive review to assess United States (US) efforts in cyber security (The White House, 2009a). From this review he concluded the following (The White House, 2009b):

> "It's now clear this cyber threat is one of the most serious economic and national security challenges we face as a nation. It's also clear that we're not as prepared as we should be, as a government or as a country."

Having realised that the US was ill-prepared to assure safety and security in cyberspace, the Cyberspace Policy Review Report brought forth various recommendations. Among these recommendations was educating the general public on cyber-related threats and cyber security. In response, the US formed the National Initiative for Cyber Security Education (NICE) (NICE, 2012). The NICE initiative aims to improve the cyber behaviour, skills and knowledge of the US population, enabling a safer cyberspace through cyber security awareness and education initiatives such as *Stop.Think.Connect*. NICE believes that awareness and education play a fundamental role in promoting cyber security (NICE, 2012).

Similarly, the UK is also faced with the challenge of cyber security. This is likewise due to the ever-increasing reliance on the Internet. In 2011, the UK issued its National Cyber Security Policy which encapsulates the manner in which the UK will ensure cyber security (Cabinet Office, 2011). Ultimately, the primary objective of this policy is creating a cyberspace that is resilient to cyber-attacks and, additionally, a cyberspace where society at large can be safe. To accomplish this objective, a number of key actions were identified. Listed below are some of these key actions (Cabinet Office, 2011):

- encouraging the development of industry-led cyber security standards for private sector companies

- expanding the use of cyber specialists to help the police tackle cybercrime

- encouraging the police and the courts to make more use of existing cyber sanctions for cyber offences

- making it easier to report financially motivated cybercrime by establishing a single reporting system for businesses and the public

- promoting cyber security awareness and education by strengthening the role of the already existing cyber security awareness and education initiative - *Get Safe Online*.

Similarly, in the UK, cyber security awareness and education is viewed as a key action with regard to ensuring cyber security. Australia also views this very seriously; as such cyber security awareness and education is regarded as a pillar of its cyber security efforts (Commonwealth of Australia, 2009). Among other cyber security measures, Australia has a considerable number of national cyber security awareness and education initiatives. This nation strongly believes that educating society not only benefits people but also contributes immensely towards a society that will embrace online opportunities and, in turn, contribute to an economically prosperous nation (Commonwealth of Australia, 2009).

Cyber security is a pressing concern all around the world (Von Solms & Van Niekerk, 2013). As it is, more than 50 nations are in possession of a cyber security-related policy or strategy (Klimburg, 2012). As can be observed from the countries just mentioned, cyber security is positioned alongside other national priorities. Hence, these countries have taken definite steps in the direction of cyber security both from a policy and a strategy point of view, and also in terms of the awareness and education facet of cyber security. The following subsection will provide some background on cyber security efforts in South Africa (SA).

1.1.2 Cyber security efforts in South Africa

As discussed in the previous subsection, cyber security is not unique to the developed countries; developing countries are also faced with this issue. In particular, as SA becomes ever more reliant on cyberspace to govern and to conduct business, it is increasingly being affected by cyber threats (Kortjan & Von Solms, 2012). Indeed, cybercrime is one of the leading threats faced by SA today. This dates back to 2010, when SA was rated seventh on the global cybercrime list (Dennis, 2010). This increase in cybercrime resulted from the 2010 Soccer World Cup event, which was held in SA (Dennis, 2010). Since 2010, SA has persistently ranked high in cybercrime (World Economic Forum, 2012). In addition, the recent increase in bandwidth has also contributed to the increase in cybercrime. Yet, cyber security efforts have not strengthened in step with cyberspace reliance.

In 2010, the South African government released a Draft Cyber Security Policy (*SA Government Gazette,* 2010). This draft policy implied that SA is not currently in a position to deal effectively with cyber-related threats (*SA Government Gazette*, 2010). In addition, the draft policy stated that SA lags behind other countries in the development of cyber security protocols and standards, as well as in the implementation of such. The objectives of this draft policy includes developing structures that will be capable of adequately supporting cyber security, as well as establishing and promoting a cyber security culture, and encouraging compliance with certain security standards. However, this draft policy has remained stagnant for a period of two years.

Nevertheless, the draft policy has paved the way for the recently published National Cyber Security Policy Framework (*SA Government Gazette*, 2011). Articulated in this policy framework is the intent to secure cyberspace and to ensure that SA's national critical information infrastructure is properly protected. This policy framework aims to create a knowledgeable society that understands cyber-related threats. Moreover, it intends to provide a cyber security approach that is holistic. In doing so, it requires the support of all role-players. These role-players include the state, the public and private sector and society at large (*SA Government Gazette,* 2011). This policy framework addresses the following:

- The development and implementation of an integrated approach to cyber security that is government led.
- The promotion of a cyber security culture that subscribes to minimum cyber security measures.
- The strengthening of legal processes to prevent and address cybercrime, cyber terrorism and cyber warfare.
- Ensuring the safety of national critical information infrastructure.
- The establishment of a partnership with public and private entities to coordinate action plans that correspond with the intentions of this policy.
- The establishment of a comprehensive legal framework to govern cyberspace.

From the above list, the second point highlights that SA wishes to cultivate a cyber security culture in its society. As such, as part of this study a paper on cultivating a cyber security culture was published and presented at the 2012 ZA-WWW Conference (Appendix A1). In this paper it was concluded that cyber security awareness and education are the basis for such a culture. Moreover, cyber security awareness and education is fundamental to cyber security implementation (Kortjan & von Solms, 2012).

However, the policy framework at hand is vague on cyber security awareness and education. Moreover, as yet SA does not have government-led cyber security awareness and education initiatives in place (Dlamini & Modise, 2012). Although there are currently existing cyber security awareness and education initiatives in SA, they are offered by academic institutions and industry (Dlamini & Modise, 2012). Consequently, this research focuses on cyber security awareness and education in SA, or the lack thereof.

1.2 Problem statement

Cyber security awareness and education is central to any attempt to secure cyberspace. Accordingly, developed countries have established national cyber security initiatives to create a society and commercial world that is knowledgeable about protecting itself from cyber-related threats. Since cyber security is a global issue, it is therefore essential that every country have a clearly defined plan for instilling cyber security knowledge in all sections of society. However, SA is still lacking in this regard, and therefore the problem statement addressed in this study can be defined as:

> *South Africa is ill prepared to educate its citizens on how to behave securely whilst active in cyberspace. For this reason, individuals put themselves, as well as businesses and governmental assets and infrastructure, at risk***.**

The problem that this study addresses is now defined. The following section will provide the objectives of this study.

1.3 Research objectives

This section defines the primary objective of this study together with the secondary objectives.

The primary research objective is:

> *To propose a cyber security awareness and education framework for SA that will assist in creating a cyber secure culture in SA among all its users of cyberspace.*

In order to fulfil this primary objective, three secondary objectives have been defined.

The secondary research objectives are:

- *To identify the position of awareness and education in a cyber security culture.*
- *To evaluate the initiatives that some developed countries have in place with regard to cyber security awareness and education.*
- *To identify the key factors that need to be addressed in developing a national cyber security awareness and education framework for SA.*

The purpose of this study, therefore, is to assist SA in creating the envisaged cyber security culture by means of a cyber security awareness and education framework. The following section will discuss the research design that was followed in this study in order to find the required solution.

1.4 Research design

This section will provide the research paradigm and the research process together with the research methods that were used in conducting this research.

This research developed and proposed a cyber security awareness and education framework in the form of an artefact. The proposed framework can assist in addressing the lack of cyber security awareness and education that is apparent in SA. Therefore, because design science also concerns itself with creating an artefact as a solution to a problem, this research was conducted in terms of the design science research paradigm.

There are various approaches to design science, one of which is that defined by Peffers Tuunanen, Gengler, Rossi, Hui, Virtanen and Bragge (2006). Peffers et al. (2006) developed a design science approach that is consistent with the design science processes found in other disciplines. This approach provides a method for conducting research and, furthermore, provides a mental model of what the research output should look like. Owing to the aforementioned factors, this is the approach that was followed in this research (Peffers et al., 2006).

According to the selected research approach, six definite steps as listed below were followed (Peffers et al., 2006).

1) *Problem identification and motivation*. Identifying the problem while motivating the value of a solution.

2) *Objectives of a solution*. Deducing the objective of the solution from the problem identified.

3) *Design and development*. Creating a solution in the form of an artefact.

4) *Demonstration.* Demonstrating the efficacy of the artefact in solving the problem.

5) *Evaluation*. Observing and measuring how well the artefact supports a solution to the problem.

6) *Communication*. Creating scholarly and/or professional publications.

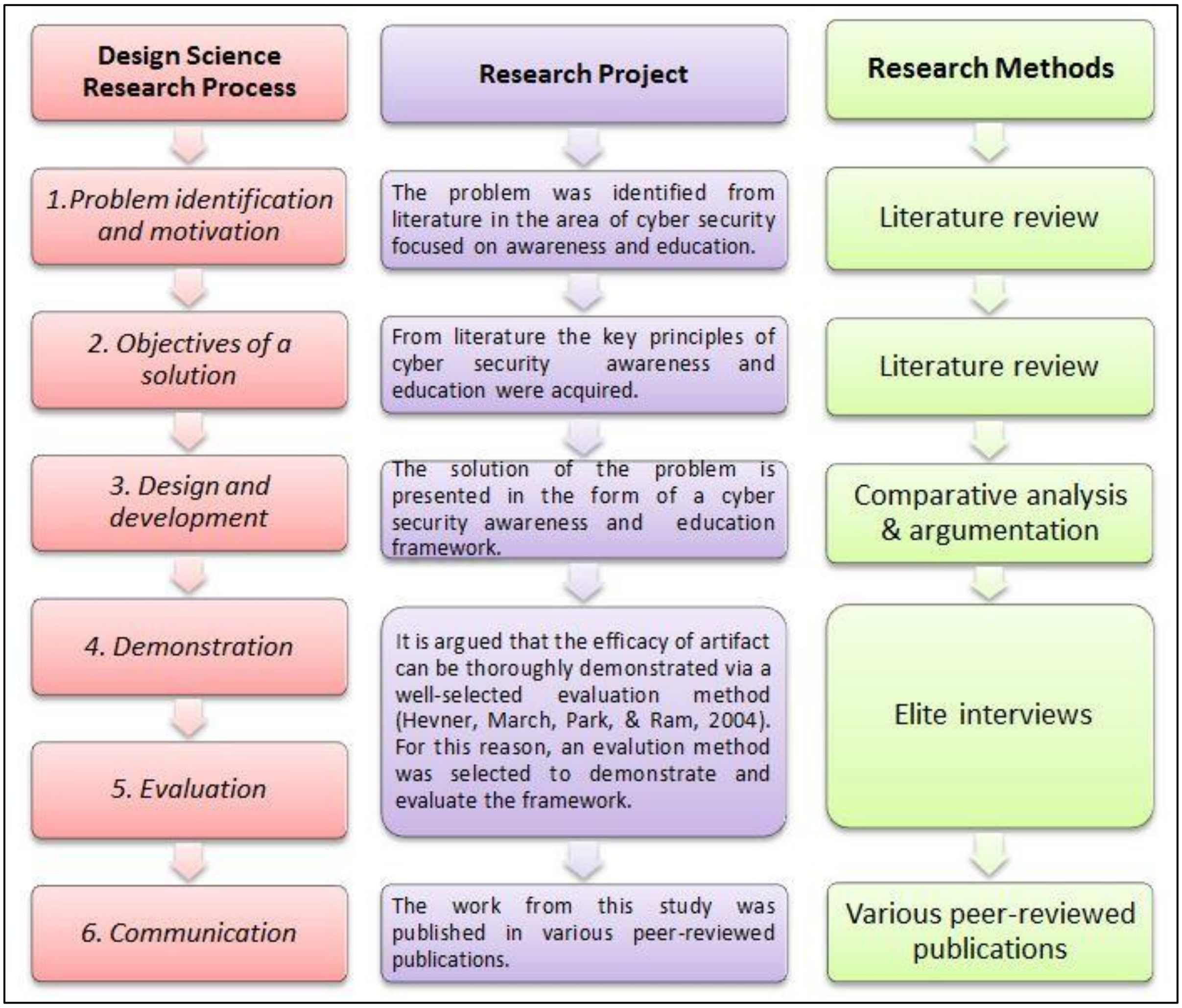
These steps are intended to lead the researcher (Peffers et al., 2006). Therefore, this research has closely followed the declared steps using relevant research methods at each step of the process to produce the expected outcome. The research methods that were employed in this study are as follows:

- literature review
- comparative analysis
- argumentation
- elite interviews

In line with Hofstee (2006), a ***literature review*** was initially conducted in order to gain insight and understanding of the research area, as well as to bring clarity and focus to the research problem as stated in section 1.2. In this study, a further literature review was conducted on the history and evolution of the Internet, reliance on the Internet, the threats associated with relying on the Internet and, finally, approaches to securing the Internet (see chapter 2 and 3). Thereafter, a ***comparative analysis*** on selected developed countries was performed. According to Mills, Van de Bunt, and De Bruijn (2006), "the underlying goal of comparative analysis is to search for similarity and variance". From the similarities and variances of the countries studied, key factors pertaining to cyber security awareness and education were ***argued*** (see chapter 4).

An initial set of key factors was published and reviewed using peer reviews and was subsequently presented at the AFRICOMM 2012 conference (see Appendix A2). Based on the feedback obtained from the conference, these factors were adapted accordingly. Subsequently, the proposed cyber security awareness and education framework was developed on the basis of the key factors (see chapter 5). This framework was then verified through the use of ***elite interviews*** as elaborated on in chapter 6.

Figure 1.1 below presents an overview of the way in which the design science steps were implemented in this study, as well as the research methods that were used in each step.



Design Science Research Process	Research Project	Research Methods
1. Problem identification and motivation	The problem was identified from literature in the area of cyber security focused on awareness and education.	Literature review
2. Objectives of a solution	From literature the key principles of cyber security awareness and education were acquired.	Literature review
3. Design and development	The solution of the problem is presented in the form of a cyber security awareness and education framework.	Comparative analysis & argumentation
4. Demonstration	It is argued that the efficacy of artifact can be thoroughly demonstrated via a well-selected evaluation method (Hevner, March, Park, & Ram, 2004). For this reason, an evalution method was selected to demonstrate and evaluate the framework.	Elite interviews
5. Evaluation		
6. Communication	The work from this study was published in various peer-reviewed publications.	Various peer-reviewed publications

Figure 1.1: Research Project Adherence to Design Science Process

This section discussed the research process followed in this study. Moving forward, the following section provides the list of the chapters within this research dissertation.

1.5 List of chapters

This chapter (**Chapter 1: Introduction)** provided some background information on the research area of the study. Moreover, it defined the problem addressed and made known the objectives of the research together with the methodology that was employed to attain these objectives.

In order to attain the objectives outlined in this chapter, an understanding of how cyberspace came into being and how it is used by society is needed. As such, **Chapter 2: The Virtual World,** defines cyberspace. It discusses the literature pertaining to the evolvement of cyberspace and discusses the way in which individuals, organisations and nations are dependent on this resource.

Although cyberspace has many advantages, it also has a 'dark side'. Thus, **Chapter 3: Safety and Security in Cyberspace,** discusses the risks associated with using cyberspace, as well as exploring security in cyberspace. Subsequently, **Chapter 4: Cyber Security Education** provides a detailed review of cyber security awareness and the education efforts of some developed countries, with the aim of abstracting the commonalities of the implementations. From the abstraction, this chapter then presents a suite of key factors for cyber security awareness and education.

The key factors identified form the basis of the cyber security awareness and education framework for SA that is sought in this research. **Chapter 5: Framework for Cyber Security Awareness and Education in South Africa,** introduces the proposed framework for SA. Thereafter, the framework is verified and **Chapter 6: The Validation of the Framework** discusses the verification of the proposed framework. Finally, **Chapter 7: Conclusion** provides concluding remarks and a summary of the research findings.

1.6 Conclusion

This chapter provided some background on the research area of this study. It further drilled down to the focus area of the study and defined the problem addressed. Accordingly, this study aims to develop and propose a cyber security awareness and education framework for SA. The research objectives that have been formulated in order to fulfil the aim of this study were outlined. Moreover, the research process that this study employed to achieve the outlined objectives was also discussed. Finally, the outline of this dissertation was presented.

CHAPTER 2: THE VIRTUAL WORLD

2.1 Introduction

“Cyberspace is a globally networked, computer-sustained, computer-accessed, and computer-generated, multidimensional, artificial, or “virtual” reality. In this reality, to which every computer is a window, seen or heard objects are neither physical nor, necessarily, representations of physical objects but are, rather, in form, character and action, made up of data, of pure information” (Benedikt, 1991).

Cyberspace had humble beginnings and has progressed immensely over time to what it is today. This chapter provides a brief history of the origin of the Internet and discusses how the Internet has evolved into what today is known as cyberspace. Furthermore, this chapter will examine the reliance of individuals, organisations and nations on the services provided by cyberspace.

2.2 The origin of the Internet

In October 1976, the first International Conference on Computer Communications held in Washington DC marked the first public demonstration of the Internet, the “network of networks” (Roberts, 1978). This was an invention of the United States (US) Department of Defense (DOD) (Roberts, 1978). At this conference the Advanced Research Projects Agency (ARPA) of the DOD demonstrated a network that linked computers and maintained data transfer from a considerable distance. This network, which was called ARPANET, was the first of its kind and it allowed different types of computers to transfer data over a distance (Abbate, 1994). This ability to transfer data over a distance had not been established at the time (Kirstein, 1999).

ARPANET was developed for use by the US military with the intention of keeping the US ahead of its military rivals (Leiner, Cerf, Clark, Kahn, Kleinrock, Lynch, Postel, Roberts, Wolff, 2009). The system was aimed at allowing computers across the country to share resources and transfer information back and forth. At the time, ARPANET linked only four computers, some of which were owned by the military university laboratories conducting defence-related research (Savetz, 1994).

Later, ARPANET allowed researchers around the US to access computers located at some universities in the country (Savetz, 1994). The network succeeded in what it had set out to do and eventually it was also used for non-military purposes. Subsequently, ARPANET was separated into two networks to cater for military work and non-military work exclusively. Accordingly, the military used MILNET while a smaller ARPANET was dedicated to non-military work (Savetz, 1994). These two networks were connected to each other through an Internet Protocol which enabled traffic to be routed between the networks (Leiner et al., 2009).

Subsequently, APRANET evolved and its structure changed as it expanded its scope of access. Soon afterwards the US National Science Foundation (NSF) funded the development of other networks that would be connected to ARPANET. Similar to APRANET, these other networks were intent driven. One such network was NSFNET, which was intended to afford the entire education community access to ARPANET (Kirstein, 1999).

ARPANET eventually became the first packet switching network and was later interconnected with a Packet Radio Network and other networks existing at the time. However, the Internet Protocol that was used to enable host-to-host communication had its limitations, which led to the introduction of the Transmission Control Protocol and Internet Protocol (TCP/IP) (Kirstein, 1999). Network protocols and technologies continued to advance as more networks interconnected. However, as the network proliferated infrastructural challenges appeared.

As a result of the infrastructural challenges ARPANET faced, NSFNET took over. The universities that were connected to ARPANET ended up connecting to NSFNET’s backbone. At this stage, a number of interconnected networks had emerged (Leiner et al., 2009). Nonetheless, eventually, from the evolution of ARPANET, the Internet formed.

This section provided a concise background to the humble beginnings of what is known today as the Internet. The following section will discuss the journey from ARPANET to Internet from a network design perspective. It will furthermore refer to the devices currently used to connect to the Internet.

2.3 Towards the Internet

As mentioned in the prior section, initially only four computers were connected to ARPANET. These computers were mainframes which were scattered all over the US. Gradually more computers were able to connect to the network. This section aims to provide a high-level snapshot of how the ARPANET expanded to ultimately become the Internet, a network of networks. Additionally, this section will cite the ways that are available for connecting to the Internet.

2.3.1 Development of the Internet

ARPANET was conceived with the underlying principle of “open architectural networking”. This type of architecture allows all the networks that will be interconnected to have the freedom to choose the network technology to implement independently without being restricted by other networks. In addition, it allows interconnected networks to work together seamlessly (Leiner et al., 2009). Thus, ARPANET could be linked to the other networks that existed at that time.

In contrast, the original model of ARPANET was intended to connect a limited number of networks. Thus, connecting various networks and computers called for major network changes. One of the many changes that took place was the introduction of TCP/IP. This protocol was intended to manage the way computers and networks communicated with one another (Leiner et al., 2009).

As time went on, even more computers were connecting to the Internet. As a result, Domain Name Server (DNS) came into being as a means of handling computer addresses. In addition to the changes in infrastructure was the development of applications and software that would run on the Internet. These included web browsers and the World Wide Web. In sum, these changes led to Internet access being spread to thousands of connected networks in different continents (Leiner et al., 2009).

Subsequently, the Internet became commercialised and Internet Service Providers (ISPs) came into play offering Internet-related services. This paved the way for the Internet to become a commodity (Leiner et al., 2009). Although the software and network structure of the Internet have advanced immensely, it continues to have the underlying principles and networking technologies of the initial ARPANET. Such technologies include TCP/IP together with switching. Today, however, connecting to the Internet is not restricted to mainframes. For this reason the following subsection will cite some of the devices that are currently being used to access the Internet.

2.3.2 Connecting to the Internet

In comparison with the ARPANET era, the way to access the Internet has changed. In addition, the number of computers that can access the Internet is unlimited and the devices that may be used to connect to the Internet have also changed. Today one can access the Internet using fixed or portable computing devices (Lehr & McKnight, 2003). A fixed computing device typically refers to desktop computers. However, there are various portable devices for accessing the Internet which include the following:

- cell phones
- personal digital assistants (PDAs)
- smart phones
- tablet computers
- notebook computers

One of the most popular mobile devices used to connect to the Internet is the Blackberry smart phone. Blackberry plays a huge part in connecting people as it simplifies the accessing of online services through services such as Blackberry Internet Service (BIS) and Blackberry Enterprise Server (BES) connection types (Blackberry, 2013). Typically, broadband technology is used for Internet connection.

Broadband has an “always on” feature which makes it faster than the dial-up connection type. Broadband technologies include wired or fibre optic cables or wireless connections (Lehr & McKnight, 2003). In contrast to portable devices, which use the wireless connection type, desktop computers generally use a fixed line to access the Internet.

The Internet has changed immensely over the years, as have the devices and connection technologies used to access Internet services. It is those services that are accessed through an Internet connection that have given birth to the prominent virtual reality; in this case cyberspace. It should be noted that while the Internet is technically the backbone of cyberspace, the terms ‘cyberspace’ and ‘Internet’ are often used interchangeably. Therefore this study will adopt this perception.

This section provided a high-level summary on the original network design of ARPANET. Moreover, it cited some of the means that are available to connect to the Internet. The following section will discuss the services afforded by the Internet in the modern day.

2.4 Cyberspace in the modern day

In the modern day, the Internet has an enormous impact on the way things are done. It allows a person the ways and means for sharing information and ideas quickly, easily and cost-effectively (Bremmer, 2010). As a result of what the Internet offers, it has become a fundamental part of the lives of many, both socially and professionally. Being online presents opportunities that make living easier and more convenient (Lehr & McKnight, 2003). Consequently, more and more people are using cyberspace, as can be seen in figure 2.1 provided by the International Telecommunication Union (ITU). This figure shows the percentage of online users in 2011 (International Telecommunication Union, 2012).

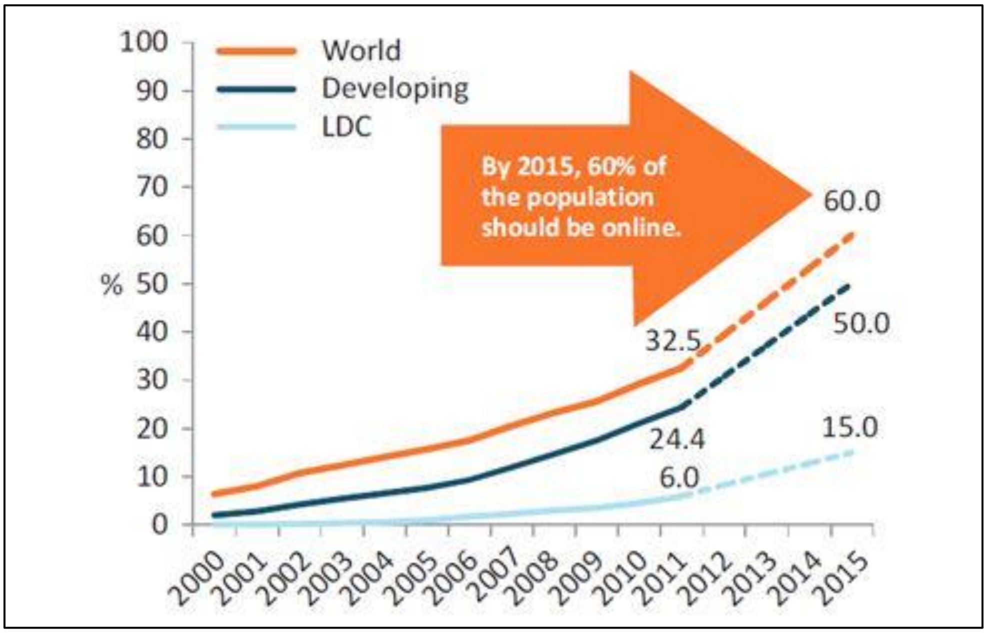


Figure 2.1: Percentage of individuals using the Internet (International Telecommunication Union, 2012)

The number of Internet users has increased exponentially over the years. Thus, the ITU predicts that by 2015, 60% of the world's population will be online. The Internet affords a wealth of services, including communication mediums, online information libraries, social networks and more. The following subsections will explore some of online services in detail.

2.4.1 Communication

The Internet is an international communication medium connecting billions of users across the globe. The way in which people communicate with one another is increasingly through electronic means rather than physical (Duderstadt, Atkins, & Van Houweling, 2002). This is due to the fact that the digital nature of the Internet transcends the capabilities in the physical world (Davinson & Sillence, 2010). For example, one can send an email to a recipient on the other side of the world, and the email is delivered in seconds. Such a timely transfer of information, independent of geographical factors, is a benefit credited to the existence of the Internet.

The Internet is used for both professional and interpersonal communication. Many people use it to send greeting cards and invitations to their family and friends. Further, people use the Internet for the purpose of planning meetings and organising dates (Fallows, 2005) and, for communication purposes, emails and Instant Messages (IM) have become popular (Radicati, 2012). Email communication is by far the most popular because information can be easily exchanged in a timely manner (Purcell, 2011).

In 2012 alone, statistics show that the total number of email accounts worldwide was 3,3 billion. However, this number is expected to increase to 4,3 billion by the end of 2016. Instant messages are also continuing to grow and the number of IM accounts in 2012 was 2,7 billion with an expected average annual increase rate of 6% (Radicati, 2012).

2.4.2 Digital library

Beyond communication, the Internet serves as a digital library. Accordingly, it has altered the way in which people seek information in that acquiring information has been simplified to entering keywords in a search engine and in return having a number of options to choose from (Bremmer, 2010; Duderstadt et al., 2002). It not only provides its users with information of all kinds but also makes it easy to manipulate and redistribute the information (Bremmer, 2010).

The Internet is also used on a regular basis for weather updates, sports scores, getting directions and news updates, to mention but a few uses (Fallows, 2004). Moreover, people seek information about others online. Such information includes home addresses and telephone numbers. A survey conducted in America in 2003 showed that over 80% of Internet users use online resources to get information on anything of interest, be it religious, health or anything else (Fallows, 2004).

This survey also reported that users feel that the Internet enables access to information that, traditionally, would have taken days to gather using offline resources. Users view the Internet as a quick and effective resource for information about matters of daily interest (Fallows, 2004).

Beyond providing information on personal interests, the Internet has influenced the way professional research is done. Finding scholarly research articles has been simplified with online databases and online journals. In addition, researchers can find and distribute their findings to a broader audience with ease (Anderson, Boyles, & Rainie, 2012).

2.4.3 Socialising

According to Bremmer (2010), the Internet has given its users limitless freedom – freedom to associate with whomever, wherever, whenever. As a result of such freedom, Healy (1997) suggests that through access to online services one lives an idyllic life, as one is free to interact with users of one's choice, users that share similar interests and goals. The Internet provides a platform for discussion where people with similar interests can share ideas and opinions. In essence, the Internet provides "limitless potential for an associational life" in more ways than one (Healy, 1997). This includes personal blogs, chat rooms and social networks. A number of social networks are available online, including the following (Duggan & Brenner, 2013):

Facebook

Facebook is the second most visited website, with millions of users across the world (Gentile, Twenge, Freeman, & Campbell, 2012). Facebook users share information constantly throughout the day by uploading photos and updating their status. Facebook is not only used by individuals, however; organisations also make use of this service for various purposes including marketing and advertising (Duggan & Brenner, 2013).

Twitter

In 2012, the percentage of Internet users that uses Twitter had doubled since 2010. Twitter users span different age groups and interact regularly on a daily basis. More and more adults are making use of Twitter's blogging service (Duggan & Brenner, 2013).

Pinterest

Pinterest is an online pinboard site. It allows its users to create, edit and share photos and videos with other users. Pinterest users can pin images together with other objects on their pinboards. They are also able to browse various other pinboards and create online scrapbooks. This social network has interested 15% of the online population from young users to adults (Duggan & Brenner, 2013).

Tumblr

Tumblr is a blogging website. It is not as popular as other social networks as it has attracted only 6% of the online population. It is, however, popular with the youth (Duggan & Brenner, 2013).

2.4.4 E-commerce

E-commerce is defined as an electronic means of buying and selling goods and services. Typically, this may be over the Internet or by means of email (Allen & Fermestad, 2000). There are two types of e-commerce, business-to-business (B2B) and business-to-customer (B2C). On one hand, B2B concerns itself with intercompany transactions and relationships within companies (Furling & Digman, 2000); while on the other hand, B2C refers to the trade conducted between a company and a customer (COMESA, 2013).

Examples of B2B e-commerce are those of manufacturer to wholesaler and wholesaler to retailer. B2C, on the other hand, affords consumers an opportunity to shop online. This is seen as a very convenient and cost-effective way of shopping. Additionally, online shopping transcends geographical factors, such that it allows one to shop anywhere in the world.

One of the numerous shopping websites is Amazon. Amazon is the most popular online shopping website (O’Connor, 2013), selling a wide range of products including books, digital devices, CDs, DVDs and more.

2.4.5 Entertainment

There is also room for entertainment online. Many people use the Internet for enjoyment and to pass the time. Entertainment activities include watching movies, watching music videos, downloading/listening to music, playing games and many more (Fallows, 2004)

In a survey done in America in 2012 to explore the ways in which people entertain themselves online in their daily life, the following findings were reported (PEW Internet, 2012):

- 36% play games online
- 84% go online to pursue their hobbies
- 23% listen to online music or radio
- 74% surf for pleasure and to pass the time
- 71% watch videos.

As can be seen from the above list, there are many ways in which people can entertain themselves online.

2.4.6 Education

Over and above entertainment, the Internet is also used for educational purposes such as teaching and learning. Teachers perceive the Internet as a tool that assists in conveying much of the information students need to learn (Eynon, 2005). Concurring with this claim, Purcell and colleagues maintain that “the internet enables students to access a wider range of resources than would otherwise be available” (Purcell, Rainie, Buchanan, Friedrich, Jacklin, Zickuhr, 2012). Thus, the Internet supports both the duties of the teacher and the objectives of the student.

Some of the benefits of using the Internet in the educational realm are the following (Jefferies & Hussian, 1998):

- It supports a more holistic and multifaceted approach to education.
- It removes time and place constraints.
- It eliminates dependence on conventional means of learning.
- It provides an environment suitable for collaborative working.

Cyberspace has introduced a variety of innovative ways of doing old things; in the same manner it has introduced humankind to a variety of new inventions. This is visible in the way that this phenomenon has been integrated into the daily lives of many. This section discussed the services available online, although these services are only a selection of what is currently offered online. As many people have grown dependent on these services, the following section will elaborate on this by exploring just how dependent individuals, organisations and nations have become on cyberspace.

2.5 Reliance on cyberspace

The President of the United States of America Barack Obama, defined cyberspace as a world of its own, a world that every level of humanity relies on to function every single day. He further stated that cyberspace is a collaboration of the hardware and software that has been interwoven in the lives of many. Moreover, many schools, hospitals and businesses, together with the infrastructure that empowers a nation, are entirely dependent on cyberspace. Most importantly, cyberspace has connected many levels of humanity in a manner that is historically very significant (The White House, 2009b).

The pervasive nature of cyberspace and the endless list of services it has made available have resulted in individuals becoming dependent on it for personal and professional activities. These may encompass online banking, shopping and/or communication. Cyberspace is not only interwoven in the daily lives of individuals, but has also found its way into the fabric of businesses and, indeed, nations. It is defining the way things are done from both a personal and a professional perspective. Consequently, the reliance on cyberspace to function could not be greater. The rest of this section will discuss in detail the reliance of individuals, organisations and nations on cyberspace.

2.5.1 Individual

The Internet plays a significant part in the day-to-day lives of many. It is interwoven in the way people communicate; the way they obtain information; the way they conduct daily transactions and the way they entertain themselves (Fallows, 2004). On the subject of communication, email usage cannot be stressed enough.

To date, email remains the most effective way to communicate in both a personal and a professional capacity. As a result email is the most popular online activity and 92% of all Internet users use email (Purcell, 2011). Despite its popularity, it is not the only service that is used to communicate online. As mentioned in section 2.4, such services include social networks, IM and chat rooms.

In 2011, Blackberry users all over Europe, the Middle East and Africa could not access online services. This was due to some technical issues experienced by Blackberry Research in Motion (RIM). This disruption of services rattled Blackberry users as they struggled to cope without being online. As a result of the inability to access emails, BBM and Twitter using a Blackberry smart phone, one of the users wrote on Twitter, "I may as well cut one of my arms off too *angry face*" (Williams, 2011). This reaction clearly demonstrates how users have become accustomed to online services and, furthermore, that being online is regarded by some as essential to their way of life.

From an interpersonal view, relying on cyberspace can reach a degree of addiction. Internet addiction stems from an excessive use of the Internet. It is a behavioural disorder manifested by various factors such as the need to use the Internet, feeling depressed if attempting to cut down access and using the Internet to escape reality (Young, 1998).

Owing to the prominent role of the Internet in society, many deny that they may be addicted because they feel that everyone is “online”. Also, the fact that some use it mainly for work-related matters makes it easy for them to be in denial (Young, 1999). However, it is worth noting that depending on the Internet to carry out certain tasks does not imply Internet addiction.

The advantages that come with using cyberspace render the physical way of doing things redundant. Consequently, people are becoming generally reliant on or even addicted to cyberspace in order to function. The following subsection will discuss how organisations are subject to cyberspace dependence.

2.5.2 Organisational

Electronic transacting has emerged as the modern way of doing business. Businesses have taken the opportunity to conduct commerce online, providing services that would normally require customers to go to physical locations. Some of these services depend entirely on the Internet to be delivered while some are aided by the Internet. This to a large extent has made organisations reliant on cyberspace.

Whether cyberspace serves as a marketing and advertising medium or just as an initiative to improve service delivery, it is nevertheless a foundation for new ways of conducting business (Gascoyne & Ozcubukcu, 1997). In addition, the Internet has been proved to offer a platform where industries can grow while simultaneously cutting costs and reaching a wide spectrum of customers in various countries across the world (Yakhlef, 2001). This platform has brought about innovative change, as can be seen by the number of industries that operate on it, including banking, retail and air travel, along with the publishing and media industry.

Banking industry

The manner in which banks have embraced online banking can be mistaken for replacing face-to-face communication. Conversely, Yakhlef (2001) believes that transacting online strengthens and complements the banking industry. Hence, migrating some of banking services to online services has given bankers more room to expand the services they provide. Furthermore, banks that use cyberspace to complement traditional distribution channels achieve the following (Yakhlef, 2001):

- better communication with customers
- better interactivity
- a decrease in transaction processing
- solid ties with customers.

These achievements are in line with the strategic aim banks have for using the Internet. As reported in a study done in the United Kingdom (UK), banks use the Internet for the following reasons (Daniel & Storey, 1997):

- to protect or enhance the organisation’s reputation for innovation
- to provide added value to customers
- to attract new customers
- to follow the route taken by competitors in launching online services
- to save costs
- to explore the existing potential to develop mass customised services.

Retail industry

In addition to banking online, people have taken liking to shopping online. In this day and age this is a novel way to shop. Online shopping enables customers to purchase goods and services from the seller over the Internet without a mediator (Chen, 2012). This way of shopping is attracting customers for the following reasons (Chen, 2012):

- convenience
- broader selection
- competitive pricing
- greater access to information.

Bricks-and-mortar retailers are also moving towards transacting online because of the simplicity of online shopping (Burt & Sparks, 2003). In the same manner, more and more organisations in different industries are making use of online capabilities.

Airline industry

According to Buhalis (2004), the airline industry has become highly dependent on technology, the Internet in particular, for operational and strategic management. On an operational level, the Internet enables day-to-day activities such as meeting customer needs and intercompany collaboration. On a strategic level, in part, the Internet supports the industry by empowering internal processes.

Buhalis (2004) also contends that the Internet enables the airline business to portray its competence to a wider audience. Similar to other industries, the Internet plays a vital part in communication for customer relations. Furthermore, in the airline industry close collaboration between different partners is crucial for delivering their service. Thus the Internet is beneficial. The cost-effectiveness and flexibility of the Internet serves as a pillar for the competitiveness of the industry (Buhalis, 2004).

Publishing and media industry

Cyberspace has transformed the publishing and media industry. Nowadays, audiences are increasingly moving away from traditional media such as television, newspaper and radio to online media (Leurdijk, Slot, Nieuwenhuis, Jean, & Simon, 2012). Figure 2.2 below demonstrates the spike in online audience.

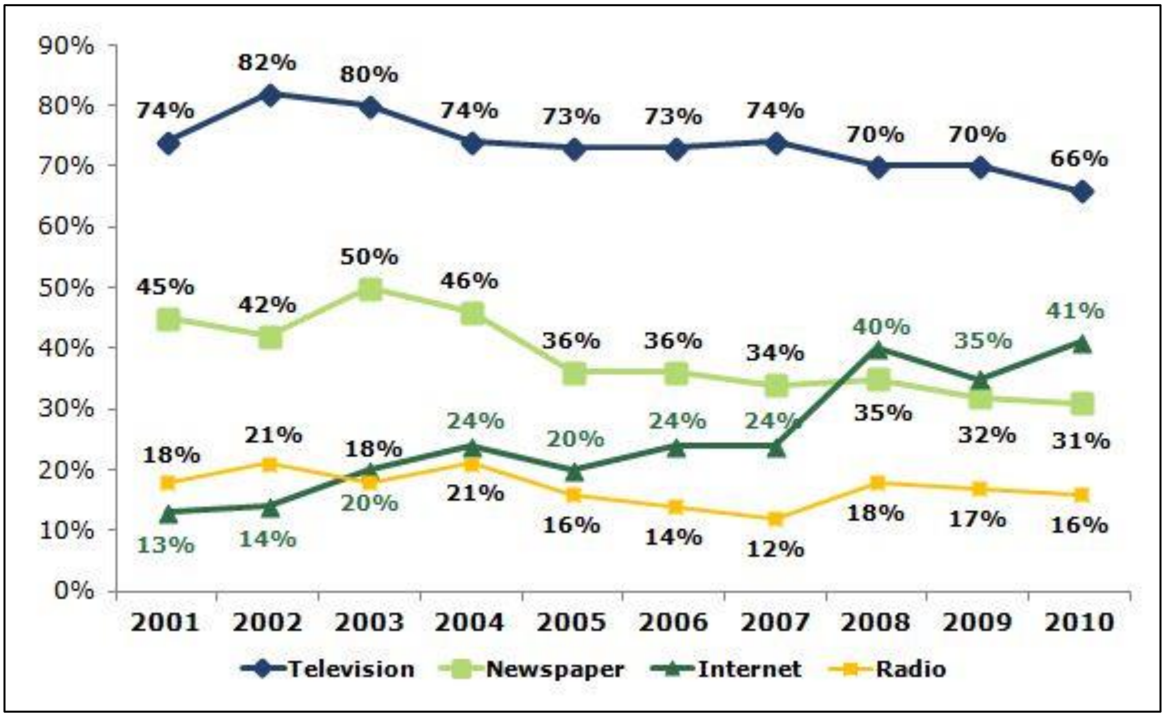


Figure 2.2: News consumption sources US (Leurdijk et al., 2012)

As seen in figure 2.2, online news is progressively taking precedence. In response, news companies are using online platforms whereby people can access the news. These platforms include news websites, portals and even social networks. Pew Internet (2011) also indicates that people prefer using the Internet to access news to newspapers. As a consequence, traditional media have suffered as people move online. There is no question that this industry is relying increasingly on the Internet.

The advantages of cyberspace cannot be overlooked by any facet of the business world. Thus, the industries mentioned in this section are just a few examples of way in which the Internet has altered the way of doing business. The following subsection will discuss the extent to which nations are dependent on cyberspace.

2.5.3 National

From a national perspective, cyberspace is embraced differently by developed countries and developing countries. This is due to a number of factors which include how technologically advanced a country is. For developed countries the question no longer lies on whether or not a country is ‘online’, but rather for what cause and to what end is the country online (Chadwick & May, 2003). Developed countries have long seized the opportunity to use cyberspace to govern. Such countries include the US, Europe and Australia to name but a few (Chadwick & May, 2003). Two distinctive ways in which countries use cyberspace is for e-government and in the realm of critical infrastructure.

Cyberspace for e-government

Among other benefits brought about by cyberspace is the opportunity for governments to communicate with citizens directly in a cost-effective and user-friendly manner. Likewise, the Internet removes the barriers of information dissemination between governments and citizens (Conklin & White, 2006). In addition, it gives citizens a platform to contribute to policy making (Ho, 2002). Moreover, the transparency contributed by cyberspace to governing can enable citizens to influence government decision-making.

The growing dependency on an electronic way of life has put pressure on government to serve citizens online (Ho, 2002). Furthermore, as society becomes ‘online’, so are their expectations for government to be ‘online’. In this way, the Internet is reinventing traditional government as e-government. E-government is an initiative aimed at strengthening the relationship between government and citizens with the intention of bringing about coordination of and external collaboration between governments (Ho, 2002).

Cyberspace for critical infrastructure

The US associates cyberspace with critical infrastructure. Critical infrastructure may be defined as “systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters” (Condron, 2007).

According to the Protecting Cyberspace as a National Asset Act of 2010, cyberspace is crucial to the wellbeing of the US (Lieberman & Carper, 2011). This is because cyberspace forms the ‘nerve centre’ of US critical infrastructure and valuable government information is stored and accessed on the Internet. Thus, it also controls a large number of the US critical infrastructure as listed below (Condron, 2007):

- financial systems
- transportation systems
- shipping
- electrical power grid
- oil and gas pipelines
- nuclear plants
- water systems
- manufacturing
- military.

The role of cyberspace in the US is significant, to such a degree that its disruption would be detrimental to the survival of the entire society. It is no different in Europe, as critical infrastructure, economy and communication are highly dependent on cyberspace (Choo, 2011). By contrast, developing countries are far less integrated into cyberspace. However, this is changing rapidly because while the developed countries have led the way to the digital era, developing countries are following suit.

It may be concluded that cyberspace is a world we are dependent on with or without realising it. Moreover, users have grown increasingly accustomed to it. The following section contains some concluding remarks.

2.6 Conclusion

The Internet of yesterday expanded from connecting just a limited number of computers for limited purposes, to the multipurpose limitless cyberspace of today. Cyberspace surpasses geographical factors by providing users with access to information from any part of the world. Similarly, it connects users from all over the world.

Nowadays one can live an ‘online’ life, communicating, transacting, researching and studying online. Such facilities make life today convenient, faster and affordable. Hence, cyberspace has become interwoven into the daily activities of individuals, businesses and nations.

The impact cyberspace has had on its users cannot be denied. Many rely on it to perform functions that are deemed critical to one’s wellbeing. However, cyberspace is not without risks and therefore the risks that go hand in hand with reliance on cyberspace cannot be disregarded. Consequently, the following chapter will discuss the risks associated with cyberspace.

CHAPTER 3: SAFETY AND SECURITY IN CYBERSPACE

3.1 Introduction

“This limitless world – cyberspace – is not without risks (Kortjan & von Solms, 2012)”.

The impact that the Internet has had on the human being’s very way of life cannot be disputed. The Internet plays an essential role in society, industry and the nation at large. As stated in the previous chapter, cyberspace is more than just a set of networked computers; it is a world that many rely on to perform various tasks that they deem important. It is imbedded in the way people communicate, socialise and work. It is furthermore a vital element in modern commerce and is increasingly defining national governance.

Cyberspace has progressively provided innovative ways for carrying out certain tasks, thus the number of Internet users continues to grow exponentially together with their reliance on it. Conversely, although cyberspace affords opportunities, it also poses certain risks to those who use it (Furnell, 2008; Livingstone & Helsper, 2007). As a consequence, there are various threats that users are exposed to when going online and they need to be mindful of these.

This chapter will discuss the risks associated with using cyberspace and it will discuss a number of the threats that may possibly confront the individuals, organisations and nations that rely on cyberspace. Once these threats have been discussed, security in cyberspace will be explored and finally a culture of cyber security will be elaborated on.

3.2 The dark side of cyberspace

Cyberspace has indisputably revolutionised our way of life. It is argued that each revolution brings forth three types of change – the good, the bad and the ugly. With regard to cyberspace, at the outset the good would seem to be the improvement in communication, information seeking, socialising, entertainment and transacting, as mentioned in the previous chapter. By contrast, the bad rests partly in the introduction of new crimes or the modernisation of existing crimes, as will be discussed in detail in this chapter. Finally, the ugly includes all the bad things that spiral out of control due to factors such as human behaviour and inadequate law enforcement (Kim, Jeong, Kim, & So, 2011).

Cyberspace is not without its ‘dark side’. Similar to the real world, flaws do exist, thus it should be expected that even cyberspace will have its flaws. This is primarily due to the fact both the real world and cyberspace are inhabited by the same people (Kim et al., 2011). Moreover, the global reach and the obscure and cross-border nature of cyberspace serve as both an advantage and disadvantage to its users when it comes to its dark side. A suite of risks that individuals, organisations and nations may be exposed to is provided in the subsequent subsections.

3.2.1 Individual

This subsection will discuss some of the risks that individuals are exposed to in cyberspace.

3.2.1.1 Identity theft

The use of online services often requires valuable information to be communicated, stored and processed. Information is a very important asset therefore if it is not properly protected it may be exploited (Von Solms & Von Solms, 2006). Perpetrators may use such information deceptively to inflict harm in many ways. Owing to the quality and quantity of information that is available online, user identities can be stolen and individuals can be impersonated (Marshall & Tompsett, 2005).

Internet services such as online purchasing using credit cards and online banking afford criminals a wealth of personal information. This, in turn, creates a gap for users to become victims of identity theft. In such cases, cybercriminals may use this information to commit fraud such as making loan applications and buying goods using the stolen identity (Marshall & Tompsett, 2005). Therefore, one of the consequences of identity theft is financial loss (Brody, Mulig, & Kimball, 2007).

Obtaining personal information in cyberspace can be achieved by various means, for example phishing. Phishing is carried out by sending out bulk emails which are meant to entice the recipients into willingly revealing personal details. These emails usually seem plausible and important and are sent randomly to many people in the hope that one of the recipients will find the email relevant and be lured into giving out personal information. Unfortunately, there is always one victim who is likely to take the bait (Brody et al., 2007).

An even more malicious form of phishing is spear-phishing. This method targets specific recipients instead of randomly hooking anyone who is likely to respond. The emails in spear-phishing appear to be legitimate and the sender appears to be a reputable source. In this way, the perpetrator selects their target based on an established relationship between the targeted recipient and the fictitious sender (Brody et al., 2007).

3.2.1.2 Online financial fraud

Financial fraud presents itself in many forms. These include real estate fraud, debit and credit card fraud and identity theft (Paget, n.d.). While identity theft concerns itself with acquiring as much information as possible in order to impersonate someone with the intention of carrying out various fraudulent activities, financial fraud is primarily concerned with the financial intent behind these types of fraud (Fletcher, 2007). As the name suggests, online financial fraud occurs in the realm of cyberspace.

As previously mentioned in subsection 3.2.1.1, cyberspace contains a wealth of personal information that may be used by cybercriminals to commit fraud. Criminals target particular people, gathering their financial information and using device scams to make quick money (Blanton, 2012). Nowadays, criminals are using social networks, such as Facebook, to target potential victims. As a result, there is an increase in the scams that are perpetrated through cyberspace (Wall, 2010).

It is reported that financial fraudsters posing as investment companies are likely to target senior citizens. Blanton (2012) suggests that this is potentially due to three characteristics of senior citizens. Firstly, this generation is more likely to have accumulated large amounts of money for retirement. Secondly, it is more likely to have large amounts of life savings. Finally, fraudsters may take advantage of the cognitive decline that comes with aging (Blanton, 2012). However, it is not only senior citizens that become potential victims. Everyone who is enjoying online services is a probable victim. In addition, scammers assume diverse personalities to appeal to different types of people or groups (Kim et al., 2011).

Similar to identity theft, financial fraudsters use phishing as one of their information gathering tools. They also use a method called pharming, which in essence is not very different to phishing (Brody et al., 2007). However, instead of using email to entice their potential victim, the fraudsters secretly install a malicious program on a computer and when users type in a website address they are redirected to a replica of the website. Using these methods fraudsters can accumulate large amounts of personal and financial information without users' knowledge.

3.2.1.3 Online child grooming

Although cyberspace has proven to be an advantage in so many facets of life it has also proven to be a disadvantage in the wellbeing of its users, predominantly children. Children in cyberspace often fall victim to sex predators that deceive and manipulate them into engaging in sexual conversations. It is no doubt that such deceitful acts existed before the existence of cyberspace (Wolak, Finkelhor, & Mitchell, 2005). However, the Internet granted a platform on which offenders can sexually groom children without raising suspicion (Krone, 2004). Sexual predators are also making use of cyberspace to lure unwary children into criminal activities such as child grooming and child pornography.

Child grooming is defined as intentional behaviour that is meant to capture the confidence and cooperation of children prior to engaging in sexual conduct. It is a process through which the offender takes a particular interest in a child victim with the aim of making them feel unique in order to gain their trust. All these efforts are in the quest of exposing the child to sexual conduct by means of introducing a sexual element into the established relationship (Choo, 2009).

It is the anonymous and deceptive nature of cyberspace that permits offenders to pretend to be children with the intention of gaining the trust of their victims. Another feature of cyberspace that aids an offender in the grooming process is the lack of visual cues. Visual cues would assist the victims in making the correct judgement about the appropriateness, credibility and honesty of those they communicate with online (Choo, 2009).

Once the offender has attracted its victims, it takes some time to ensure that they have won their trust before exposing them to sexual elements (Choo, 2009). In addition to exposing children to sexual material, the offenders have been known to fish for personal information from children for the purposes of further potential criminal activity, such as the fraudulent use of the information.

3.2.1.4 Cyber bullying and harassment

Cyberspace has extended the traditional bullying in schoolyards to bullying in cyberspace. Traditionally, bullying involves the abusive and aggressive treatment one experiences from another person. It can occur in three forms: physical, verbal or a combination of both. Physically, the perpetrator may punch, hit or spit at the victim. Verbally, the perpetrator may tease, insult or be sarcastic towards the victim (Campbell, 2005). Contrary to traditional bullying, the contemporary form of bullying involves the use of electronic tools to deliberately inflict harm on others. This type of bullying is known as cyber bullying (Li, 2007).

Cyber bullying entails the use of text messages, instant messages (IM) and/or emails to deliberately cause harm to others. The use of these mediums makes cyber bullying even more rigorous than traditional bullying because the perpetrator can easily reach their victim without the constraints of time and location (Swartz, 2009). In addition, it is argued that cyber bullying is even more intimidating in comparison with traditional bullying in the boundaries of a schoolyard. This is attributed by the limitlessness of cyberspace, as the teasing and insults online is just as limitless. In accordance with this, Li (2007) reports that online bullies feel invincible because there is no face-to-face interaction with the victim and this allows the bully to say anything they like.

With traditional bullying, school children were generally bullied by their peers. However, cyber bullying has extended the category of bullies, as one now finds adults victimising children (Swartz, 2009).

3.2.1.5 Cyber stalking

Mullen, Pathé, Purcell, and Stuart (1999) define stalking as a behaviour that involves persistent and repeated efforts to forcefully compel communication or contact on an unwilling person. This behaviour often threatens and instils considerable fear on the one who encounters it (Mullen et al., 1999). Cyber stalking is no different from traditional stalking in that it also imposes unwanted communication in a forceful manner which, consequently, instils fear in the victim. However, the difference in traditional and cyber stalking is the medium of communication used. Cyber stalking makes use of electronic communication mediums such as email (Philips & Morrissey, 2004).

There are three known varieties of cyber stalking, namely, email stalking, Internet stalking and computer stalking (Ogilvie, 2001). In email stalking, as the name suggests, email is primarily used for communicating. The stalker will send threatening and harassing emails to the victim. Moreover, the stalker may spam the victim by sending vast amounts of junk email. When considering the fact that in traditional stalking stalkers use mail and telephone to intimidate the victim, email stalking presents itself as the most similar to traditional stalking (Ogilvie, 2001).

In Internet stalking, the stalker can track the victim's online activities, following the victims while online, from site to site. Moreover, in some instances the stalker will post false information intending to scare the victim. This form of stalking is often accompanied by traditional stalking tendencies such as threatening mail and phone calls or even physical assaults. Thus, the line between physical stalking and cyber stalking is often blurred (Ogilvie, 2001).

Unlike Internet stalking, computer stalking does not spill over into physical harassment; however, it uses the Internet to assume control of the victim's computer. Therefore this form of stalking occurs when the stalker gains unauthorised control of the victim's computer intending to have direct communication with the victim (Ogilvie, 2001). Accordingly, email, Internet and computer stalking all occur in the realm of cyberspace.

There are many dangers that individuals are exposed to in cyberspace. This sub-section highlighted just some of these threats. The following subsection will explore cyberspace threats associated with organisations.

3.2.2 Organisational

This subsection provides insight into some of the risks that organisations are exposed to in cyberspace.

3.2.2.1 Cybercrime

Cybercrime is the term used to refer to Internet-based criminal activities (Gorge, 2007). There is a wide range of cybercrimes; however, this subsection refers to cybercrime against businesses. The National Computer Security Survey (NCSS), developed by the US Department of Justice to produce quality data in relation to cyber intrusions against industry, suggests three types of cybercrime that are perpetrated against organisations (Davis, Golinelli, Beckman, Cotton, Anderson, Bamezai, Steinberg, 2008). These include cyber-attacks, cyber theft and other computer security incidents. In cyber-attacks, computer systems are targeted by means of computer viruses such as worms, Trojan horses, and denial of service (DoS) attacks. For cyber theft, computer systems are used to steal money and/or valuable information, and to commit fraud (Davis et al., 2008). Other computer security incidents encompass hacking in to company systems and theft of privileged information.

A cyber-attack such as a DoS attack prevents customers from accessing a particular service on the Internet. It does this by flooding the organisation’s server with millions of false requests. These requests are intended to overwhelm the targeted system and further utilise all the capacity it generally uses to handle customer demand (Burden &

Palmer, 2003). Besides forging requests, the perpetrator may create excessive error messages that need to be logged by the system or may even exploit network flaws. These methods are all intended by the perpetrator to disrupt the operation of the targeted system.

DoS intrusions are attacks that appear to be genuine system entries therefore they are difficult to prevent (Kim et al., 2011). The perpetrator does not, at any stage of the attack, break into the system or attempt to take control of the system as hackers do (Kim et al., 2011). By contrast, hackers use cyberspace to gain unauthorised access to the targeted system, with the aim of committing cyber theft, stealing intellectual property or information or committing fraud (Kim et al., 2011).

Both cyber-attacks and cyber theft have an adverse effect on organisations, costing businesses a great deal of money. In addition to monetary loss, there is the downtime that businesses have to face as a result of cybercrime. Rantala (2008) reports that many businesses suffer both these effects of cybercrime.

3.2.2.2 Industrial espionage

Industrial espionage is defined as the spying of one company on another with the aim of gaining a commercial advantage (Jones, 2008). This encompasses theft of company secrets and sensitive information that has a bearing on the competitiveness of an organisation (Introduction to the new old world of netspionage, 2000). Industrial espionage, like many other crimes, is not a new crime. However, nowadays criminals are using cyberspace as a new frontier for such crimes.

In essence, online industrial espionage involves the use of technology, particularly the Internet, to spy in order to gain access to and steal sensitive information from a rival company (Kovacich, 2000). Some of the fundamental rationales for espionage include increasing economic power and gaining competitive advantage. Spies are at an advantage as organisations are becoming increasingly digitalised. For this reason company secrets have become fairly easy to access with the aid of cyberspace (Moore, 2010). Industrial espionage is difficult to recognise because while the spy may have access to a company's sensitive information, the victim can also access the information.

Cyberspace serves not only as a benefit to organisations, but also as a disadvantage in some instances as it is associated with various risks. This subsection mentioned some of the risks to organisations that are apparent in cyberspace. The following subsection will discuss cyberspace threats related to countries and nations.

3.2.3 National

This subsection will elaborate on some of the risks that nations are exposed to in cyberspace.

3.2.3.1 Cyber terrorism

There is much debate on what the term 'cyber terrorism' actually means (Gorge, 2007). On one hand it is argued that this term has been overused and furthermore misused. On the other hand it is argued that the line between cyber-attacks and cyber terrorism is often blurred (Embar-Seddon, 2002). Generally, however, cyber terrorism can be defined as the employment of information and communications technology (ICT), in this case cyberspace, by an individual and/or terrorist group to implement its agenda (Gordon & Ford, 2002). Cyber terrorism includes the use of cyberspace to arrange and perform cyber-attacks against the targeted computer systems, networks or critical infrastructure. It also encompasses terrorist threats made via electronic communication such as email, hacking into computer systems and DoS attacks (Gordon & Ford, 2002).

According to Schudel and Wood (2000), the main characteristics of cyber terrorists are the following:

- Regardless of the assumption that they have only limited funds cyber terrorists are able to accumulate the funds they need to further their agenda.
- They have the ability to access commercial resources which include consultants and commercial skills.
- They are likely to be able to attain all the design information pertaining to a system that they deem to be appealing.

Taking these characteristics into consideration, cyber terrorists are skilful; moreover since nations relate cyberspace to their critical infrastructure, cyber terrorists see this as a gap that they can exploit. The motivation behind cyber terrorism may be political or social, but whatever the motive, cyber terrorism negatively affects the targeted nation. Such effects may be economic since modern economies rely heavily on cyberspace (Hua & Bapna, 2012). Cyber terrorism is a real threat to nations and should be taken seriously and handled as such.

3.2.3.2 Cyber warfare

Similar to cyber terrorism, there is much debate regarding the definition of cyber warfare (Nicholson, Webber, Dyer, Patel, & Janicke, 2012). The US 2001 Congressional Research Service Report for Congress on cyber warfare states that: “Cyber warfare can be used to describe various aspects of defending and attacking information and computer networks in cyberspace” (Hildreth, 2001). Fundamentally, in cyber warfare cyberspace is the battlefield. On this battlefield, attackers use a range of cyber ‘weapons’ to sabotage the targeted country. These weapons take the form of DoS attacks, hacking and malicious software (malware) (Ophardt, 2010).

According to Nicholson and colleagues (2012), there are two types of adversary – internal and external. Some internal adversaries are disgruntled employees and hackers in a country and some external adversaries include terrorists and non-state hackers.

Cyber warfare has features that an adversary is likely to find beneficial, some of which are the following (Molander, Riddile, Wilson, & Williamson, 1996):

- *Low entry cost*. Nowadays it is not costly to own a computer with an Internet connection; moreover the Internet has information about what can be used as weapons in cyber war.
- *Blurred traditional boundaries*. The opponent can be anywhere in the world. This makes it hard for the country that is being attacked to respond.
- *Difficulty of practical warning and attack assessment*. In cyberspace anyone can initiate a cyber-attack; as a result it is difficult to separate an attack from a thrill seeker from an attack from an enemy.

Cyber warfare is most likely to have a real impact in countries that are highly integrated in cyberspace. As mentioned in subsection 2.5.3, such countries include the US and the UK, as the critical infrastructure of these countries is related to cyberspace. In such cases, the critical infrastructure becomes the target of politically motivated cyber-attacks.

Cyber terrorism and cyber warfare are just a couple of the potential risks that face nations relying on cyberspace for critical operations. The following subsection will discuss the existing overlap in threats to individuals, organisations and nations.

3.2.4 The overlap between threats to individuals, organisations and nations

Often individuals, organisations and nations are exposed to altogether dissimilar threats. An example of this would be that an organisation or a nation is not exposed to cyber bullying and cyber stalking as individuals are. However, with that said in some instances there is an overlap. This overlap is noticeable predominantly in identity theft. Organisations can fall victim to identity theft just as individuals can (Milne, Rohm, &

Bahl, 2004). In addition to identity theft, cybercrime does not affect organisations only; all users of cyberspace are vulnerable to such crime.

It is also important to note that the overlap is not only in the threat itself, but also in the impact of the threat. An example would be if an employed individual’s computer is hacked into and it happens to contain sensitive company information; then the damage suffered by the individual in this event may also have an impact on the organisation. Thus, such an overlap is an indication that some users can render other users vulnerable.

All users of cyberspace at all levels of society or the corporate world, or even at government level, need some form of safeguard against cyber-related offences, not only to protect themselves but also other parties that might be affected. Moreover, the dark side of cyberspace affects all its users, particularly those who depend on cyberspace to perform certain tasks.

This section identified some of the risks that individuals, organisations and nations are exposed to in cyberspace. It furthermore discussed the noticeable overlap of these risks between the different parties. The following section will discuss security in cyberspace by introducing information security and cyber security and, furthermore, elaborating on how these security domains are related. The following section will discuss how cyber security can be put into practice and, in conclusion, the fostering of a cyber security culture.

3.3 The need for security

In cyberspace, the identity of the user can be revealed by the information they communicate online (Milne et al., 2004). This is because online services often involve the communication, transmission and processing of valuable information. It is this information that becomes vulnerable to the threats that are apparent online (Thomson &

Von Solms, 2005). Thus, it can be concluded that it is unlikely that users of cyberspace – individuals, organisations and nations – will be safe online if the information used is not properly secured. Based on this deduction, the effort of securing cyberspace is closely related to information security. This section will elaborate on this correlation by defining both information security and cyber security. Moreover, it will discuss how cyber security can be implemented, as suggested by the cyber security guide of the International Telecommunications Union (ITU).

3.3.1 Information security and cyber security

Information security is defined as the protection of information from various threats that have the potential to compromise the confidentiality, integrity and availability of information (ISO/IEC 27002, 2005). The confidentiality, integrity and availability of information are usually referred to as CIA. Confidentiality refers to information being accessible only to authorised people; integrity refers to information being reliable, unaltered and complete; and availability refers to information being available at the correct time to authorised users (ISO/IEC 27002, 2005). Therefore, information security ensures that the correct information is constantly available and accessible to authorised users.

Information security is put into practice to ensure business continuity and minimal risk to the organisation, as well as to increase return on investment and business opportunities (Futcher, Schroder, & von Solms, 2010). It involves employing appropriate controls, policies, procedures and processes that will ensure the CIA of information in an organisation. Thus, in the main, information security is concerned with protecting information in an organisational setting.

Securing information is, however, a necessity even beyond the boundaries of an organisation. This is because the use of online services, as already mentioned, often involves sharing and disclosing information. In contrast, while there is a close correlation between information security and securing cyberspace, there are aspects in securing cyberspace that fall outside the scope of information security (Von Solms & Van Niekerk, 2013). Thus, a separate security domain has materialised, known as cyber security.

According to ISO/IEC 27032, cyber security may be defined as the preservation of the CIA of information in cyberspace (ISO/IEC 27032, 2012). This definition is directly adapted from that of information security. ISO/IEC 27032 suggests that cyber security is concerned with what users and service providers should do in order to establish and maintain security in cyberspace (ISO/IEC 27032, 2012).

The ITU identifies a number of things that can be done when approaching cyber security. It suggests, for example, the implementation of cyber security policies, best practices and security guidelines. The following section includes an overview of cyber security as a process, as indicated by the ITU.

3.3.2 Cyber security – a course of action

According to the ITU, the illicit use of cyberspace has the potential to negatively affect the economy, public health, safety and the overall security of a nation (Wamala, 2011). As it is the role of every government to ensure the overall security of a nation and its citizens, cyber security then becomes the duty of government. Moreover, in view of the fact that there is an evident dependency on cyberspace, cyber security should be a national priority.

The ITU encourages nations to adopt a holistic, multi-stakeholder and strategy-led approach when addressing cyber security. Thus, the ITU identifies ten elements which it considers important in a strategy-led national cyber security programme (Wamala, 2011).

1) *Top government cyber security accountability.* The government is responsible for establishing a cyber security strategy. Not only that, but it is also responsible for promoting cooperation between local, national and international entities.

2) *National cyber security coordinator*. An office or an individual should be given the role of overseeing cyber security activities.

3) *National cyber security focal point*: This is a body that serves as a central point for all cyber security-related activities.

4) *Legal measures.* It is normal for a country to review or, if needed, draft new criminal regulations, measures and policies to discourage, counter and act against cybercrime.

5) *National Cyber Security Framework*. This is a framework that stipulates the least number of security requirements, as well the compulsory security requirements.

6) *Computer Incident Response Team (CIRT)*. This is a dedicated team that will coordinate all the necessary information on cyber threats.

7) *Cyber security awareness and education*. There should be a national programme that will be dedicated to raising awareness on cyber threats.

8) *Public–private sector cyber security partnership*. Relevant partnerships should be established by the government between the public and the private sectors.

9) *Cyber security skills and training programme*. There should be a programme in place to prepare cyber security professionals.

10) *International cooperation*. The global nature of cyberspace calls for international relationships.

The first element identifies the government as being responsible for cyber security. As such, the government should define a strategy that will lead to cyber security activities. Taking the above-mentioned elements into consideration, the ITU proposes a model that can assist in devising a holistic national cyber security strategy (Wamala, 2011). This model captures the elements that a national cyber security strategy should have in order to ensure security for all users of cyberspace. Figure 3.1 below is adapted from the ITU's National Cyber Security Strategy Model (Wamala, 2011). It has been redrawn by the author using Microsoft Visio.

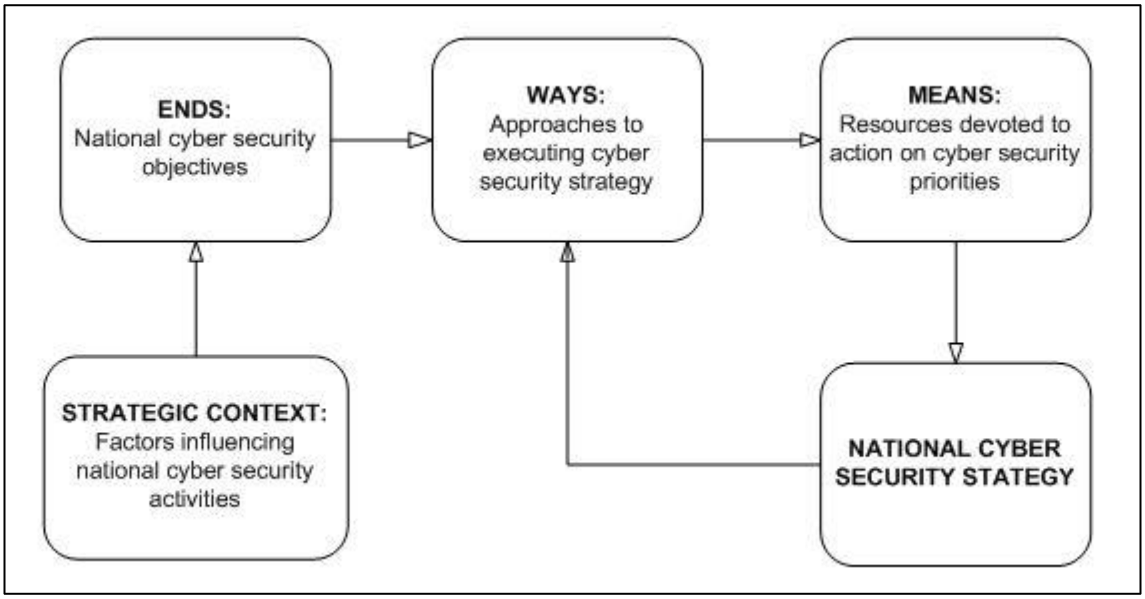

ENDS:
National cyber security objectives
WAYS:
Approaches to executing cyber security strategy
MEANS:
Resources devoted to action on cyber security priorities
STRATEGIC CONTEXT:
Factors influencing national cyber security activities
NATIONAL CYBER SECURITY STATEGY

Figure 3.1: National Cyber Security Strategy Model (adapted from Wamala [2011])

In the following paragraphs the National Cyber Security Model as proposed by ITU will be elaborated on (Wamala, 2011).

STRATEGIC CONTEXT:

The strategic context of the model deals with the classification of all the factors that influence national cyber security activities. As a guide the considerations should include:

- international treaties and conventions
- national interests
- threats and risks

One of the elements that is central to cyber security is collaboration between local, national and global entities. From a global perspective, there is a need for a treaty and a convention that will serve as a guide for global response. The ITU maintains that having a guide for global cooperation would contribute to the effectiveness of national cyber security. From a national perspective, values and principles that are core to the nation should also be identified as they shed light on specific national interests.

The general national interests as cited by the ITU include the defence of the homeland, economic wellbeing, a favourable world order and the promotion of values. These interests should be kept in mind when establishing a cyber security strategy, as failure to preserve these interests jeopardises national values. In addition, it is important to determine the impact of cyber threats and risks on these interests.

ENDS:

The ITU argues that cyber security should not be treated as an ‘end’ in itself, but rather as a means to an end. In the context of the model, ‘ends’ refers to the objectives that a cyber security strategy wishes to accomplish. Ends illustrate what a nation has to do in order to maintain national interests in cyberspace. Moreover, the ITU implies that a cyber security strategy should be of assistance in focusing efforts on ensuring that cyberspace keeps a country secure and thriving.

WAYS:

The ITU has chosen the five pillars declared in the Global Cyber Security Agenda as the priorities to be pursued by national cyber security strategies. These pillars are Legal

Measures, Technical and Procedural Measures, Organisational Structures, Capacity Building, and International Cooperation. Thus, according to this perspective, the ‘ways’ categorise strategic activities to assist countries in governing the pillars. The ways furthermore identify the manner in which a nation can distribute resources, and organise and manage the activities of all cyber security stakeholders.

Each of the pillars represents different priorities in establishing the national cyber security strategy. Firstly, with the Legal Measures pillar, the aim is to support the devising of policies that will govern the development of cybercrime legislation that is universally effective and which aligns with existing national and regional legislative processes. Secondly, the Technical and Procedural Measures pillar focuses on the establishment of processes that will address vulnerabilities in hardware and software. Thirdly, the Organisational Structures pillar focuses on developing appropriate organisational structures within the government to help in preventing, detecting and countering attacks against critical infrastructure. Fourthly, the Capacity Building pillar focuses on building the necessary skills and capabilities in cyber security as a whole; these may be managerial skills or even technical skills. Lastly, the International Cooperation pillar focuses on developing strategies to coordinate international efforts.

The ITU uses these pillars to facilitate the assigning of roles and responsibilities to relevant stakeholders in order to avoid overlapping and often conflicting obligations that tend to have adverse effects on many national cyber security programmes.

MEANS:

The ‘means’ flow directly from the five pillars that represent the ways and define the resources essential to achieve the stated ends.

Having used the model as a guide, a country can expect a cyber security strategy that befits the values and interests of the particular nation. Furthermore, the product of this will be a strategy with achievable objectives and with reasonable priorities within the strategic context of the specific nation. However, once the national cyber security strategy is completed, the 'ways' should be monitored continuously to ensure that the strategy meets the national cyber security requirements.

It can be concluded that securing cyberspace is a process; one that should be strategically led by the government. The ITU advocates the role of governments in heading cyber security; however, it also realises the responsibility of everyone who uses cyberspace. The ITU also suggests that the manner in which each nation implements cyber security may differ owing to the values and interests of the nation and other influencing factors. However, all users of cyberspace are vulnerable to online threats regardless of nationality. For this reason, no matter how different the influences may be from country to country, cyber security remains a priority for all who use cyberspace.

This section provided an overview of the top-down approach the ITU proposes for the practice of cyber security. The following section will discuss cyber security in SA. It will also discuss SA's National Cyber Security Policy Framework and analyse it against the ten elements identified by the ITU as being core to a strategy-led national cyber security programme.

3.4 South Africa's cyber security approach

SA is currently in the early stages of protecting its cyberspace and its activities in cyberspace. As discussed in chapter 1, the South African National Cyber Security Policy Framework was approved in 2012 (Department of State Security, 2012). However, although this policy framework has been approved, only a draft version is currently available. The draft policy framework sets out this nation's vision regarding cyber security. In summary, this vision eventually anticipates a cyber security culture among its citizens.

The previous section discussed cyber security as a course of action based on guidance provided by the ITU. The ITU defines ten elements which it deems to be significant to a "holistic, multi-stakeholder and strategy-led" cyber security approach. Based on these elements the ITU proposes a model that encapsulates a route that can be taken to produce a national cyber security strategy. In view of these elements as the focus of the proposed model, this section will analyse SA's draft National Cyber Security Policy Framework against the ten elements defined by the ITU as being core to a strategy-led national cyber security programme.

3.4.1 SA's National Cyber Security Policy Framework

Drafting a National Cyber Security Policy Framework is a promising start for SA. However, it remains just that, a promising start – a policy framework should be followed by implementation. Sadly, SA's draft policy framework is far from being implemented judging from the fact that although it has been approved, the final document has not yet been published. The list below gives a number of points that the 2011 draft policy framework wishes to address (*SA Government Gazette*, 2011) (see chapter 1):

- Developing and implementing an integrated approach to cyber security that will be government led.
- Promoting a cyber security culture that subscribes to minimum cyber security measures.
- Strengthening legal processes to prevent and address cybercrime, cyber terrorism and cyber warfare.
- Ensuring the safety of national critical information infrastructure.

- Establishing a partnership with public and private entities to coordinate action plans that correspond with the intents of this policy.
- Establishing a comprehensive legal framework to govern cyberspace.

From what the draft policy framework seeks to address, one can already see that some of the elements of the ITU national cyber security programme have been taken into consideration. The subsections below provide a clear mapping of the respective ITU national cyber security programme elements onto what is stated in SA's draft policy framework and in some cases what is stated in the relevant literature.

3.4.1.1 Element 1: Top government cyber security accountability

SA admits its responsibility towards its citizens in terms of ensuring a secure cyberspace (*SA Government Gazette*, 2010; *SA Government Gazette*, 2011). Thus, it has taken the initiative in establishing a draft cyber security policy framework. This draft policy framework elaborates on some of the elements of a national cyber security programme as proposed by the ITU.

3.4.1.2 Element 2: National cyber security coordinator

Section 5.2 of the draft policy framework recognises the need to have a dedicated coordinator for cyber security activities. It is stated in the policy that a Cyber Security Response Committee will be established to assume responsibility for coordinating cyber security activities (*SA Government Gazette*, 2011).

3.4.1.3 Element 3: National cyber security focal point

According to the draft policy framework at hand, a National Cyber Security Coordinating Centre (NCSC) will be established to serve as a focal point (*SA Government Gazette,* 2011).

3.4.1.4 Element 4: Legal measures

SA already has legislation in place that deals with the prosecution of some cyber-related crimes. These include the Electronic Communications and Transactions Act 25 of 2002, the Regulation of Interception of Communications and Provision of Communication-related Information Act 70 of 2002 (Wolf Pack, 2012).

3.4.1.5 Element 5: National Cyber Security Framework

The Draft South African National Cyber Security Policy Framework serves as an outline of the least number of security requirements as well the compulsory security requirements that should be in place.

3.4.1.6 Element 6: Computer Incident Response Team (CIRT)

The lack of an operational CIRT in SA has been identified as a point of concern. However, SA is well aware of this; as a result the policy proposes the development of national, government and sector computer security incident response teams (CSIRT) (*SA Government Gazette,* 2011). SA is already in the process of establishing one of the CSIRTs. This venture is headed by the Department of Communications and joint partners (Wolf Pack, 2012).

3.4.1.7 Element 7: Cyber security awareness and education

The point of developing a cyber security awareness and education programme is not well elaborated in the draft policy framework. It merely states that a national awareness and education programme should be implemented and promoted (*SA Government Gazette*, 2011). However, the ‘implementation and promotion’ of this cyber security programme cannot occur without its development.

3.4.1.8 Element 8: Public–private sector cyber security partnership

The draft policy framework also outlines the promotion and strengthening of local partnerships. According to section 10.1 of the draft policy, the National CSIRT will "foster cooperation and coordination between the public sector, private sector and civil society" (*SA Government Gazette,* 2011).

3.4.1.9 Element 9: Cyber security skills and training programme

SA has a shortage of the relevant professional skills (Wolf Pack, 2012). These include computer forensics, incident handlers and secure software coding skills (Wolf Pack, 2012). Consequently, the development of a skills and training programme would be of benefit for SA. Section 11 of the draft policy framework promotes the development of the necessary skills programme (*SA Government Gazette*, 2011).

3.4.1.10 Element 10: International cooperation

SA realises the borderless nature of cyber security. Thus section 10.3 of the draft policy framework outlines the measures SA will take to partner with the international community (*SA Government Gazette*, 2011). SA is already part of cyber security-related international initiatives; these include the Budapest Convention on Cyber Crime, the Forum for Incident Response and Security Teams (FIRST) and the United Nations Convention Against Corruption (UNCAC) (Wolf Pack, 2012).

From a policy point of view, SA's draft policy framework is to some degree in line with what the ITU regards as a "holistic, multi-stakeholder and strategy-led" cyber security approach. However there is still significant room for improvement, more specifically in implementing what the draft policy framework sets out. According to this policy framework, SA wishes to promote a culture of cyber security among its cyber-using citizens. However, the policy fails to provide comprehensive details on how this culture of security will be cultivated. Thus, the following section aims to discuss what constitutes such a culture of cyber security.

3.5 Cyber security culture

“Cyber security needs the development of a cyber-culture and acceptable user behaviour in the new reality of cyberspace, but it is also based on norms of correct behaviour and the capacity to pursue wrong-doers and bring them to justice, albeit in the online world” (ITU, 2008). The growing dependency on cyberspace and other digital resources has introduced its own set of security issues. Consequently, this dependence has added cyber security to the nation’s list of security concerns (Choo, 2011).

ITU defines the creation of a cyber security culture as the “best guarantee” for cyber security (International Telecommunications Union, 2008). Moreover, according to Ghernouti-Helie (2010), one of the pillars of such a culture is awareness and education. This pillar is discernible in the guidelines provided by the UN General Assembly Resolution 57/239 on the Creation of a Global Culture of Cyber Security, and the OECD’s Guidelines for the Security of Information Systems and Networks. These guidelines have a number of aims which depict what a cyber security culture should encompass. These aims are as follows (OECD, 2002):

- promoting a secure digital environment among all users of cyberspace
- raising awareness about the risks that are apparent online, as well as counter measures for these risks
- increasing the confidence of all users of information systems and networks, and the way in which they are provided and used
- serving as a general frame of reference for the development and implementation of cyber security measures

- promoting cooperation and information sharing, as appropriate, among all the participants in the development and implementation of security policies, practices, measures and procedures

- promoting the consideration of security as an important objective among all participants involved in the development or implementation of standards.

The aims defined above may be used as guidelines for fostering a cyber security culture (OECD, 2002). Such guidelines reflect the aforementioned aims. A number of guidelines are listed and explained below. They refer to all users of cyberspace as ‘participants’, including governments, businesses, other organisations and individual users:

- *Awareness.* Participants should be well informed about the necessity for cyber security and the steps they can take to promote it.
- *Responsibility*. All participants should assume responsibility for security information systems and networks. Hence, cyber security is a responsibility shared by all the participants.
- *Response*. There has to be a central point for information sharing for participants to facilitate appropriate and joint prevention, detection and response to security incidents.
- *Ethics*. Participants need to be respectful towards one another and also to act in a manner that is appropriate.
- *Democracy*. Security measures should be implemented in such a way that the rights of participants are not infringed.
- *Risk assessment*. All participants should conduct periodic risk assessments that identify threats and vulnerabilities. These assessments should be sufficiently broad-based to encompass key internal and external factors, such as technology, physical and human factors, policies and third-party services with security implications; should allow the determination of an acceptable level of risk; and

should assist in the selection of appropriate controls to manage the risk of potential harm to information systems and networks in the light of the nature and importance of the information to be protected.

- *Security design and implementation*. Participants should incorporate security as an essential element in the planning and design, operation and use of information systems and networks.
- *Security management*. Participants should adopt a comprehensive approach to security management based on risk assessment that is dynamic, encompassing all levels of participants' activities and all aspects of their operations.
- *Reassessment*. Participants should review and reassess the security of information systems and networks and should make appropriate modifications to security policies, practices, measures and procedures that include addressing new and changing threats and vulnerabilities.

From the aforementioned guidelines, it is important to note that 'awareness' is the first guideline, implying that in fostering a cyber security culture, one has to firstly realise that need for security; and secondly, one needs to be informed on how to apply the needed security. Thus, spreading awareness and educating the users of cyberspace is an important element of promoting the cyber security culture envisaged by SA.

In addition to these guidelines, the ITU has drawn up eight steps that should be taken in order to promote a cyber security culture. These steps are listed below (ITU, 2008):

1) Implement a cyber security plan for government-operated systems
2) Implement security awareness programmes and initiatives for users of systems and networks.
3) Encourage the development of a culture of security in firms.
4) Support outreach to civil society.
5) Promote a comprehensive national awareness programme.

6) Enhance science and technology (S&T) and research and development (R&D) activities.
7) Review the existing privacy regime and update it to the online environment.
8) Develop awareness of cyber threats and available solutions.

Considering the guidelines and the above-mentioned steps it becomes clear that education and awareness are elements that underpin cyber security as a whole. This is conveyed by step 5 which states that a comprehensive national awareness programme should be promoted. As such, “awareness-raising and the availability of resources are cross-cutting issues that need to be dealt with separately” (ITU, 2008). This calls for dedicated focus on awareness and education.

It is patent in the aforementioned guidelines and steps presented by the ITU that both awareness and education play a vital role in cyber security as a whole. They play an even more important role in the harnessing of a cyber security culture. Therefore, for SA to succeed in its attempts in promoting this culture, it should have a steady, well-defined approach to cyber security awareness and education. Most importantly, the government must take charge and lead this course of action. In addition, every user of cyberspace has a duty in this regard although this responsibility can only be appreciated when the users are well informed through effective awareness and education campaigns.

3.6 Conclusion

Cyberspace offers a variety of benefits that many have become accustomed to; however, it also has its dark side. It is therefore important that everyone take cognisance of not only the benefits but also the threats associated with cyberspace. Threats apparent in cyberspace affect individuals, organisations and nations alike. This dark side of cyberspace calls for proper cyber security measures.

All those who benefit from cyberspace have a role to play in cyber security. The ITU argues that cyber security should be led by the government. Moreover, the government has a responsibility to foster a culture of security in cyberspace. This culture consists of many pillars and one of those pillars in awareness and education. It is safe to say that awareness and education play an important role in cyber security. Therefore, if SA is to accomplish its objective of a cyber security culture it will need to work towards national cyber security awareness and education initiatives. As such, the following chapter will examine the cyber security awareness and education efforts in developed countries in order to identify key factors that will guide SA's approach to cyber security awareness and education.

CHAPTER 4: CYBER SECURITY EDUCATION

4.1 Introduction

“Education can prepare the general public to identify and avoid risks in cyberspace; education will ready the cyber security workforce of tomorrow; and education can keep today’s cyber security professionals at the leading edge of the latest technology and mitigation strategies” (NICE, 2012).

Awareness and education play a fundamental role in preparing all groupings of society for promoting cyber security. As argued in the previous chapter, education is fundamental in cultivating a culture of security among cyber users. South Africa (SA) is envisaging a cyber security culture; however, as the previous chapter illustrates, the draft SA National Cyber Security Policy Framework seems to lack emphasis on awareness and education as fundamental building blocks for a cyber-secure culture.

To explore the way in which other countries promote cyber security awareness and education, this chapter will provide a comparative analysis of a selection of four developed countries. This comparative analysis will focus on the national cyber security strategies of these countries, as well as on particular nationally initiated and driven cyber security awareness and education initiatives. From this analysis, the principle factors will be extrapolated in order to form the basis of a similar envisaged cyber security awareness and education framework for SA. Extrapolating these key principles is the primary objective of this chapter.

4.2 Cyber security education initiatives in developed countries

This section will provide a comparative analysis on the awareness and education components of the national cyber strategies and relevant documentation of four developed countries. It will, furthermore, analyse the national awareness and education initiatives of the each of the countries. The developed countries to be analysed are the United States (US), the United Kingdom (UK), Australia and Canada.

These countries have been chosen because they have national cyber security strategies, they have at least one national cyber security education and awareness initiative and they are members of the Organization for Economic Co-operation and Development (OECD). Being a member of the OECD is of relevance to the study because this organisation promotes the development of policies that improve a country's economic and social wellbeing (OECD, n.d.).

It is important to note that this section does not intend to examine all existing cyber security awareness and education initiatives in each country; it will merely scrutinise a selection of government-led national awareness and education initiatives. The analysis will be based on the following thematic questions:

- Why is cyber security awareness and education important to the country?
- What is the country's foremost aim regarding cyber security awareness and education?
- Who is assigned the duty of overseeing cyber security awareness and education related tasks?
- How is the country planning to work towards cyber security awareness and education?

An analysis of each country's national cyber security awareness and education initiatives will be provided as part of this inquiry mainly because these initiatives are in fact a major element of how each country is promoting cyber security awareness and education. The criteria to be used in the analysis are listed as follows:

  - *Host organisation* – the department or organisation that will be leading the initiative.
  - *Target audience* – the grouping of people that the initiative targets.
  - *Topics covered* – the topics that are covered by the content of the initiative.
  - *Campaign tools* – the methods that are used to deliver the message.
- When is the implementation of cyber security awareness and education initiatives expected to take place?

4.2.1 United States

In the US the need for cyber security awareness and education was realised in 2009 (The White House, 2009a). In this year a cyberspace policy review was issued, which recommended the expansion of national cyber security awareness and education. In this review it was acknowledged that securing cyberspace goes beyond implementing technical measures; that there is a further need for cyber security experts with the right set of skills, as well as a knowledgeable society with the ability to make secure choices while active online.

To address these needs, several initiatives where established, among them the National Initiative for Cyber security Education (NICE) (Paulsen, McDuffie, Newhouse, & Toth, 2012). NICE has been mandated to furnish all that is necessary for public awareness and education, and with the development of cyber security experts. NICE was also given the duty of managing cyber-related talent (NICE, 2012).

The US takes cognisance of its ever growing dependence on cyberspace. As such, it is preparing its workforce to have the necessary pool of individuals with cyber security expertise and, furthermore, equipping society at large with the knowledge and skills to be able to at the least manage their own security online (NICE, 2012).

4.2.1.1 Why?

US society and organisations and the nation at large are increasingly relying on cyberspace. Along with this reliance the US has become exposed to various cyber risks (The White House, 2003). These cyber risks threaten the security of national interests such as critical infrastructure and the economy. Consequently, there is a necessity for a cyber security workforce that is well equipped with the requisite knowledge, as well as cyber citizens who are well aware of the nature of cyberspace and the risks that come with a lifestyle that is highly interwoven into cyberspace (The White House, 2003). Thus, through education NICE envisages three main benefits. The first benefit is a general public with the ability to recognise and avoid online risks. Secondly, a cyber security workforce that is well equipped; and lastly, cyber security professionals who are armed with the most modern technology and mitigation strategies (NICE, 2012).

4.2.1.2 What?

NICE's mission is to complement the holistic cyber security stance of the US (NICE, 2012). To do so it has identified three goals in the NICE strategic plan. The first goal is raising the level of awareness of the nation about the risks in cyberspace. The second goal is preparing individuals for a US cyber security workforce. The last goal is promoting competitiveness within the current cyber security workforce in order to place it on a global scale. Each of these goals has a particular audience which it targets. Goal 1 focuses on individuals and organisations, goal 2 focuses on students and goal 3 focuses on the current cyber security workforce.

Each goal is mapped to a specific target audience because the level of interaction and the responsibility of each targeted audience correlate to the awareness and education requirements. However, even though each goal focuses on a specific target audience, there is an overlap in that some people interact with cyberspace on multiple levels and have inherently varying responsibilities (NICE, 2012).

To achieve the specified goals NICE comprises four elements as listed below (NICE, 2012):

- Component 1: National Cyber Security Awareness
- Component 2: Formal Cyber Security Education
- Component 3: Cyber Security Workforce Structure
- Component 4: Cyber Security Workforce Training and Professional Development

Component 1 covers the first goal, which is promoting national cyber security awareness and education. Component 2 is in line with goal two, which is focused on formal cyber security qualifications. In combination, component 3 and 4 work to achieve the third goal; which is focused on cultivating global scale competitiveness within the current cyber security workforce. All four of these components run collaboratively to achieve the mission of NICE (NICE, 2012).

4.2.1.3 Who?

As previously mentioned, NICE was established to meet the US's need to expand cyber security awareness and education. Therefore, NICE is responsible for coordinating all cyber security awareness and education related activities. Within NICE there are different roles according to the four components that NICE comprises. Each of these components has an overall leader and in some instances additional assistance is made available as listed below (NICE, 2012).

- *Component 1 – National Cyber Security Awareness*. The Department of Homeland Security (DHS) is the lead agency for this component. The DHS is working hand in hand with private, non-profit organisations and also with academia.

- *Component 2 – Formal Cyber Security Education*. This component is co-led by two agencies, the National Science Foundation (NSF) and the Department of Education (ED). These two agencies are working hand in hand with the Federal Government and academia.

- *Component 3 – Cyber Security Workforce Structure*. The DHS is also the lead agency for this component; it is working in collaboration with a number of federal departments and agencies and furthermore brings together Industry and academia.

- *Component 4 – Cyber Security Workforce Training and Professional Development*. This component is co-led by four parties: the DHS, the Department of Defense (DoD), and the Office of the Director of National Intelligence. These agencies work together with state, local, tribal and territorial (SLTT) governments, industry and academia.

Thus, it can be seen that the role of NICE also includes formal education, which largely focuses on formal qualifications and also workforce education. This study, however, will only focus on component 1, thus goal 1, which is raising the level of awareness in the nation about the risks of cyberspace.

4.2.1.4 How?

The NICE strategic plan has outlined a number of strategies to be implemented in order to ensure that each goal is accomplished. The table below presents goal 1, with the objectives that stem from this goal, together with the identified strategies to meet the objectives of goal one 1 (NICE, 2012).

Table 4.1: NICE Goal One (NICE, 2012)

Goal	Objective	Strategy
1.Raise national awareness about risks in cyberspace	1.1 Improve knowledge of risks and vulnerabilities in cyberspace	1. Promote cyber security awareness through campaigns such as *Stop.Think.Connect.*
		2. Promote strategies for training the public to manage cyber risk
	1.2 Promote the use of cyber security resources and tools	1. Partner with external stakeholders
		2. Encourage participation in cyber security-focused activities

To a large extent, there has been progress made towards this goal, because the *Stop.Think.Connect* campaign, which is identified as a strategy for improving the understanding of risks and vulnerabilities in cyberspace, is currently active. In addition, there are a number of secondary campaigns and programmes that stem from *Stop.Think.Connect* that are also in place.

Stop.Think.Connect:

The *Stop.Think.Connect* online awareness and education campaign underpins the notion that cyber security is the responsibility of everyone who benefits from using cyberspace (Department of Homeland Security, 2012a). Therefore, everyone should take a moment to **stop** and **think** carefully about the risks associated with using cyberspace. Once the risks are considered one can make an informed choice and continue to **connect** and enjoy cyberspace. *Stop.Think.Connect* has a number of other programmes and activities which will also be discussed briefly (Department of Homeland Security, 2012a).

- *Host organisation*: The DHS is leading this campaign.

- *Target audience*: All segments of American society are targeted. These include children younger than eight and children between the ages of nine and 12, as well as undergraduate students, parents and teachers, young professionals, older Americans, government, industry, small business, and law enforcement.

- *Topics covered*: When addressing children, the topics include cyber bullying, cyber predators, online netiquette, securing personal information, identity theft, and digital lives. For undergraduate students, the topics covered include social networking, information sharing, online identities, cyber predators, identity theft, fraud, and phishing. For parents and teachers, the topics covered include cyber ethics, cyber bullying, cyber predators, identity theft, protecting children online, scams, integrating cyber education, and cyber incident response. For young professionals, the topics include cyber incident response, device security, cyber security, online shopping and online banking. For older Americans, the topics include fraud, identity theft, scams, communicating online, safe online behaviour, and phishing. For governments the topics include a coalition programme, which will be discussed later, security policies, information security, compliance resources, cyber security assessment, and risk management. For industry the topics include information security, passwords, monitoring, awareness outreach, and defence strategies, information for small business includes topics like cyber-attacks, cyber breaches, information security, employee training, network security, back-ups and policy development. Finally, for law enforcement the topics include law enforcement responsibilities, the coalition programme, community outreach, and the US Secret Services Electronic Taskforce.

- *Tools*: Tip sheets, advice, posters, videos, programs, blogs, sub-campaigns, public service announcements, toolkits and social networks are used in this campaign.

National Cyber Security Awareness Month (NCSAM)

The National Cyber Security Awareness Month is an annual event held in October every year. At this time American citizens are made particularly aware and are reminded that cyber security is a shared responsibility (Department of Homeland Security, 2012a).

- *Host organisation*: This a joint effort of the DHS, National Cyber Security Alliance (NSCA) and the Multi-State Information Sharing and Analysis Center (MS-ISAC)
- *Target audience*: The general public and the public and private sectors are targeted.
- *Topics covered:* Topics covered include online safety, identity theft, and cyber security defence tools for businesses, cybercrime, cyber security and digital literacy. The topics are subject to change annually.
- *Tools*: The tools include the use of traditional media, posters and tips, and a series of events.

Cyber Awareness Coalition:

The Coalition serves as an interface that allows federal agencies and SLTT governments an opportunity to work directly with the Department of Homeland Security and the *Stop.Think.Connect* campaign in order to promote awareness on cyber threats and online safety measures that can be of benefit within their organisations and to the general public (Department of Homeland Security, 2012b).

- *Host organisation*: This programme is an initiative of the *Stop.Think.Connect* campaign.
- *Target audience*: US federal agencies and SLTT governments.

- Topics covered: Cyber security awareness and education, online threats and safety practices.

- *Tools*: There are no noted tools for this programme.

Cyber Tours:

This programme is an effort of the Department of Homeland Security through *Stop.Think.Connect*. It is intended to encourage communities to engage with one another to embrace a more proactive approach towards cyber security awareness and education. Through this programme communities are able to engage directly with American society about cyber security issues. This programme brings together American citizens from different sections of society to unite in the shared responsibility of cyber security by spreading awareness (Stop.Think.Connect, 2012).

- *Host organisation*: This programme is hosted by *Stop.Think.Connect*.

- *Target audience*: Target audience includes, but is not limited to, children, teens, college students, educators, parents, young professionals, and older Americans.

- *Topics*: Online safety, online threats.

- *Tools*: Tours with a series of events and forums.

Stop.Think.Connect.Friends

This programme gives everyone the opportunity to become a ‘Friend Campaigner’ to help in reaching a greater audience to spread cyber security awareness and education. *Stop.Think.Connect* prescribes the type of outreach activities that a Friend Campaigner can assist in. These activities include distributing the resources provided by *Stop.Think.Connect*, hosting cyber security awareness events, and promoting cyber security awareness among friends and family or colleagues. The Friend Campaign is an assistive campaign that aims to achieve the broader aims of *Stop.Think.Connect* (Department of Homeland Security, 2012c).

- *Host organisation*: This programme is hosted by *Stop.Think.Connect*.
- *Target audience*: The programme targets anyone who has an interest in assisting *Stop.Think.Connect* in its mission, including students, parents, school teacher's community leaders and people in industry.
- *Topic covered*: The topics to be covered are those that *Stop.Think.Connect* campaign covers.
- *Tools*: There are no particular tools prescribed for a Friend Campaign; however, what is of importance is the cyber security message that will be passed on, be it through a blog, event or publications.

4.2.1.5 When?

As discussed, NICE has already established cyber security awareness and educational campaigns for the purpose of goal 1. Although no particular timeframes are stated in the NICE strategic plan, to measure the progress in achieving its goals certain success indicators have been declared (NICE, 2012). NICE believes that the progress towards its goals, particularly goal 1, will be evident when both individuals and organisations understand online safety measures and are encouraged to act securely online.

4.2.2 United Kingdom

The UK Cyber Security Strategy was published in November 2011 (Cabinet Office, 2011). The strategy comprehensively outlines what the government intends to accomplish in securing cyberspace and how it plans to do so. The main vision of the strategy is for everyone to unite in combating cybercrime and creating a cyberspace that embraces economic and social growth. The strategy aims at a cyberspace that is more resilient to cyber-attacks, moreover a cyberspace that enhances the UK's economic and social prosperity (Cabinet Office, 2011). The strategy requires the assistance of both the individual and enterprises, because both benefit from cyberspace and therefore they should participate in making it a secure infrastructure. Alongside the strategy is a budget of £650 million to fuel UK cyber security initiatives. This funding will be allocated to the relevant departments and agencies to carry out their intended roles.

4.2.2.1 Why?

The UK cyber security strategy outlines four objectives for an envisaged vibrant, resilient and secure cyberspace where it can reap full economic and social benefits. The first objective is combating cybercrime and becoming one of the world's most secure places to do business in cyberspace. The second objective is a cyber-attack resilient nation that is capable of protecting its values in cyberspace. The third objective is promoting a cyberspace that is stable and used securely by society. The last objective is having the necessary understanding, skills and capabilities to strengthen the cyber security objectives (Cabinet Office, 2011).

For each of the objectives identified, a dedicated action plan has been defined, and cyber security awareness and education is one of the actions that will assist in achieving the fourth objective of the strategy (Cabinet Office, 2011). Thus, it can be concluded that UK cyber security awareness and education is not the end but the means to the end, as it is afforded to strengthen all the cyber security objectives that are stated in the cyber security strategy.

4.2.2.2 What?

The UK cyber security strategy identifies cyber security awareness and education as one of the key actions underpinning cyber security (Cabinet Office, 2011). As such, the UK has committed itself to empowering and supporting individuals and businesses with the information and skills necessary to protect themselves in cyberspace.

4.2.2.3 Who?

The UK has delegated *Get Safe Online* with this task. This organisation receives funding and support from government as well as the public and the private sectors. Moreover, the policy states that the Office of Cyber Security and Information Assurance should work in conjunction with the public and private sector and their international counterparts to assist in ensuring the safety of people and organisations from online risks and threats (Cabinet Office, 2011).

4.2.2.4 How?

A budget of £6,5 million has been allocated to educate UK citizens and businesses (Cabinet Office, 2011). The UK is bolstering the role of *Get Safe Online*, an already functional campaign, as the leading national internet security awareness initiative (Cabinet Office, 2011). The purpose of *Get Safe Online* is to assist organisations and the general population with cyber-related issues, as well as providing advice related to cyber threats and how to recognise and recover from the threats.

Get Safe Online:

Get Safe Online is the UK's national cyber security awareness and education campaign. It is an online campaign that is highly focused on providing individuals and businesses with resources that can assist them in managing their own security in cyberspace (Get Safe Online, 2012).

- *Host organisation*: *Get Safe Online* is leading this campaign.
- *Target audience*: Individuals and businesses are targeted.
- *Topics covered*: For individuals the topics covered include fraud, cyber stalking, online shopping, passwords, online gaming, social networking, identity theft, mobile device security, privacy, online dating, spam, online scams, viruses,

spyware, online money transfer, online banking, and safeguarding children. For businesses the topics covered include cloud computing, business fraud, data encryption, data loss prevention, information security, policy development and protecting company websites.

- *Tools*: The resources provided include videos, top tips, guides, blog, fact of the week, real-life stories and articles.

Get Safe Online Week:

Get Safe Online Week is an annual event intended to spread awareness of online safety across UK society. This initiative is a joint venture between government and industry (Get Safe Online, 2012).

- *Host organisation*: *Get Safe Online* is leading this campaign.
- *Target audience*: *Get Safe Online Week* targets the general public of the UK and small businesses.
- *Topics covered*: The topics covered range from online safety to cyber security.
- *Tools*: The tools include, but are not limited to, outreach events, social media and posters

4.2.2.5 When?

The UK has already started to provide the nation with a national cyber security awareness and education campaign and has set 2015 as the year that its cyber security objective will be met (Cabinet Office, 2011). By virtue of that, it is envisaged that by 2015 individuals and businesses will have sufficient knowledge and be capable of protecting themselves online.

4.2.3 Australia

The Australian cyber security strategy, which was released in 2009, outlines the intentions that the Australian government has to educate and empower its citizens with the required awareness and knowledge (Commonwealth of Australia, 2009). Cyber security awareness and education is the cornerstone of this strategy because it contributes immensely towards a society that will embrace online opportunities and, in turn, contribute to an economically prosperous Australia.

4.2.3.1 Why?

The foremost objective of Australia’s cyber security policy is promoting knowledgeable and aware users. This policy aims at providing Australians with a secure, resilient and trustworthy cyberspace in order to take full advantage of the digital economy. The digital economy has given Australia the opportunity to strengthen its economy and also maintain its global status (Commonwealth of Australia, 2009).

One of the key elements to the digital economy is a community that is digitally literate and empowered (Commonwealth of Australia, 2009). However, owing to the security implications of cyberspace, people are not empowered to participate in the concept of a digital economy. Thus, promoting secure behaviour among Australians through awareness and education has become vital to Australia.

4.2.3.2 What?

Australia’s cyber security policy outlines three objectives. One of these objectives is that “all Australians are aware of cyber risks, secure their computers and take all steps to protect their identities, privacy and finances online”. Australia seeks to foster a culture of security so that Australians may be confident in using online services and most importantly behave securely while making use of these services (Commonwealth of Australia, 2009).

Australia considers aware and educated users a benefit to its economy. This is because Australia believes that such users will embrace online services, particularly the digital economy, which will, in turn, enhance the Australian economy (Commonwealth of Australia, 2009).

4.2.3.3 Who?

There are two primary agencies within the Australian government that are tasked with the coordination of cyber security awareness and education efforts (House of Representatives, 2010). These agencies are the Department of Broadband, Communications and Digital Economy (DBDCE) and the Australian Competition and Consumer Commission (ACCC). Also involved is the Australian Communications and Media Authority (ACMA), which has the responsibility for implementing what the policy refers to as a "comprehensive range of education activities" (Commonwealth of Australia, 2009).

4.2.3.4 How?

The Australian cyber security policy has identified strategic priorities for achieving its objectives (Commonwealth of Australia, 2009). For the purpose of awareness and education, the strategic priority is to "educate and empower all Australians with the information, confidence and practical tools to protect themselves online" (Commonwealth of Australia, 2009). Australia has also made available a number of awareness and education campaigns and online information outlets, either through websites or publications such as the booklets listed below.

Stay Smart Online:

Stay Smart Online is an online campaign which provides access to information, resources and advice on how to secure personal computers and insights into how to be smart in cyberspace (Department of Broadband Communications and Digital Economy, n.d.).

- *Host organisation*: This campaign is an initiative of the DBCDE.
- *Target audience*: It is aimed at home users, children, teenagers, schools and small businesses.
- *Topics covered*: For home users the topics covered include mobile phone security, mobile phone parental controls, passwords, firewalls, file sharing, wireless network security, spam, online shopping, online banking, and identity and privacy. For schools it provides links to the “Budd:e” campaign which will be discussed subsequently. For businesses, the topics include security policies and spam, data backup, computer security, data theft, staff training and data theft. *Stay Smart Online* also provides schools with on cyber security education packages. For children and teens, social networking site security, online grooming, cyber bullying and mobile phone security are the topics included.
- *Tools*: These include a range of material in the form of top tips, quizzes, guides, CD-ROM and videos. This campaign also has a blog where Australians can share their insights and comments and ask questions.

Budd:e:

Budd:e consists of an e-security study module for primary and secondary school learners meant to assist teachers in teaching cyber security issues in a fun way using interactive games. It is available online or on CD-Rom. Learners can access Budd:e online games by creating an account and registering or playing a demo Budd:e. Once a learner has completed the game a certificate can be printed showing what topics have been covered (Australian Communications and Media Authority, 2010).

- *Host organisation*: This campaign is hosted by ACMA

- *Target audience*: Learners and teachers from primary and secondary schools.

- *Topics covered*: The teaching materials for primary schools include the following topics: malware, cybercrime, computer security, emails, spam, junk mail, scams, passwords, protecting personal information and online identity. For secondary schools information on cyber security fundamentals, malware, scams, truth, ownership, privacy, posting, sharing, and transacting is provided. The games for primary school learners include topics such as private and personal information, choosing a safe username, passwords, blocking, pop-ups, scams, spam, secure websites, backups, basic computer security such as virus scanning, firewalls, filtering and security updates. The games for secondary school learners do not differ much from the primary school topics although there are additional topics such as digital footprint, transacting and cyber bullying.

- *Tools*: Activity-based modules, curriculum maps, lesson plans, videos, live games.

Cybersmart:

Cybersmart is a national cyber security initiative developed to cater for the requirements of Australian society by providing information, resources and advice to promote secure behaviour online (Australian Communications and Media Authority, 2013).

- *Host organisation*: This is an initiative of the ACMA.

- *Target audience*: Young children aged four to seven, children aged eight to 12, teenagers aged 13 to 19, parents, teachers and library staff

- *Topics covered*: Topics for children include cyber bullying, computer security and securing personal information. For young children topics include cyber bullying, offensive contents, social networking, online netiquette, and digital footprints. Information for teens includes cyber bullying, online reputation, identity theft, illegal content, trolling, unwanted contact, online shopping, social networking and file sharing. Topics for parents and teachers include those covered for teens but have additional topics such as Internet addiction, e-security, sexting, online acronyms and online banking. For libraries topics include secure behaviour, risk management, cyber rules and online support

- *Tools*: Videos, games, quizzes, puzzles, guides, presentations, outreach programmes, workshops, DVDs, galleries, drawing boards, websites, lesson plans and policies. These tools are used in combinations applicable to a particular audience.

Scam Watch

SCAM Watch is a website that provides information on types of scams. It also provides information on how to identify, avoid and report these scams (Australian Competition and Consumer Commission, 2013).

- *Host organisation*: This is an initiative of the ACCC.
- *Target audience*: Small businesses and customers are targeted.
- *Topics covered*: Topics include types of scams, such as chain letter scams, identity theft scams, mobile phone scams, money transfer scams, online scams, investment scams, competition scams, and employment scams.
- *Tools*: The tools that are used include reporting systems, top tips, videos, victim stories, fact sheets, booklets, and reporting systems.

Cyber Security Awareness Week:

The Cyber Security Awareness Week is an annual event held by the Australian government in partnership with industry. It is aimed at helping Australians understand how to be safe online (Department of Broadband Communications and Digital Economy, n.d.).

- *Host organisation*: This initiative is led by the DBCDE.
- *Target audience*: All Australian citizens and industry are targeted.
- *Topics covered*: Cyber security
- *Tools*: A series of events is held, including seminars and webinars, using media, social media and other distribution channels.

Because the Australian government places such importance on cyber security awareness and education, the House of Representatives Standing Committee on Communications (the Committee) was requested to conduct an inquiry into the impact of cybercrime and related threats on society and the Australian economy. In addition, the inquiry was conducted to identify the level of adequacy of the measures that are already in place for combating cyber threats (House of Representatives, 2010).

In the report from the inquiry it was argued that there should be a shift in what drives most cyber security measures (House of Representatives, 2010). The committee was concerned that most of these measures were driven by an underlying intent to preserve national security and safeguard national critical infrastructure. Although focusing on these two points is important for every country, the impact of cybercrime to society at large is also a point that is worth instilling in the cyber security objectives of a nation. Thus, educating end-users in order to establish a cyber security culture should not be an add-on but rather one of the main objectives of national cyber security efforts (House of Representatives, 2010).

The Committee also argued that awareness and education alone do not produce the expected results of a culture of cyber security because knowledge of cyber security threats does not necessarily translate to secure behaviour (House of Representatives, 2010). However, the role that awareness and education plays is far too significant to ignore. As such, a number of recommendations were made to improve the position of Australia in terms of cyber security awareness and education.

In this inquiry it was concluded that although the cyber security strategy places much emphasis on cyber security awareness and education, there is no clear action plan or strategy guiding the efforts. Therefore, establishing a nationally coordinated education strategy was highly recommended. The strategy is intended to guide Australia in its endeavours to spread awareness and educate its citizens and moreover sets benchmarks for what Australia considers a successful national awareness and education programme (House of Representatives, 2010).

The inquiry also found that regardless of the fact that Australia has numerous cyber security information outlets, such as websites, publications and media releases, there is a need for a better integrated approach. Due to the fragmented approach to providing information, it is reported that users tend to be confused because of the inconsistencies that are apparent. As a result, the Committee recommended that the *Stay Smart Online* and *SCAM watch* websites should be linked to the national cyber crime reporting centre in order to have consistent, trustworthy and up-to-date cyber security information, with a single point of focus (House of Representatives, 2010).

Extending from the notion that knowledge alone is not enough to change behaviour; the Committee recommended that Australia should implement a “public health style” campaign using different media to spread key messages on cyber security issues and appropriate user conduct (House of Representatives, 2010). What is meant by a public health style campaign is a cyber security awareness and education campaign that learns from how the Australian public health campaigns are developed and delivered to the community.

Finally, the Committee recommends that an IT literacy training programme should be developed. It is said that this programme should be available to the entire community in order to promote computer literate citizens who not only know what to do, but that also have the necessary set of technical skills to implement personal security measures (House of Representatives, 2010).

4.2.3.5 When?

In 2008 a budget of $125,8 million was committed for a range of cyber security measures (Commonwealth of Australia, 2009). Such measures included education and outreach activities that are coordinated by the ACMA, the DBDCE, the ACCC and other agencies. Thus, seemingly, Australia has already started but still improving on what is already in place.

4.2.4 Canada

According to Canada's cyber security policy, the Canadian economy relies heavily on cyberspace (Government of Canada, 2010b). In 2007, an estimated $62,7 billion in revenue stemmed from online sales. Moreover, it was recorded that over 87% of businesses in Canada have embraced the opportunity to conduct commerce online (Government of Canada, 2010b).

The Canadian government has also moved quickly in adopting an electronic way of governing. Moreover, a hundred and thirty government services are offered online. These services include tax returns and student loan applications (Government of Canada, 2010b). Canadians are also increasingly using online services.

4.2.4.1 Why?

The Canadian cyber security policy outlines three main pillars in its efforts to secure cyberspace. The first pillar is securing government digital systems, the second is partnering with the private sector in securing the digital systems outside the Federal Government but which are vital to the government, and the third and last pillar is helping Canadians to being secure while active online (Government of Canada, 2010b).

Thus, due to such economic dependence on cyberspace, the Canadian government has committed to helping Canadians to be secure online.

4.2.4.2 What?

As stated, the Canadian cyber security strategy is built on three pillars, among which is helping Canadians to be secure online. With regard to this pillar, the ultimate goal is a cyber security culture. The method for moving towards the envisaged culture identified in the strategy is awareness and education (Government of Canada, 2010b).

4.2.4.3 Who?

The strategy does not reveal which department within the government will be handed the duty of ensuring that Canadians are equipped with the necessary awareness and education to ensure the creation of the envisaged culture. However, in the action plan for the cyber security policy, which was subsequently published, the Department of Public Safety in Canada was declared the lead department in the national cyber security awareness and education initiatives (Government of Canada, 2010a).

4.2.4.4 How?

According to the cyber security strategy, society will be reached through the use of websites, creative materials and outreach efforts (Government of Canada, 2010b). In addition, the action plan for the cyber security policy makes reference to a number of deliverables that have taken place or are still in progress towards awareness and education (Government of Canada, 2010a). These efforts include the development of a strategy that will govern the manner in which the message of cyber security is communicated to the Canadian public. According to the action plan, this communication strategy was completed in 2011, however its implementation is still underway (Government of Canada, 2010a).

In the same year, the Canadian government conducted baseline opinion research to assess the cyber security behaviour, opinions, attitudes and awareness levels of Canadians (Government of Canada, 2010a). In addition to these efforts, Canada has formed partnerships with various stakeholders in order to strengthen the delivery of cyber security awareness and education to the public.

Canada has in place some national initiatives in the form of a website and an outreach effort used to reach society and communicate cyber security issues. These campaigns are explained below.

Get Cyber Safe

Get Cyber Safe is a Canadian cyber security awareness and education campaign. This campaign is dedicated to preparing Canadian society for secure online behaviour (Public Safety Canada, 2013).

- *Host organisation*: Public Safety Canada is leading Get Cyber Safe.
- *Target audience*: This campaign targets general Canadian public.
- *Topics covered*: Email security, online shopping, file sharing, mobile security, fraud, scams, common threats, identity, online banking, computer security, network security, passwords, cloud-computing and others.

- *Tools*: Videos, websites, publications, web banners, blogs, tip sheets, and “did you know” questions are used as tools for this campaign.

Cyber Security Awareness Month:

This initiative is very similar to that of the US. The designated month in Canada is also October. This campaign is a joint effort between government and business across Canada and a number of international partners (Public Safety Canada, 2013).

- *Host organisation*: The campaign is being hosted by Public Safety Canada and industries across Canada.
- *Target audience*: Canadian Society is the main audience.
- *Topics covered*: The topics covered encompass cyber security.
- *Tools*: A series of events together with outreach activities.

Canada has also partnered with *Stop.Think.Connect*, the US initiative in order to promote the alignment of awareness and education initiatives across nations. This partnership was established in 2011 and is one of the efforts that will contribute in fostering a culture of security (Government of Canada, 2010a).

4.2.4.5 When?

The Action Plan for the cyber security policy spans five years from 2010 to 2015 (Government of Canada, 2010a). Thus Canada has progressed immensely in implementing its objective for cyber security awareness and education. Going forward, periodic reviews will be performed to measure any apparent progress that will come to pass.

It is evident that the US, the UK, Australia and Canada have taken definite steps towards promoting cyber security awareness and education within the respective nations. In all the cases presented above, it is clear that the government is committed to creating a culture of security within the country by means of awareness and education. The following section will provide a discussion on the comparative analysis with the aim of identifying key factors in any national cyber security awareness and education framework.

4.3 Findings from the comparative analysis

The previous section presented a comparative analysis of national cyber security strategies and national cyber security awareness and education initiatives in the US, the UK, Australia and Canada. Based on this analysis, this section will provide a discussion of the deductions and conclusions thereof. The layout of the discussion will conform to the thematic questions that were posed in the analysis, as listed below:

1) **Why** is cyber security awareness and education important to the country?

2) **What** is the country's foremost aim regarding cyber security awareness and education?

3) **Who** is assigned the duty of overseeing cyber security awareness and education related tasks?

4) **How** is the country planning to work towards cyber security awareness and education?

5) **When** is the implementation of cyber security awareness and education initiatives expected?

4.3.1 Why is cyber security awareness and education important to the country?

In the four developed countries investigated, it is evident that cyber security awareness and education efforts are the result of a national directive outlined in the respective national cyber security policies. From these policies, it can be seen that each country has a particular purpose behind cyber security awareness and education.

In the US, the primary purpose is deeply rooted in protecting national critical infrastructure. In the UK, on the other hand, the main reason behind cyber security awareness and education is to serve as a tool for accomplishing its high-level cyber security objectives (Cabinet Office, 2011). In Canada and Australia, the growing reliance on cyberspace has greatly influenced the economy of these countries, thus strengthening the respective economic stances, cyber security awareness and education included as high-level cyber security objectives in the national cyber security policies (Commonwealth of Australia, 2009; Government of Canada, 2010b).

It can therefore be concluded that the rationale behind pursuing cyber security awareness and education varies from country to country. Moreover, in all these cases the national cyber security awareness and education campaigns are a consequence of the respective policies. Thus, it can be argued that a country should consider cyber security awareness in its own context in order to understand how it will benefit from it.

Considering this purpose can have an influence on the types of campaign and programme to include as part of the national initiatives. In addition it can also influence the way each country perceives and prioritises cyber security awareness and education. It is true, however, that for all the countries awareness and education are core to the holistic cyber security effort, regardless of the level on which a country has placed it.

4.3.2 What is the country’s foremost aim regarding cyber security awareness and education?

In the US the goal of cyber security awareness and education is to raise the level of awareness in the nation about the risks of cyberspace (NICE, 2012). In the UK, the goal is to support individuals and businesses by informing and educating them about cyber security (Cabinet Office, 2011). Finally, in Australia and Canada, the ultimate goal is a cyber security culture that will be fostered through awareness and education (Commonwealth of Australia, 2009; Government of Canada, 2010b).

From the four developed countries one can see that the purpose of promoting cyber security awareness and education is accompanied by certain goals that have been set. As such, setting definite goals can be regarded as vital as it sheds light on what the country wants to achieve and also sets some targets by means of which progress can be measured.

4.3.3 Who is assigned the duty of overseeing cyber security awareness and education related tasks?

In the US a new organisation, NICE, has been formed which is entirely dedicated to cyber security awareness and education (NICE, 2012). NICE is made up of a combination of government departments. Some of these departments assume the role of leading certain directories that exist within NICE. In the case of the UK, cyber security awareness and education has been delegated to an external organisation, *Get Safe Online*.

Similar to the US, in Australia multiple departments form the focal point of cyber security awareness and education (House of Representatives, 2010). However, in Australia, as noted by the Committee, there is no partnership between the departments and this causes a lot of confusion for the target audience about which source to trust (House of Representatives, 2010). Finally, in Canada, Public Safety Canada takes the lead in cyber security awareness and education.

In all these countries it is evident that the documented cyber security awareness and education goal is assigned to one or more departments or organisations to carry out. This allocation of responsibilities promotes accountability and furthermore establishes a focal point. Thus, there should be a dedicated administration that will serve a focal point for cyber security awareness and education implementation.

4.3.4 How is the country planning to work towards cyber security awareness and education?

Following the publication of the national cyber security policies, the US and Canada published action plans outlining their approach to cyber security awareness and education (Government of Canada, 2010a; NICE, 2012). The US NICE Strategic Plan indicates that campaigns such as *Stop.Think.Connect* would be used to equip the American public with the necessary knowledge and skills. As indicated, *Stop.Think.Connect* is well-designed and through it more campaigns and programmes are made available.

Canada's action plan presented the actions that were to be taken to accomplish each of the objectives that are defined in the national cyber security policy. In addition, it stated the timelines and the status of every deliverable together with the lead department (Government of Canada, 2010a). This action plan clearly encapsulated the actions to be taken, timelines, and the current status of progress and the lead department.

In contrast to the US and Canada, the UK and Australia have not published any action plans in addition to their national cyber security strategies. However, in Australia in the enquiry that was performed as mentioned in subsection 4.2.3, the Committee recommended that an action plan be drafted. Therefore it may be concluded that there should be a strategy in place that clearly articulates how a country will approach cyber security awareness and education.

Having examined some of the national cyber security awareness and education initiatives of the relevant countries, a number of deductions can be made. Firstly, the focus of the cyber security awareness and education campaigns and programmes is on every grouping of society. These groupings include parents, children, teachers and businesses. This focus is essential, as it was concluded in chapter 3 that individuals, organisations and nations are equally exposed to the risks of cyberspace, thus all the levels require both awareness raising and education.

Secondly, each target audience is presented with topics that are relevant to it, which suggests that research has been done to identify their individual needs. This relationship between the target audiences and topics can be seen in the cases of the business environment and children. For example, knowledge about cyber bullying is directed primarily at individuals and not the business environment; similarly knowledge about cyber security policy making is directed at organisations and not really at children. Therefore, it is important for cyber security awareness and education campaigns and programmes to present each target audience with topics that are relevant to them.

Thirdly, there is a difference in the medium of communication used to deliver the awareness-raising and education information to a particular audience. Using the same example of organisations and children, it can be seen that from the analysis that children are often presented with cyber security awareness and education through games, whereas organisations are offered guides and toolkits. Thus, the medium of communication used to deliver cyber security awareness and education should be well suited to a particular target audience.

Fourthly, it is evident that the environment in which the awareness raising and education takes place, may differ for each target audience. Again using the same example of children and organisations, children can be reached in schools and homes whereas organisations can be reached in the workplace. Therefore, the environment should be taken into consideration when developing cyber security awareness and education campaigns and programmes because it may influence the approach and/or tools to be used by the campaign or programme.

Finally, within the analysed cyber security awareness and education initiatives there are role-players. It is clear that cyber security awareness is a shared responsibility and everyone enjoying the cyberspace has a role to play. This is evident in that in all the countries examined, the governments have taken for to leading and resourcing cyber security awareness and education. In addition, industry has also assumed some of the responsibility and has partnered with government. As such, when planning cyber security awareness and education campaigns and programmes the role-players should be identified and their respective responsibilities should be defined. Moreover, partnerships with relevant stakeholders should be in place.

4.3.5 When is the implementation of cyber security awareness and education initiatives expected?

All four countries have implemented a suite of cyber security awareness and education measures. As far as the UK and Canada are concerned, 2015 is the year in which all cyber security objectives should be accomplished; this includes awareness and education. It is indeed promising that both of these countries aim to have fostered a culture of cyber security among their citizens by 2015, as both countries have already taken definite steps to promote awareness and education. In addition, Canada is committed to generating periodic status reports in order to monitor its progress closely.

In the US, the NICE strategic plan makes no mention of a particular time frame in which its cyber security awareness and education objectives will be accomplished. However, it has defined a number of success indicators. Having both individuals and organisations understand online safety measures and being encouraged to act securely online will serve as an indication that NICE has accomplished its aim. This approach suggests that in the US, cyber security awareness and education is an ongoing process that will continue until the established indicators materialise.

It is evident that these countries have in some way defined benchmarks that will assist them in evaluating the progress they have made towards accomplishing their goals. It can therefore be concluded that there should be some sort of monitoring and evaluation of the progress made in these cyber security awareness and education efforts.

Cyber security awareness and education is indeed a cross-cutting matter that warrants diligent handling. The government should take the lead in this regard and, accordingly, establish national and international partnerships and encourage all users of cyberspace to play their part.

This section provided a discussion of the analysis in terms of the deductions and conclusions that were made based on the questions posed at the beginning of this chapter. The discussion contained in this section arrived at a number of key factors related to cyber security awareness and education. These will be presented in the following section.

4.4 Key factors in cyber security awareness

The need for cyber security awareness and education was established in chapter 3. This chapter has provided a comparative analysis of the cyber security awareness and education efforts that have been made by the US, the UK, Australia and Canada. From this analysis key factors have been extrapolated for the purpose of forming the basis of the proposed awareness and education framework for South Africa, which is the main objective of this study. The key factors are listed below:

- Clearly articulated **goals** should be defined.
- A **dedicated team** should be appointed.
- An **action plan** should be outlined.
- A **national cyber security awareness and education campaign** should be defined.

- **Partnerships** should be established.
- **Resources** should be in place.
- **Monitoring techniques** should be defined.

These key factors stem from the conclusions and deductions arrived at in terms of the analysis. Moreover, these have been argued and reviewed in a peer-reviewed paper which was published and presented at the AFRICOMM 2012 conference (Appendix A2). As mentioned, these factors will form the basis of a framework to be developed and will be further elaborated on in the following chapter. A number of concluding remarks follow.

4.5 Conclusion

Cyber security awareness and education is core to the holistic cyber security effort. Further, it is clear that, in line with the draft SA Cyber Security Policy Framework, security awareness and education should play an integral part in cultivating a cyber-secure culture in South Africa. As may be deduced from the above, it should be a priority for governments to provide resources that can afford all groupings in society the necessary awareness and education to equip them to act securely online. This can be achieved by means of cyber security awareness and education campaigns and programmes.

To examine the approach taken by developed countries this chapter focused on the awareness and education components of the national cyber security policies of the US, the UK, Australia and Canada. It presented a comparative analysis of the policies and of the cyber security awareness and education initiatives of these countries. Based on this analysis, this chapter went on to draw a number of conclusions and deductions from which a set of key factors was identified on which the proposed framework will be established. The basis on which the proposed cyber security awareness and education framework will be developed has now been established. Thus, the following chapter will make use of the key factors identified to draft a framework which is intended to assist SA in raising awareness of and educating its citizens on cyber security and thus fostering a cyber-secure culture.

CHAPTER 5: FRAMEWORK FOR CYBER SECURITY AWARENESS AND EDUCATION IN SOUTH AFRICA

5.1 Introduction

“South Africa has a huge responsibility to promote cyber security awareness” (Grobler, Van Vuuren, & Leenen, 2012).

In considering this responsibility, the ultimate aim of this chapter is to propose a cyber security framework that will assist SA in promoting cyber security awareness and education. Having studied the United States (US), the United Kingdom (UK), Australia and Canada in the previous chapter, this chapter will attempt to graphically outline the way in which these countries have addressed cyber security awareness and education. The outlines will then be compared to one another in order to learn more from these countries. Subsequent to the comparison, the proposed cyber security awareness and education framework will be developed according to the outline that is deemed most suitable.

It should, however, be noted that this by no means counters the notion that the framework will be developed on the basis of the key factors defined in chapter 4. However, in addition to the key factors, the manner in which the proposed framework will be developed will conform to the approach that will be obtained from this chapter.

Therefore, the objective of this chapter is to develop a cyber security awareness and education framework for South Africa. This framework will be developed by adopting a suitable outline and on the basis of the following key factors, as established in the previous chapter:

- Cleary articulated **goals** should be defined.
- A **dedicated team** should be appointed.
- An **action plan** should be outlined.
- A **national cyber security awareness and education campaign** should be defined.
- **Partnerships** should be established.
- **Resources** should be in place.
- **Monitoring techniques** should be defined.

The following sections present graphical representations of the cyber security awareness and education efforts of the US, the UK, Australia and Canada. Thereafter, the proposed framework will be presented.

5.2 Towards a cyber security awareness and education framework

Chapter 4 (section 4.2) provided an analysis of the cyber security initiatives of the US, the UK, Australia and Canada. As such, this section will attempt to graphically present a summary of the analysis in order to learn from the approaches taken by these countries in affording cyber security awareness and education. It is worth noting that the figures presented in this section are the authors' concepts.

5.2.1 The United States (US) blueprint

All the developed countries studied have an ultimate vision regarding cyber security awareness and education. Giving rise to such a vision is the respective national cyber security policy and/or other relevant documentation. In the case of the US, as mentioned in chapter 4 (subsection 4.2.1), the cyberspace policy review recommended the expansion of national cyber security awareness and education.

It was further revealed in chapter 4 (subsection 4.2.2) that the National Initiative for Cyber Security Education (NICE) was commissioned to coordinate all that is necessary in carrying out the vision of expanding the national cyber security awareness and education goal. As such, by means of a comprehensive strategic plan, NICE outlines the way in which it will deliver awareness and education to the people of the US. Below is a diagram that captures the essence of the US's approach to cyber security awareness and education.

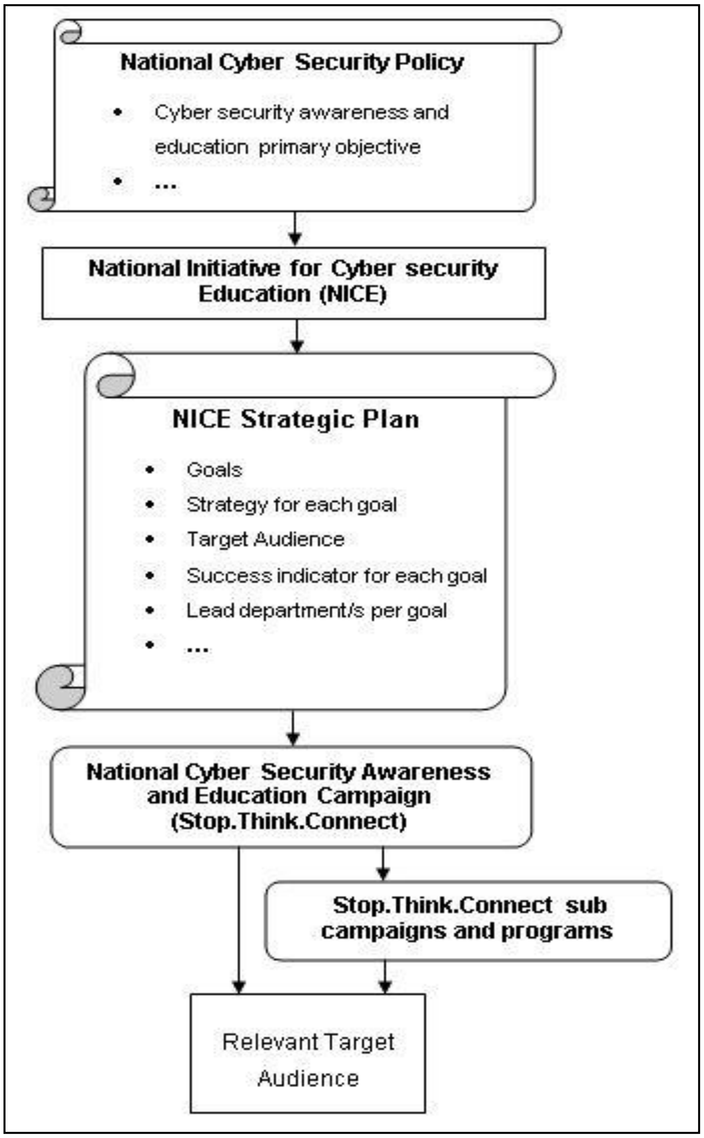

National Cyber Security Policy
• Cyber security awareness and education primary objective
• ...
National Initiative for Cyber security Education (NICE)
NICE Strategic Plan
• Goals
• Strategy for each goal
• Target Audience
• Success indicator for each goal
• Lead department/s per goal
• ...
National Cyber Security Awareness and Education Campaign (Stop.Think.Connect)
Stop.Think.Connect sub campaigns and programs
Relevant Target Audience

Figure 5.1: The US cyber security awareness and education approach

Figure 5.1 clearly communicates the linear flow of measures from the cyber security awareness and education aim defined in policy, to how this aim materialises, to a campaign that is offered to a particular audience. As stated in chapter 4 (section 4.2.1), NICE uses *Stop.Think.Connect* as a strategy for spreading awareness and knowledge of cyber security. Accordingly, *Stop.Think.Connect* and its subsidiary campaigns and programmes are fashioned in a manner that is suited to their audience.

5.2.2 The United Kingdom (UK) blueprint

In chapter 4 (subsection 4.2.2), it is concluded that the UK national cyber security policy identifies awareness and education as means for strengthening the holistic cyber security objectives of the country. Figure 5.2 below illustrates the approach taken by the UK in affording the nation cyber security awareness and education.

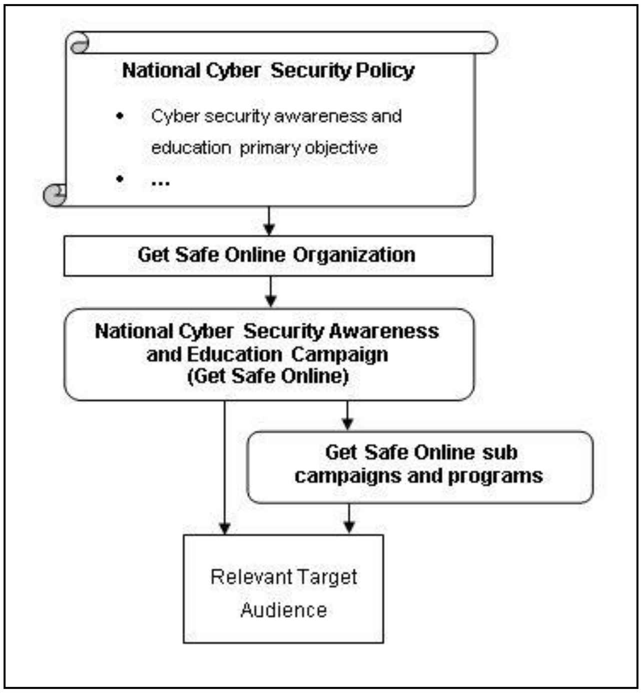
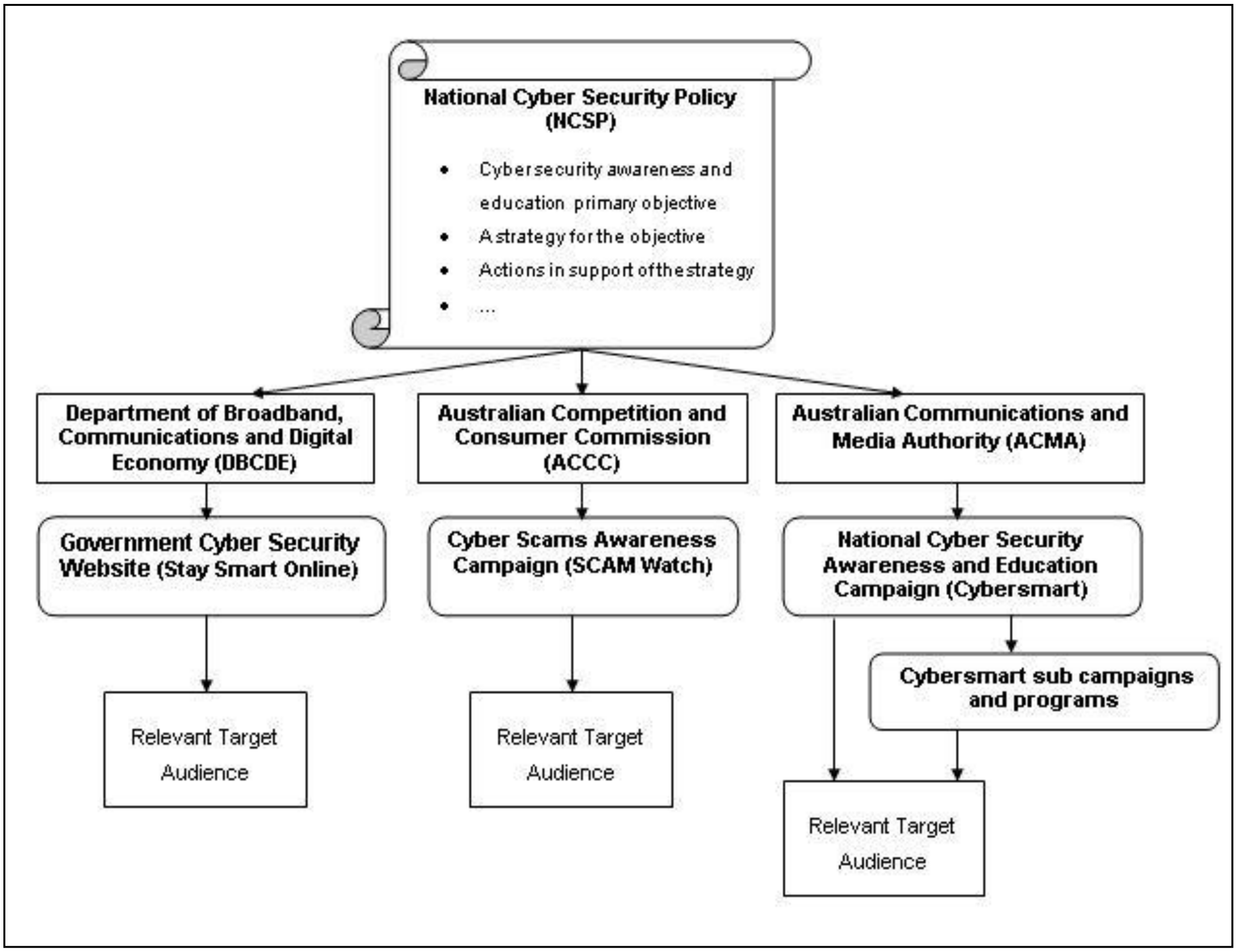

National Cyber Security Policy
• Cyber security awareness and education primary objective
• ...
Get Safe Online Organization
National Cyber Security Awareness and Education Campaign (Get Safe Online)
Get Safe Online sub campaigns and programs
Relevant Target Audience

Figure 5.2: The UK cyber security awareness and education approach

As mentioned in section 4.2.2, the UK states in its cyber security policy that it will bolster the role of *Get Safe Online*. Hence, as illustrated by in figure 5.2, the *Get Safe Online* organisation assumes responsibility for steering the national cyber security awareness and education campaign in the UK. Figure 5.2 also exemplifies that it is *Get Safe Online,* together with its subsidiary programmes, which delivers awareness and education to the relevant target audience.

5.2.3 The Australian blueprint

According to chapter 4 (section 4.2.3) Australia regards cyber security awareness and education as one of the foremost objectives in its national cyber security policy. As a result, there are three departments that share responsibility for this. Figure 5.3 below gives a snapshot of the Australian approach.



National Cyber Security Policy (NCSP)
Cyber security awareness and education primary objective
A strategy for the objective
Actions in support of the strategy
...
Department of Broadband, Communications and Digital Economy (DBCDE)
Australian Competition and Consumer Commission (ACCC)
Australian Communications and Media Authority (ACMA)
Government Cyber Security Website (Stay Smart Online)
Cyber Scams Awareness Campaign (SCAM Watch)
National Cyber Security Awareness and Education Campaign (Cybersmart)
Cybersmart sub campaigns and programs
Relevant Target Audience
Relevant Target Audience
Relevant Target Audience

Figure 5.3: The Australian cyber security awareness and education approach

As illustrated in figure 5.3, the policy makes reference to three government agencies that will be associated with cyber security awareness and education. As mentioned in chapter 4 (subsection 4.3.3), these agencies are the Department of Broadband, Communications and Digital Economy (DBCDE), the Australian Competition and Consumer Commission (ACCC) and the Australian Communications and Media Authority (ACMA). All these agencies have coordinated some form of cyber security awareness and education initiative. However, only one department, the ACMA, assumes the role of coordinating the national awareness and education campaign, *Cybersmart*. Likewise, *Cybersmart* works together with its subsidiary campaigns and programmes to offer cyber security awareness and education to the relevant target audiences. Similarly, *Stay Smart Online* by the DBCDE and *SCAM Watch* by the ACCC offer cyber security awareness and education to the relevant target audiences.

5.2.4 The Canadian blueprint

Similar to Australia, Canada regards cyber security awareness and education as a core pillar of its national cyber security policy. Figure 5.4 attempts to capture the approach taken by Canada in cyber security awareness and education.

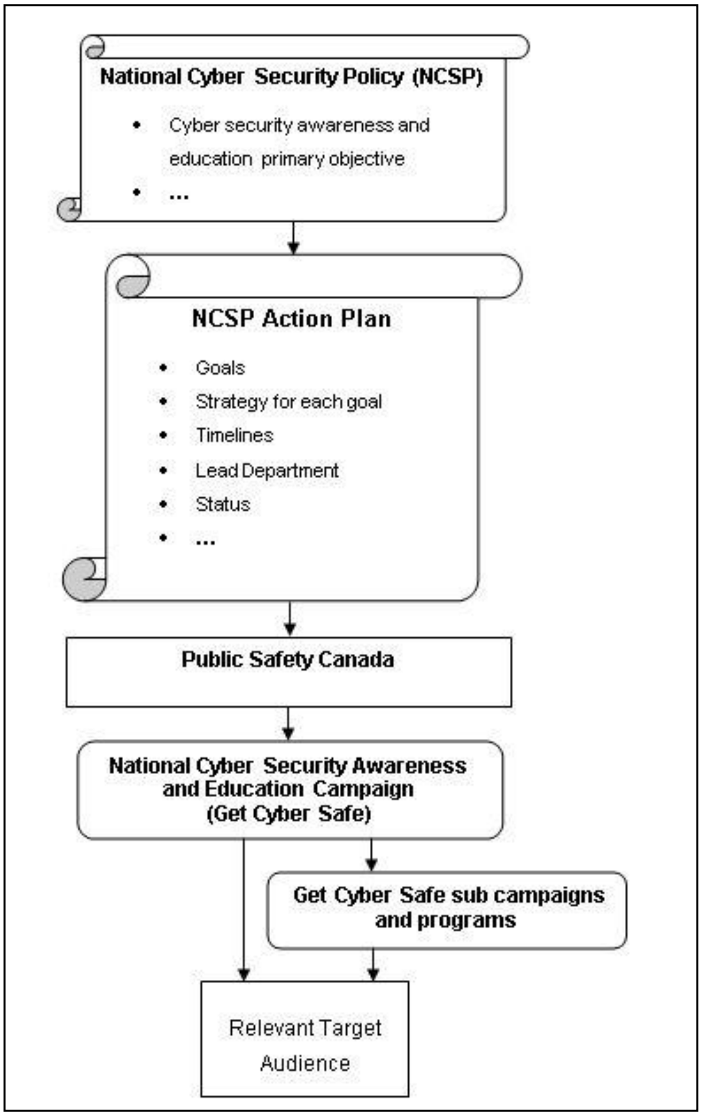

National Cyber Security Policy (NCSP)
Cyber security awareness and education primary objective
...
NCSP Action Plan
Goals
Strategy for each goal
Timelines
Lead Department
Status
...
Public Safety Canada
National Cyber Security Awareness and Education Campaign (Get Cyber Safe)
Get Cyber Safe sub campaigns and programs
Relevant Target Audience

Figure 5.4: The Canadian cyber security awareness and education approach

As mentioned in chapter 4 (subsection 4.2.4), figure 5.4 shows that, following the publication of the Canadian cyber security policy, an action plan was published announcing Public Safety Canada as the lead department in cyber security awareness and education. Likewise, stemming from the lead department is a national cyber security campaign which offers subordinate campaigns and programmes to the designated recipients.

From the outlines presented in this chapter, there is an apparent order of proceedings starting with the national cyber security policy through to awareness raising and education being delivered to a target audience. It can be seen that the Canadian approach largely mirrors that of the US, although there are variations in what proceeds from the cyber security policy.

Both Canada and the US have either a strategic plan or an action plan that details the manner in which cyber security awareness and education will be carried out. However, it may be noted that in the US this strategic plan is exclusively dedicated to cyber security awareness and education, while the Canadian action plan is inclusive of every aspect outlined in its cyber security policy. By virtue of that, the US is more comprehensive and specific than Canada and that makes the US approach preferable to that of Canada.

The UK's approach, on the other hand, is more industry oriented in that cyber security awareness and education are outsourced by *Get Safe Online*. Although the UK government is funding and supporting this organisation, it can be argued that it is not entirely a government initiative. With regard to the Australian outline, as discussed in subsection 4.2.3, there is an apparent fragmentation within the appointed departments. Furthermore, there is no focal point and collaboration within these departments. Moreover, Australia criticises itself for not having a strategic plan that is solely focused on awareness and education.

As a result of the issues raised in these approaches it can be deduced that the US approach seemingly has merit in comparison with its counterparts. In view of its similarities with Canada, however, and because of its comprehensiveness and exclusivity in terms of cyber security awareness and education, it is argued that this is the most preferable. Therefore, the proposed framework will be developed by adopting the US outline for the following reasons:

- The UK approach is less detailed and is vastly industry oriented.
- The Australian approach is fragmented and criticises itself.
- The Canadian approach, though similar to that of the US, is not as comprehensive and thorough.

The following section will discuss the cyber security awareness and education framework that has been proposed for SA.

5.3 SA’s cyber security awareness and education framework

The previous section provided a brief summary of the cyber security approaches of the US, the UK, Australia and Canada. It concluded by stating the approach according to which the proposed cyber security awareness and education would be developed and gave the reasons for this decision. Moving forward, this section will discuss the elements of the proposed cyber security awareness and education framework individually. However, prior to discussing the proposed framework, it is essential to define the type framework it is.

There are two known types of frameworks, namely, a theoretical and a conceptual framework. A theoretical framework is defined as a set of theories put together to provide a basis or support for explaining, viewing or contemplating a phenomenon (Labaree, 2013). Miles and Huberman (1994) define a conceptual framework as “a written or visual presentation that explains either graphically, or in narrative form, the main things to be studied – the key factors, concepts or variables – and the presumed relationship among them”.

Camp (2001) further explains the difference between a theoretical and a conceptual framework by stating that while theoretical frameworks elaborate on the concepts relating to the phenomenon, a conceptual framework is a structure that best portrays the concepts borrowed from a particular phenomenon. The proposed framework is, therefore, a conceptual framework.

Jabareen (2009) suggests that a conceptual framework can be developed and constructed by means of qualitative analysis methods. Accordingly, a comparative analysis was performed in chapter 4 in order to accumulate the concepts to be included in the proposed framework. The proposed framework is divided into five layers and one overarching component as listed below:

- *The strategic layer* – this layer reflects the overall vision of the government concerning cyber security awareness and education.
- *The tactical layer* – this layer suggests the schemes that SA should employ to realise its cyber security awareness and education goals.
- *The preparation layer* – this layer prepares the contents of the scheme identified in the tactical layer.
- *The delivery layer* – this layer defines the recipients of the preparations made in the preparation layer, namely, the target audience.
- *The monitoring layer* – this layer examines the progress made by the scheme towards fulfilling the government's vision.
- *Resources* – this component defines the resources which should form the inputs to all the aforementioned layers.

The abovementioned layers respectively illustrate the six themes embodied in the cyber security awareness and education framework. Firstly, the cyber security awareness and education vision of the government; secondly the proposed strategies to be used to fulfil the vision; thirdly, the preparations that have to be made in order to realise this vision, fourthly, the heirs to the vision; fifthly, the monitoring of the progress towards the vision;

and finally, the necessary resourcing. These layers will be discussed in detail in the subsequent subsections.

5.3.1 The strategic layer

Chapter 2 (section 2.4) discussed the fact that cyberspace has afforded people a vast array of services that many people have grown dependant on. These services include, but are not limited to, communication services, social networks, entertainment, digital libraries, and e-commerce. Owing to these services, cyberspace has brought about positive change not only for individuals, but also for organisations and nations in general.

By contrast, chapter 3 argued that while cyberspace offers numerous services, it also has a dark side; a dark side that has introduced risks which many users are often unaware of. As a result, the reliance on cyberspace necessitates cyber security. Chapter 3 (section 3.2) highlighted the role played by government in ensuring the safety and security of the nation and its citizens in cyberspace. Thus, as a course of action, the South African government should have a national cyber security policy in place that will articulate the government's approach to safety and security in cyberspace. Accordingly, from a government point of view, a national cyber security policy is important.

As mentioned, the strategic layer reflects the overall vision (the dream) of the government concerning cyber security awareness and education. Chapter 3 (section 3.4) made it known that SA's overall vision is a cyber security culture. In this layer, this vision is delineated into three components as presented below in figure 5.5.

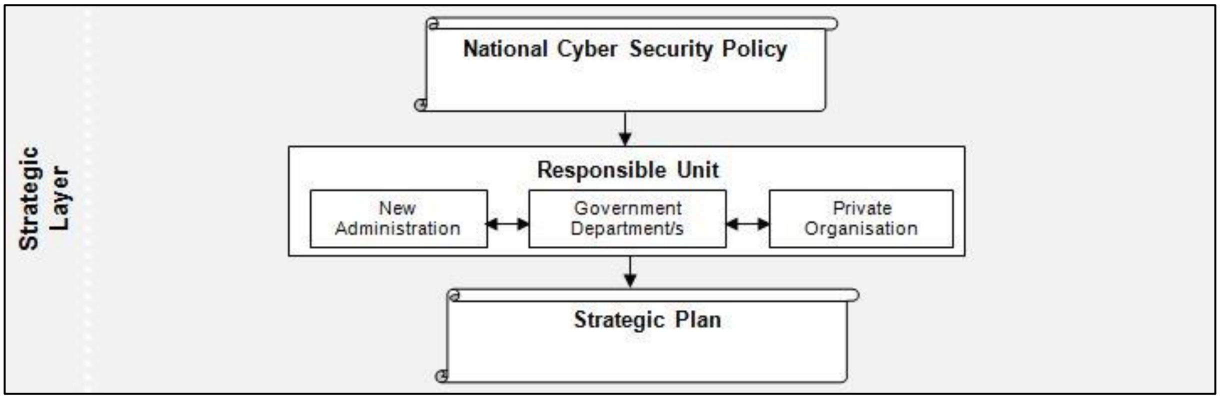


Figure 5.5: The strategic layer of the cyber security awareness and education framework

As was gathered from the cyber security awareness and education approaches summarised in section 5.2, national cyber security policies are indeed important because the objectives of the country for cyber security awareness and education are detailed in such policy. Thus, this policy is the initial component of the framework.

This layer inherits three of the cyber security awareness and education key factors as listed below:

- Cleary articulated **goals** should be defined.
- A dedicated **team** should be appointed.
- An **action plan** should be outlined.

The first component in figure 5.5 is the national cyber security policy detailing the primary objective of cyber security awareness and education. The second component is a responsible unit, as the findings in chapter 4 (section 4.3) indicated that there should be a dedicated administration for cyber security awareness and education. Thus the responsible unit component proposes three ways in which this administration can be formed. These ways are listed below:

- Forming a new administration.

- Using one or multiple government departments.
- Delegating a private organisation.

In chapter 4 (subsection 4.3.4), it was concluded that there should be a strategic plan that clearly articulates how a country will approach cyber security awareness and education; hence the last component, which is the strategic plan. The framework recommends that once an administration is appointed, a comprehensive strategic plan should be drafted.

It is beyond the scope of this study to elaborate on every aspect that the strategic plan should consist of. However, taking into consideration the US approach, this strategic plan should make known the methods that the country could employ to realise its cyber security goals. Such methods will fall into the next layer which will be discussed in the following subsection.

5.3.2 The tactical layer

The tactical layer lies below the strategic layer. As stated, this layer takes up where the strategic plan defined in the strategic layer left off. In this layer, the suggested elements to drive cyber security awareness and education are stated. Figure 5.6 below presents the tactical layer.

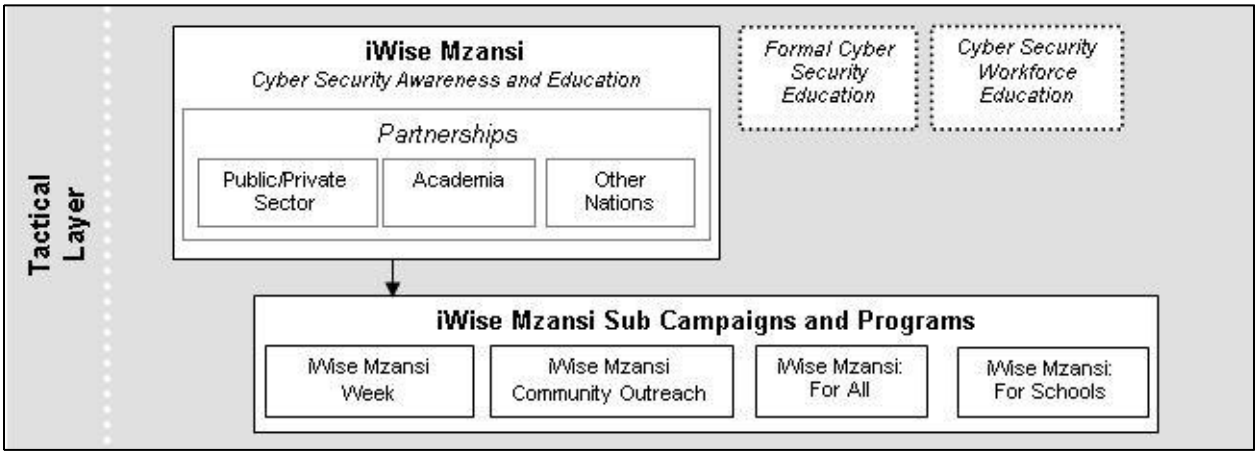

Tactical Layer
iWise Mzansi
Cyber Security Awareness and Education
Partnerships
Public/Private Sector
Academia
Other Nations
Formal Cyber Security Education
Cyber Security Workforce Education
iWise Mzansi Sub Campaigns and Programs
iWise Mzansi Week
iWise Mzansi Community Outreach
iWise Mzansi: For All
iWise Mzansi: For Schools

Figure 5.6: The tactical layer of the cyber security awareness and education framework

This layer integrates two of the cyber security awareness and education key factors, as listed below.

- A **national cyber security awareness and education campaign** should be defined.
- **Partnerships** should be established.

The tactical layer has four components which are proposed in the framework. The first component is a national cyber security awareness and education campaign. Chapter 3 (subsection 3.3.2) identified cyber security awareness and education as a core element of a holistic, multi-stakeholder and strategy-led approach when addressing cyber security. This suggestion was confirmed by the fact that all the countries analysed in chapter 4 (section 4.2) have one or more cyber security awareness and education initiative.

In addition, chapter 3 (section 3.5) revealed the role of awareness and education in achieving SA's vision of creating a culture of cyber security. As such, it is suggested in the framework that a campaign to spread awareness and education be developed. The proposed name for the South African campaign is *iWise Mzansi*.

iWise Mzansi suggests an informative SA, hence the “i”, and cyber wise SA, hence the name Mzansi. “Mzansi” is an accepted name that refers to SA. The findings in chapter 4 (subsection 4.3.4) indicate a variety of aspects that should be considered in such a campaign. One of those aspects is the establishment of partnerships with the following:

- public/private sector
- academia
- other nations

These partnerships would allow industry, academia and other nations to contribute to a country’s cyber security awareness and education. Such partnerships, particularly with other nations, would promote the alignment of cyber security awareness and education among nations. Moreover, in partnership with academia, *iWise Mzansi* would benefit current research that would help to align what the campaign has to offer with the specific needs of South African citizens.

From the cyber security awareness and education approaches of the countries discussed in this document, the subordinate campaigns and programmes are apparent. In accordance to this feature, it is proposed in the framework that *iWise Mzansi* should have the following subordinate campaigns and programmes:

- *iWise Mzansi* Week
- *iWise Mzansi* Community Outreach
- *iWise Mzansi*: For All
- *iWise Mzansi*: For Schools

It is proposed that *iWise Mzansi* could reach the people of SA through the abovementioned campaigns. *iWise Mzansi* week is intended to be an annual event aimed at all South African citizens. This week should serve as a reminder that cyber security is a shared responsibility and should also spread awareness of current cyber security issues. With all these campaigns, a South African flavour should be adopted, meaning the South African context should be taken into consideration.

iWise Mzansi Community Outreach is intended to give everyone an opportunity to lend a helping hand, similar to the campaign *Stop.Think.Connect*.*Friends*, as discussed in chapter 4 (subsection 4.2.1). This programme will allow any member of society to be part of *iWise Mzansi* by volunteering to participate in spreading the cyber security awareness and education to communities. This programme is closely linked with the well-known philosophy of ubuntu (humility) in SA (Murithi, 2006).

It is proposed that *iWise Mzansi*: For All should be an all-encompassing website addressing the general public in SA. This campaign could incorporate elements of the cyber security awareness and education websites analysed in chapter 4 (section 4.2). Finally, it is proposed that *iWise Mzansi*: For Schools should target primary and secondary schools.

Since cyber security education is broad in nature, a national cyber security awareness and education campaign is not the only end to cover. Alongside *iWise Mzansi*, are two more proposed components; these encompass formal cyber security education for students and cyber security education for those in the workforce. However, providing insight on what these two components should comprise of falls outside of the scope of this study. Furthermore, students together with people in the workforce are also part of society; therefore they will be included in *iWise Mzansi*.

The major facet of the tactical layer is the cyber security awareness and education campaign, *iWise Mzansi,* and also the suggested subordinate campaigns and programmes that should be used to reach South African citizens. The analysis of the campaigns in chapter 4 found that there are a number of topics that a campaign should cover; moreover, there are numerous tools available that can be used to communicate to different groups of people. Having said this, the following questions arise:

- What topics will *iWise Mzansi* cover?
- What communication tools will be employed?

Therefore, the following subsection will introduce another layer that will answer the questions posed above.

5.3.3 The preparation layer

In the previous layer, iWise Mzansi was introduced as the proposed South African national cyber security awareness and education campaign. Similar to the national cyber security awareness and education campaigns studied in chapter 4 (section 4.2), such a campaign must define the topics it will cover and the tools it will use. Therefore, the preparation layer will answer the questions posed in the previous subsection.

The preparation layer takes up where the tactical layer left off. Figure 5.7 presents the preparation layer.

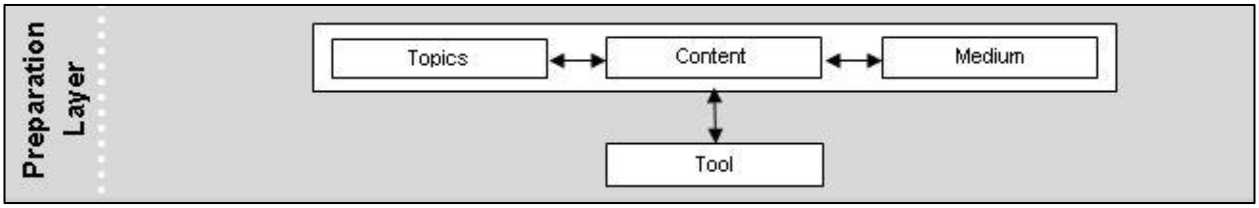


Figure 5.7: The preparation layer of the cyber security awareness and education framework

The preparation layer consists of four components:

- topics
- content
- medium
- tools

With regard to topics, from the analysis of cyber security awareness and education initiatives in chapter 4, a number of topics that are common throughout the initiatives may be identified. Such topics include, but are not limited to, cyber bullying, cyber stalking, identity theft, online scams, cyber crime, cyber-attacks, fraud, phishing, securing personal and private information online, and secure behaviour. These topics and more could be covered by *iWise Mzansi*. However, further research has to be done in order to find out the particular needs of South African citizens.

Figure 5.7 suggests a particular relationship between content and topic. This relationship is guided by the target audience that the material will be offered to. For example, if material on cyber bullying is offered to children, the content may include how to report a cyber bully. However, the same topic, offered to a different target audience such as a parent, may include such content as the warning signs of a cyber bullied child. Thus, there is a link between topic and content.

Figure 5.7 further presents a link between content and medium. This relationship suggests that based on the defined topic together with the content, a suitable medium of communication should be chosen. There are two acknowledged mediums referring to, that is, paper based and electronic. Once these elements are clear, the tools that will be used must be defined. As identified in chapter 4 (section 4.2) different tools are used in such campaigns. These tools include websites, videos, games, quizzes and so forth. Thus, a suitable tool should be chosen based on the topic, content and medium.

The preparation layer concerns itself with defining the cyber security awareness and education resources that *iWise Mzansi* will offer to the people of SA. From this layer one further question arises:

- To which target audience will *iWise Mzansi* deliver cyber security awareness and education?

This question will be answered in the following subsection.

5.3.4 The delivery layer

In chapter 3 (section 3.2), it was concluded that all levels of society are exposed to cyber security risks. Thus, cyber security awareness and education should be afforded to all levels of society. Chapter 4 (section 4.2) testifies to this as the cyber security awareness and education initiatives that were analysed proved to target different groups. Accordingly, the delivery layer concerns itself with the process of defining the target audience to which *iWise Mzansi* will deliver awareness and education. In addition, it will also define the roles that this audience will play within *iWise Mzansi* and amongst each other. Figure 5.8 below presents the delivery layer.

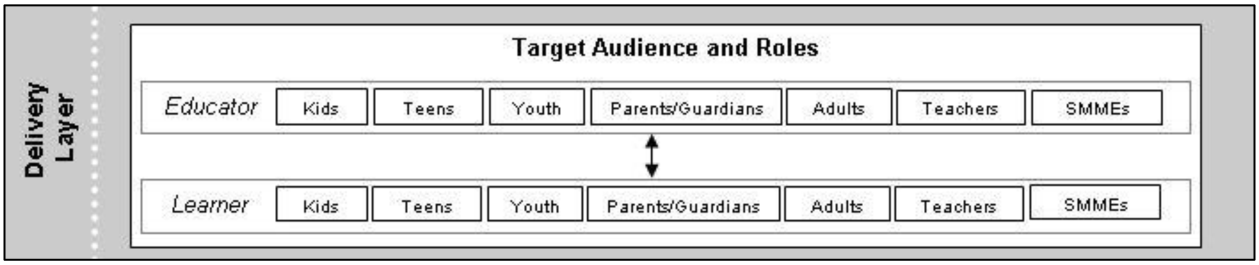


Figure 5.8: The delivery layer of the cyber security awareness and education framework

As portrayed by figure 5.8, the framework suggests that seven different target audiences should be defined, namely:

- children younger than 13 years
- teenagers
- youth
- parents/guardians
- adults
- teachers
- small, medium and micro-sized enterprises (SMMEs)

Chapter 3 (section 3.2) concluded that individuals, organisations and the nation at large are all exposed to the risks associated in cyberspace. Therefore, it is proposed in this layer that *iWise Mzansi* deliver cyber security awareness and education to the above-mentioned audiences as they represent the nation at large. In addition, this layer identifies two roles that these audiences should play:

- a learner role
- an educator role

It is clear that cyber security is the responsibility of everyone who enjoys the benefits offered by cyberspace. Therefore, it is recommended that the defined target audience take responsibility for using the resources that *iWise Mzansi* will offer to educate them, thus assuming the role of learner. Moreover, it is also recommended that everyone will pass on what they have learnt to other people, thus assuming the role of educator.

Once the target audiences and roles in *iWise Mzansi* are clear, what is left is defining the manner in which the progress towards achieving the primary cyber security awareness and education goal will be monitored. The monitoring component will be discussed in the following subsection.

5.3.5 The monitoring layer

One of the findings in chapter 4 (section 4.3) is that there should be monitoring and evaluation of the progress made in the cyber security awareness and education efforts. In addition, the effectiveness of the campaign should be evaluated. Therefore, this layer concerns itself with monitoring and evaluation. Figure 5.9 below presents the monitoring layer.

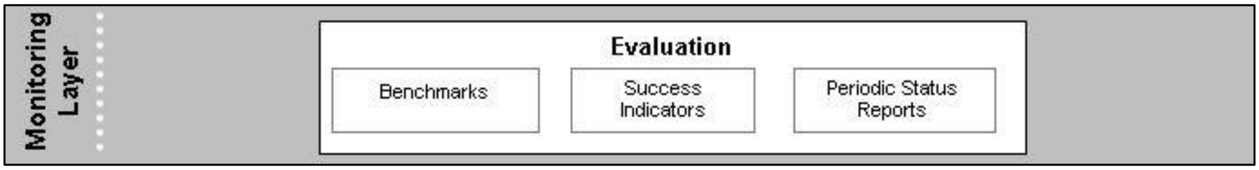


Figure 5.9: The monitoring layer of the cyber security awareness and education framework

The monitoring layer is the final layer of the cyber security awareness and education framework. It integrates one of the cyber security awareness and education key factors, as listed below.

- **Monitoring techniques** should be defined.

As identified in chapter 4 (section 4.3), some of the techniques that can be employed to measure progress are declaring benchmarks, defining success indicators and generating periodic status reports. In accordance to these findings, figure 5.9 shows that the framework suggests the following:

- Benchmarks must be declared.
- Success indicators must be defined.
- Periodic status reports must be generated.

It is suggested that the results of the evaluation should inform *iWise Mzansi*. In so doing this national cyber security awareness and education campaign should be adapted on the basis of the feedback from the evaluation. For instance, if a declared benchmark or certain success indicator fails to materialise, *iWise Mzansi* may possibly need to make some changes in the Preparation Layer. In this layer the topics, content or tools may be adapted in order to get the expected results.

The monitoring layer serves as the last layer of the framework. The following subsection will discuss the resources component.

5.3.6 Resources

In order for all the components identified in the framework within each layer to be addressed, certain resources have to be in place. As such, it was concluded in chapter 4 (section 4.2) that resources are needed to ensure cyber security awareness and education efforts. Therefore, it is suggested in the framework that such resources be taken into consideration and made available in order to achieve the primary cyber security awareness and education objective as detailed in the national cyber security policy. The figure below presents the resources component.

Resources
(People, Information, Applications, Infrastructure, and Financial Capital)

Figure 5.10: The resources relating to the cyber security awareness and education framework

The resources component is in line with the following cyber security awareness and education key factor:

- **Resources** should be in place.

The framework identifies five types of resource that will be needed as input in all the framework layers, as shown by figure 5.10. These resources are as follows:

- People – the people needed to carry out a certain function.
- Information – the information required to carry out a function.
- Applications – computer applications such as the software programs that will be needed.
- Infrastructure – the physical hardware such as computers and servers.
- Financial capital – the monetary resources that will be needed.

These resources are adopted from the Information Technology Infrastructure Library (ITIL) and have been identified as being essential to delivering an information technology service (Kim & Renée, 2007). In the context of this framework, cyber security awareness and education is the service which will be delivered. Therefore, within the five layers of the framework, appropriate resources have to be identified.

In the strategic layer, all the resources will be required in order for the three components of this layer to be in position. In addition, people will be needed who have the capacity to establish the responsible unit and develop the strategic plan, as will information that will inform the decision of the route to be taken in establishing the responsible people. Further, the infrastructure and computer applications to develop the strategic plan will also be required and, finally, the financial capital to fuel these efforts will be essential.

The tactical layer necessitates people to initiate the iWise Mzansi campaign together with its sub-campaigns and programmes. It will therefore require relevant information on the steps that should be taken to establish a cyber security awareness and education campaign. Finally, it will require money to instigate the initiative.

With regard to the preparation layer, all the resource types should be made available. These include people to define the topics, content, medium and tools. In addition, relevant information to guide the decision on the subject of which topics to include for each target audience will be needed. Therefore, infrastructure and the computer applications for compiling the study resources will be essential in this layer. Likewise, the funds to afford all the other resources will play a part.

The delivery layer will require guiding information as an input, in order to govern the way the target audience should play the roles that have been identified for them. In the monitoring layer, the people who will be commissioned to define the benchmarks, that is, the success indicators will be needed. For the infrastructure, computer applications and information will be needed in order to generate the report. Likewise, funds should be made available to meet the expense of additional resources.

Table 5.1 gives a summary of the types of resource that are essential in each layer of the proposed framework.

Table 5.1: Resources for the cyber security awareness and education framework

Layers	People	Information	Applications	Infrastructure	Financial capital
Strategic layer	✓	✓	✓	✓	✓
Tactical layer	✓	✓	-	-	✓
Preparation layer	✓	✓	✓	✓	✓
Delivery layer	-	✓	-	-	-
Monitoring layer	✓	✓	✓	-	✓

It can be gathered from table 5.1 that each and every layer of the cyber security awareness and education framework will need one or more resources in order for the components for each layer to be in place. Hence, the government has a duty to ensure this.

This subsection marks the last component of the proposed framework. Therefore, the next subsection will present the complete proposed cyber security awareness and education framework.

5.3.7 The framework

Up to now, this section has discussed the separate layers of the proposed cyber security awareness and education framework. This subsection will present the complete framework.

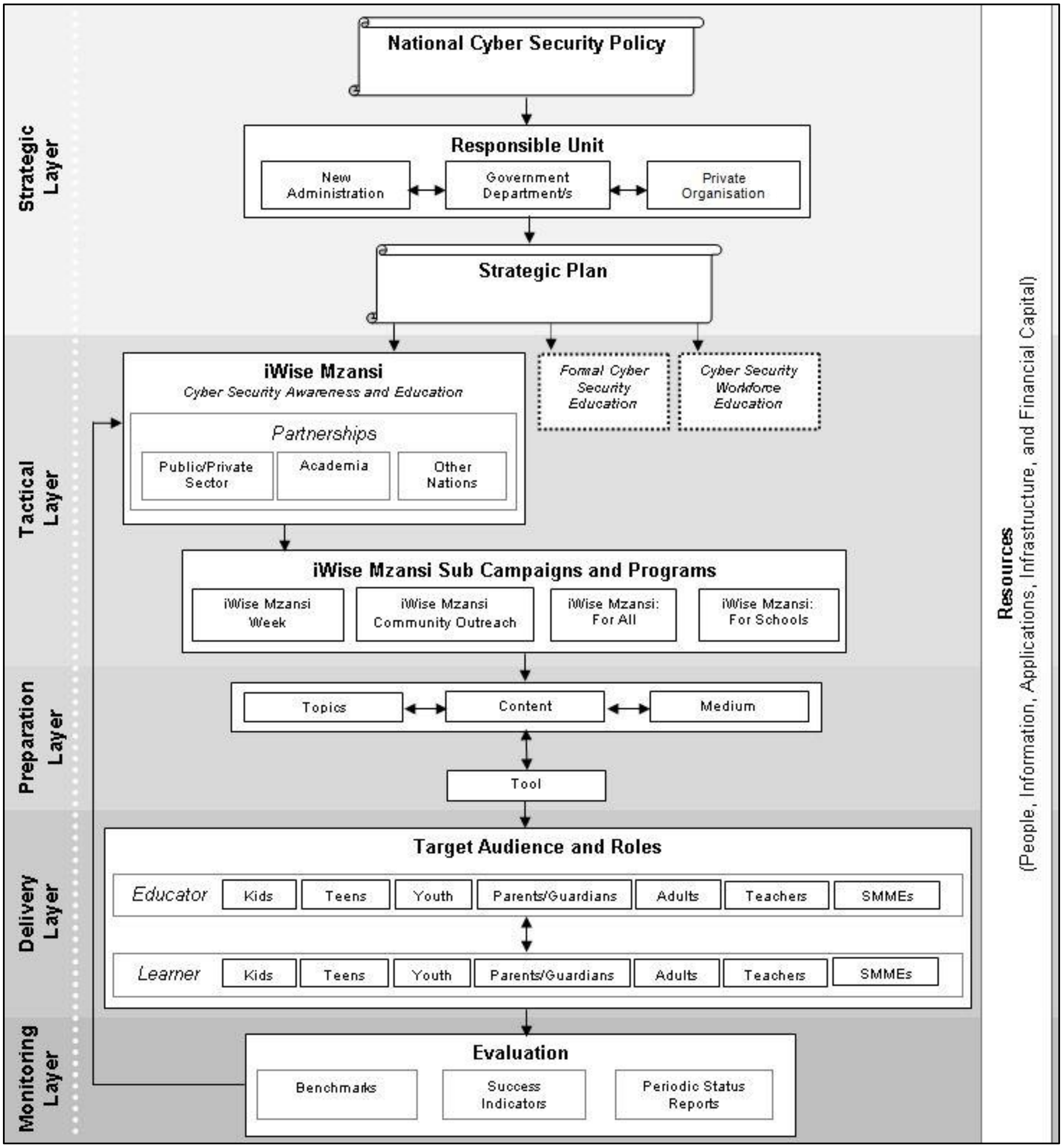


Figure 5.11: Cyber security awareness and education framework

Figure 5.11 presents the proposed cyber security awareness and education framework which integrates all the previously discussed layers. The following reiterates the framework layers:

- The strategic layer – this layer reflects the overall vision of the government concerning cyber security awareness and education.
- The tactical layer – this layer suggests the schemes that SA should employ to realise its cyber security awareness and education goals.
- The preparation layer – this layer prepares the contents of the scheme identified in the tactical layer.
- The delivery layer – this layer defines the recipients of the preparations made in the preparation layer, namely, the target audience.
- The monitoring layer – this layer examines the progress made by the scheme towards fulfilling the governments' vision.
- Resources – this component defines the resources which should be inputs to all the aforementioned layers.
- The previous subsections make reference to each of the cyber security awareness and education key factors incorporated within the layers. These therefore form the basis of the framework.

The primary objective of this study is to propose a framework that will assist SA in achieving its cyber security awareness and education objectives as detailed in the Draft National Cyber Security Policy Framework. This objective, as recorded in chapter 3 (section 3.4), is to create a cyber security culture among South African citizens. The ingredients of such a culture were sought in chapter 3 (section 3.5) and it was concluded that cyber security awareness and education was one the core ingredients of creating the envisaged culture.

Further investigation was conducted in chapter 4 in order to identify the key factors of cyber security awareness and education. Accordingly, these key factors formed the basis of the proposed framework. The layers of the proposed framework are in line with the Plan-Do-Check-Act (PDCA) cycle presented by figure 5.12.

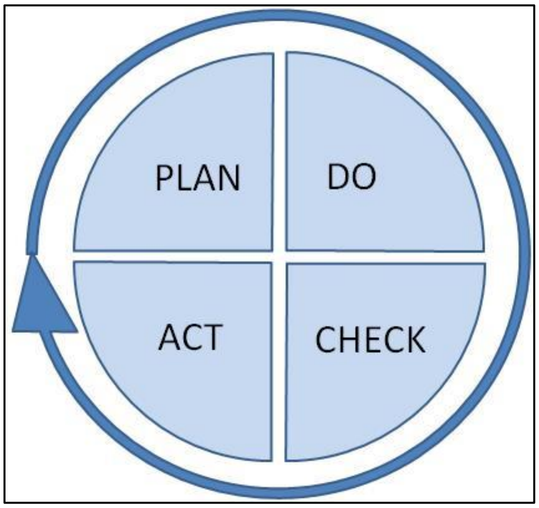


Figure 5.12: PDCA cycle (Expert Program Management, 2009)

Figure 5.12 depicts the iterative four-step process of the PDCA Cycle. According to ISO/IEC 27000 these steps signify the following (ISO/IEC 27000, 2009):

- Plan – establishing objectives and processes which are necessary in order to deliver certain outcomes.
- Do – implementing the outlined plan.
- Check – monitoring and measuring progress against particular requirements.
- Act – taking action in accordance to the feedback obtained from the monitoring.

These steps overlap well with the layers of the proposed framework, as the “planning” step can be recognised in the strategic and tactical layers, and the “doing” step can be seen in the preparation and delivery layers. In addition, the checking step can be recognised in the monitoring layer. Finally, the feedback from the monitoring layer triggers the acting step, as elaborated in subsection 5.3.5 of this chapter.

The use of this framework will enable SA to define a national cyber security awareness campaign, *iWise Mzansi.* This campaign will serve as a means for providing SA citizens with the necessary cyber security understanding and knowledge, and will therefore contribute to the creation of the envisaged culture.

5.4 Conclusion

It is an established fact that awareness and education are core to cultivating a cyber security culture. Accordingly, this chapter introduced a proposed cyber security awareness and education for SA. It is envisaged that this framework will assist SA in its endeavour of fostering a culture of cyber security among its citizens.

The implementation of this framework will afford SA a national cyber security awareness campaign, *iWise Mzansi*. Furthermore, making use of its subsidiary campaigns will mean that South African citizens will be the recipients of cyber security awareness and education that is suitable for a South African audience.

This chapter has accomplished the primary objective of this study, which is to propose a framework that will assist SA in creating a cyber secure culture among all of its users of cyberspace. The following chapter will evaluate the proposed framework.

CHAPTER 6: THE EVALUATION OF THE FRAMEWORK

6.1 Introduction

“Evaluation is a crucial component of the research process” (Hevner, March, Park, & Ram, 2004).

The previous chapter introduced the proposed cyber security awareness and education framework for South Africa (SA). Since evaluation is deemed crucial to the research process, this chapter intends to provide the evaluation of the proposed cyber security awareness and education framework. This is in line with the demonstration and evaluation steps in the design science approach introduced in chapter 1.

This chapter will define the approach that was employed to evaluate the framework. Thereafter, it will discuss the feedback obtained during the evaluation process. In light of this feedback, this chapter will furthermore indicate how the framework was adapted. This will be followed by a number of concluding remarks.

6.2 Evaluation approach

As a result of the research paradigm of this study – design science – evaluation is deemed as a very important component of the research process. Through evaluation, the extent to which the artefact supports the solution to the identified problem can be measured (Peffers, Tuunanen, Rothenberger, & Chatterjee, 2008). Among other effects, the use of well-executed evaluation methods also demonstrates the quality of an artefact (Hevner et al., 2004). This makes it possible to address both the demonstration and the evaluation steps of design science.

An artefact can be evaluated using evaluation methods that exist within the body of knowledge (Hevner et al., 2004). The artefact to be evaluated in the case of this study is the proposed cyber security awareness and education framework. As such, this framework will be evaluated through the use of semi-structured interviews.

Semi-structured interviews are more flexible in nature when compared to structured interviews (Kajornboon, 2005). With structured interviews, all respondents are asked standardised questions that have been formally structured in the interview guide (Kajornboon, 2005). Closed-ended questions are usually posed in this type of interview (Bryman, 2001). Corbetta (2003) argues that structured interviews are somewhat rigid. As a result, this rigidity becomes a problem if the interview wishes to further explore a particular response from the respondent.

In the case of semi-structured interviews, instead of standardised questions the interview guide may consist of specific themes that suggest the topics the interviewer wishes to cover, although the questions to be asked may vary from respondent to respondent (David & Sutton, 2004). This form of interview gives the interviewer the opportunity to probe deeper into any given topic (Kajornboon, 2005). For this reason semi-structured interviews, in the form of elite/expert interviews, were used to evaluate the proposed cyber security awareness and education framework. The following subsection will elaborate on these elite/expert interviews.

6.2.1 Elite interviews

Elite/expert interviews are defined as “a discussion with someone knowledgeable about a problem or its possible solution” (Cooper & Schindler, 2003). As previously mentioned, elite/expert interviews are semi-structured interviews. As such, they are flexible in nature and do not require a standard set of questions to be included in the interview guide. In this form of interview, the interview guide consists of a list of themes, which largely guides the questions asked. However, as already mentioned, questions vary from respondent to respondent.

According to Cooper and Schindler (2003), this method of interviewing is used to discuss a subject with a knowledgeable person, the ‘elite’. Hochschild (2009), Marshall and Rosman (2011) and Tansey (2007) shed light on some of the advantages of expert/elite interviews. These are outlined below.

Advantages of the elite/expert interview:

- The interviewer has the opportunity to triangulate information among interviewees without revealing the names of other respondents.
- Elites are more capable of providing a general view of a particular subject.
- The interviewees are able to provide valuable information as a result of their respective positions.

With elite/expert interviews, the interviewer has the opportunity to probe a topic in depth in order to gain more insight and understanding on a particular subject. The subject in this case is cyber security awareness and education. Thus, the chosen elite are knowledgeable on the subject of cyber security awareness and education. The following subsection will discuss the elites.

6.2.1.1 The ‘elites’

Marshall and Rossman (2011) define an elite individual as someone who is influential, prominent and well informed about a particular area in the research study. Hochschild (2009) further maintains that the person’s position is also a contributing factor when considering elites. There are known categories of elites, namely, ultra-elites and professional elites. Zuckerman (1972) refers to ultra-elites as individuals who possess a lot of power within a group of elite individuals, while McDowell (1998) defines professional elites as “highly-skilled, professionally competent and class-specific”.

Smith (2006) argues that researchers define the term ‘elite’ in a manner that is subjective to the relevant respondents. By contrast, this research will not seek a new definition for the term ‘elite’; it will merely adopt the definition provided by Marshall and Rossman (2011).

Owing to the nature of elites, gaining access can be a challenge (Mikecz, 2012). However, in the case of this research gaining access was comparatively easy. Contrary to Conti and O’Neil (2007), who recommend the use of formal letters followed by phone calls to make contact with elites, emails where used. This decision was influenced by the electronic nature of the modern day. As such, using emails to contact the elites proved to work well as they gave prompt responses.

In this study, the elites where chosen based on their line of work, experience and knowledge in the field of cyber security, particularly in the awareness and education domain. Two elites where selected to review the proposed framework in an elite interview. The following section will present an account of the two interviews.

6.2.1.2 The framework validation

A week prior to conducting the elite interview, an interview brief was sent to the elites. This was a three-page document aimed at introducing the framework and also providing some background on the form of the interview to be conducted. This was done in order to allow the elites to understand what was expected them. The brief can be seen in Appendix B.

Before interviewing the elites, the proposed cyber security awareness and education framework was presented in the form of a PowerPoint slide show. This presentation was intended to elaborate on the underlying research that forms the basis of the proposed framework. In addition, all the layers and components of the proposed framework were presented in detail so that the elites could have a clear understanding of the context. Subsequently, the elite interview was conducted.

As mentioned in section 6.2, an elite interview is semi-structured and does not call for standardised questions. However, in this case the questions were fairly standard and both elites were asked the same questions. Nevertheless, even though the questions were fairly standard, with this choice of interview the researcher had the opportunity to probe information provided by the elites.

The interview guide containing the list of questions is presented in Appendix C. The questions asked were intended to verify the layers, components and comprehensiveness of the proposed cyber security awareness and education framework. Furthermore, what was essential was to obtain the elites' confirmation that the proposed framework would contribute to cyber security.

The interview was audio taped using a mobile phone. The audio tape was then transcribed and the transcription can be found in Appendix D. The elites noted a few concerns regarding the proposed framework. With regard to the five layers of the framework, both elites approved these layers and one of the elites expanded by saying:

> *"Yes, I do agree with the layers of the framework, one of the phases of any awareness that we always have, which I have picked up from various studies that, others have three and others they have two. These phases are preparation phase, followed by the design phase, and then you have implementation phase and your review phase for your monitoring.*
>
> *So, those four phases are cyclic, you make sure that the awareness is the continuous thing, simply because as you mentioned there are always threats, the more we use the internet the more we come across these threats. So, those phases will make your framework to … I don't know … It will ensure that each*

> *and every layer is revisited annually to check how did it go and where they can improve. That will make your framework more right, I mean more alive. So I agree with it, it does look like it has all of them."*

The tables below provide a summary of other remarks made by the elites and how the researcher responded to them. More detail on the feedback from the elites is recorded in Appendix D.

Table 6.1: Elite no. 1

Raised Concerns	**Response to concern**
"In the line that indicates the feedback from the monitoring layer to the tactical layer. **So you should write 'continuously'**	Characteristically, if there is a feedback link from a monitoring to other layers it is implied that a loop will occur if needs be. Thus it was not seen necessary to insert a label to the framework that will specifically state 'continuous'.
"…From the strategic layer I prefer personally if you would call it a strategic implementation plan so that as soon as it comes to the tactical layer, although they are still designing it [strategic plan] they are busy with its implementation."	In the analysis in Chapter 4, it was argued that a 'strategic plan' should be drafted. Accordingly, should the framework propose a 'strategic implementation plan' it might seem as though there is variation from what was deducted in Chapter 4. Moreover, some aspects in the strategic plan are inherently meant to be implemented.
In the delivery layer, I suggest you **add guardians as a target audience** because	Guardians where added as target audience in Delivery Layer of the proposed

speaking from a professional's point of view, when I am at work it is the guardians who are with the children and helping them with homework and all".	cyber security awareness and education framework.
"I do feel that giving kids the responsibility to educate others is too much of a responsibility. Also, depending on the culture of the audience that your framework targets having a child educate a parent might not work out well. Please do consider such factors"	It is known that cyber security is the responsibility of everyone who enjoys its benefits. This notion also applies to kids. Furthermore, the UK adopts this methodology and believes that kids more easily learn and accept input from their peers (Atkinson, Furnell, & Phippen, 2009). In addition, de Lange and von Solms (2013) state that children can also play the role of educating older individuals. Therefore in the proposed framework, giving the kids the responsibility to pass on knowledge and awareness is not viewed as too much responsibility
"In the preparation layer, **the tools and the medium both falls under delivery methods**, therefore I suggest you group them together."	Chapter 4 (subsection 4.3.3) brings forth a relationship between topics, contents and medium. If we remove medium and group it with tools this relationship will be neglected. For this reason it is suggested that medium remains as is.

Table 6.2: Elite no. 2

Raised concerns	**Response to concern**
"The one thing is from the delivery layer, if you look at schools you will have a problem with awareness being the responsibility of the DOC as opposed to schools being the responsibility of the Department of Basic Education. So I think you should make reference to the two governments [i.e. departments], the interrelationship between the government departments. That means, **your framework must make provision for the interrelatedness of cyber security and different government departments**"	This concern was addressed by adding a relationship indicator to the responsible unit component found in the strategic layer.
"In the comparative analysis you did to come up with the key factors, you did not mention Estonia. The reasons **I suggest you include Estonia** are that it was the first country to react to a cyber-attack. Estonia is the only country with the highest governance and integration of IT; you will see if you read that in Estonia you pay for almost everything electronically. That means if their banking systems go down the economy goes down. They had a DDos attack in their banking systems, and	Chapter 4 (section 4.1) makes known the criteria used to select the developed countries that were studied. As such, in the case of Estonia, some of the documentation deemed important to the study needed to be translated before being used. This was a disadvantage, mainly because the integrity of the information would come into question. However, Estonia is recognised in the background chapters.

that is the reason why Estonians are leaders in driving cyber security in Europe and in the world.”	
“**Propose a month for *iWise Mzansi*** because most countries have a month and a week is too short”.	Although it is an established fact that developed countries have a cyber security month, a week is advised for SA since the country is in the early stages of initiating its government-led cyber security awareness and education campaign.

In addition to the above-mentioned concerns, the elites were positive about the contribution the proposed cyber security awareness and education framework would make to the cyber security culture envisaged by SA.

> *“The framework will contribute to cyber security awareness and education because it structures things that people are currently doing a little bit there and there, things that people don’t see as a full blown framework. The framework nicely links all these facets.”*

Based on the feedback received from the elites it can be concluded that the proposed framework was sufficiently validated. Moreover, the demonstration and evaluation steps as part of a design science approach have been conducted satisfactorily. Therefore it can be argued that the cyber security awareness and education framework is sound.

6.3 Conclusion

This chapter discussed the validation of the proposed cyber security awareness and education framework. It furthermore discussed the approach that was taken to perform the validation, together with the inputs provided by the elites. The manner in which their remarks were addressed was also provided in this chapter. Accordingly, the proposed framework was refined from its initial design to incorporate the feedback from the elites who were interviewed.

As the validation shows, the layers and components of the framework were approved by the elites. The elites furthermore confirmed that the framework proposed by this study would indeed contribute to the creation of a South African cyber security culture. In conclusion, one may say that the use of this framework will bring SA one step closer to its envisaged cyber security culture.

CHAPTER 7: CONCLUSION

7.1 Introduction

“A writer needs to keep in mind that the conclusion is often what a reader remembers best” (Holewa, 2004).

This study focused on South African efforts towards cyber security awareness and education. It was established that even though the South African government seeks to create a cyber security culture, it does not currently have government-led cyber security awareness and education initiatives in place. Therefore the aim of this study was to propose a framework for cyber security awareness and education in SA. This framework was presented in chapter 5 and validated in the previous chapter (chapter 6). With that accomplished, this chapter will conclude this dissertation by providing an overview of the chapters and highlighting the major aspects and arguments. Furthermore, the objectives of this study will be revisited. Thereafter, a discussion concerning how these objectives were addressed will be provided. Finally, possible further research will be discussed.

7.2 Summary of chapters

In **chapter 1**, it was established that awareness and education form an integral part of cyber security. As such, after determining the cyber security awareness and education situation in SA, it became clear that in SA there is a definite lack of government cyber security awareness and education initiatives. This conclusion suggests that SA is ill prepared to afford cyber security awareness and education for its citizens. Based on the identified problem, research objectives were formulated. In addition, the research process that this study employed to accomplish the outlined objectives was also discussed.

A brief history about the origin of the Internet as well as its evolution to what today is known as cyberspace was provided in **chapter 2**. It was concluded that cyberspace has become interwoven in the daily activities of individuals, businesses and nations. Some of the online services used by such groups were also discussed. It was emphasised that many rely on cyberspace to perform various functions on a daily basis.

Considering this reliance on cyberspace, it was deemed necessary to investigate the risks that individuals, businesses and nations are exposed to while active online. Accordingly, this was done in **chapter 3**. It was concluded that all users of cyberspace are affected by the malicious acts apparent online and, as a result, there is a need for security measures. It was furthermore deduced that a holistic approach to cyber security necessitates awareness and education.

Owing to the significant role that awareness and education play in cyber security, **chapter 4** focused on examining the cyber security awareness and education initiatives of various developed countries. This examination was done in order to extrapolate key factors that would form the basis of the framework that was to be developed.

In view of these key factors, the framework for cyber security awareness and education was developed in **chapter 5**. It was then argued that this framework would contribute to the creation of a culture of cyber security as intended by the South African government.

Consequently, the framework was verified. **Chapter 6** discussed the approach taken to verify the framework. It furthermore presented the feedback obtained from the verification process, as well as explaining how the framework was adapted in line with the feedback. Thus, on the basis of the performed verification the framework is considered sound.

7.3 Summary of contribution

Cyberspace has modified the manner in which things are done by introducing online services intended to enhance people’s lifestyles. In view of this, individuals, organisations and nations have become increasingly dependent on cyberspace to perform many functions. By contrast, cyberspace has also supported crime by introducing new risks. As a result, the need for cyber security has never been greater.

In the interests of promoting safety and security in cyberspace, spreading awareness and educating citizens about the risks online was recognised as one of the fundamental aspects. However, it was shown that SA is lacking in this regard. Thus, the problem that this study addressed is that *SA is ill prepared to educate its citizens on how to behave securely whilst active in cyberspace. For this reason, individuals put themselves, as well as businesses and governmental assets and infrastructure, at risk.*

In an attempt to address the identified problem, the primary objective of this study, as set out in chapter 1 (section 1.3), was *to propose a cyber security awareness and education framework for South Africa that would assist in creating a cyber secure culture in SA for all its users of cyberspace.*

In order to address this objective, secondary objectives were outlined in chapter 1 (section 1.3) as listed below:

- *to identify the position of awareness and education in a cyber security culture*
- *to evaluate the initiatives that some developed countries have in place for cyber security awareness and education*
- *to identify the key factors that need to be addressed in developing a national cyber security awareness and education framework for SA*

Secondary objective 1 – *to identify the position of awareness and education in cyber security culture* – was addressed in chapter 3. It was established that awareness and education are pillars of a cyber security culture. Furthermore, as part this study, a peer-reviewed paper on cultivating a cyber security culture was published and presented at the 2012 ZA-WWW Conference (Appendix A1).

Secondary objective 2 – *to evaluate the initiatives that some developed countries have in place for cyber security awareness and education* – was addressed in chapter 4. This chapter provided an analysis of the United States (US), the United Kingdom (UK), Australia, and Canada, focusing on the national cyber security strategies of these countries, as well as nationally initiated and driven cyber security awareness and education initiatives. Thus, this objective was satisfactorily met.

Secondary objective 3 – *to identify the key factors that need to be addressed in developing a national cyber security awareness and education framework for SA* – was also addressed in chapter 4. Based on the analysis of the US, the UK, Australia and Canada, a suite of cyber security awareness key factors were identified. These key factors are as follows:

- Cleary articulated **goals** should be defined.
- A **dedicated team** should be appointed.
- An **action plan** should be outlined.
- A **national cyber security awareness and education campaign** should be defined.
- **Partnerships** should be established.
- **Resources** should be in place.
- **Monitoring techniques** should be defined.

These key factors were argued and reviewed in a peer-reviewed paper which was published and presented at the AFRICOMM 2012 conference (Appendix A2). These key factors formed the basis of the cyber security awareness and education framework for SA. In addition, a paper concerning the framework was submitted in the South African Computer Journal (SACJ) (Appendix A3).

It is evident that each of the secondary objectives has been met. It can, therefore, be argued that the primary objective of this study, which was to develop a cyber security awareness and education framework for SA, has been met satisfactorily.

7.4 Future research

It was established that a cyber security culture is fundamental to promoting cyber security. In addition, cyber security awareness and education form the pillars of a cyber security culture. This study proposed a framework to assist SA in creating a cyber security culture that, as was argued, would enable SA to define a national cyber security awareness campaign, *iWise Mzansi.* This campaign would provide the necessary cyber security understanding and knowledge for South African citizens, and would therefore contribute to the creation of the envisaged culture.

This framework is just one step towards the envisaged cyber security culture. As such, in order for this framework to be useful, it needs to be implemented. However, this study had its limitations in that it did not focus on the implementation of the framework. Therefore, future research focusing on addressing the practical implementation of the proposed framework would be beneficial.

7.5 Final word

Cyberspace had humble beginnings. Over time it has progressed immensely providing individuals with endless opportunities. Embedded in these opportunities, however, are risks that compromise the safety and security of the individuals that participate in cyberspace. To a large extent people are unaware of these risks; and so they put themselves, as well as businesses and governmental assets and infrastructure, at risk.

In recognition of this, SA wishes to promote a culture of cyber security among its citizens. This study revealed that cyber security awareness and education plays a big role in cultivating such a culture. Accordingly, this study developed and evaluated a cyber security awareness and education framework that will assist SA in promoting its envisaged cyber security culture.

REFERENCES

Abbate, J. E. (1994). *From ARPANET to Internet: A history of ARPA-sponsored computer networks*. University of Pennsylvania. Retrieved July 20, 2013, from http://repository.upenn.edu/dissertations/AAI9503730

Allen, E., & Fermestad, J. (2000). E-Commerce Strategies: The Manufacturer Retailer Consumer Relationship. In *Proceedings of the 5th Americas Conference on Information Systems: 2000*. New York NY: IRWIN.

Anderson, J., Boyles, J., & Rainie, L. (2012). Higher Education: Experts Expect More Efficient Collaborative Environments and New Grading Schemes; They Worry about Massive Online Courses, the Shift Away. *Pew Internet & American Life Project*, 1–43. Retrieved April 16, 2013 from http://www.eric.ed.gov/ERICWebPortal/recordDetail?accno=ED534048

Atkinson, S., Furnell, S., & Phippen, A. (2009). Securing the next generation: enhancing e-safety awareness among young people. *Computer Fraud & Security*, *2009*(7), 13–19. doi:10.1016/S1361-3723(09)70088-0

Australian Communications and Media Authority. (2010). Newsroom. *Cyberzine*. Retrieved June 15, 2013, from http://www.cybersmart.gov.au/About Cybersmart/Newsroom/Cyberzine/Cyberzine Issue 3.aspx

Australian Communications and Media Authority. (2013). Cyber(smart:). *CyberSmart*. Retrieved June 20, 2013, from http://www.cybersmart.gov.au/

Australian Competition and Consumer Commission. (2013). ScamWatch. *ScamWatch*. Retrieved June 25, 2013, from http://www.scamwatch.gov.au/content/index.phtml/itemId/693900

Benedikt, M. (1991). *Cyberspace: first steps* (M. Benedikt, Ed.) (p. 436). MIT Press.

Blackberry. (2013). BlackBerry Technical Support Services. Retrieved April 05, 2013, from http://za.blackberry.com/support/programs/technical.html

Bremmer, I. (2010). Democracy in Cyberspace: What Information Technology Can and Cannot Do. *Foreign Affairs*, *86*(6), 86–92.

Brody, R. G., Mulig, E., & Kimball, V. (2007). Phishing, pharming and identity theft. *Academy of Accounting and Financial Studies Journal*, *11*(3), 43–57.

Bryman, A. (2001). *Social research methods*. Oxford University Press.

Buhalis, D. (2004). eAirlines: strategic and tactical use of ICTs in the airline industry. *Information & Management*, *41*(7), 805–825. doi:10.1016/j.im.2003.08.015

Burden, K., & Palmer, C. (2003). Internet crime: Cyber Crime—A new breed of criminal? *Computer Law & Security Review*, *19*(3), 222–227.

Burt, S., & Sparks, L. (2003). E-commerce and the retail process: a review. *Journal of Retailing and Consumer Services*, *10*(5), 275–286. doi:10.1016/S0969-6989(02)00062-0

Cabinet Office. (2011). *The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world* (p. 43). Retrieved April 25, 2012, from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf

Camp, W. G. (2001). Formulating and evaluating theoretical frameworks for career and technical education research. *Journal of Vocational Education Research*, *26*(1), 4-25.

Campbell, M. A. (2005). Cyber bullying: An old problem in a new guise? *Australian Journal of Guidance and Counselling*, *15*(1), 68–76.

Chadwick, A., & May, C. (2003). Interaction between States and Citizens in the Age of the Internet: “e-Government” in the United States, Britain, and the European Union. *Governance*, *16*(2), 271–300. doi:10.1111/1468-0491.00216

Chen, Y.-Y. (2012). Why Do Consumers Go Internet Shopping Again? Understanding the Antecedents of Repurchase Intention. *Journal of Organizational Computing and Electronic Commerce*, *22*(1), 38–63. doi:10.1080/10919392.2012.642234

Choo, K.-K. R. (2009). *Online child grooming: a literature review on the misuse of social networking sites for grooming children for sexual offences*. (A. I. of Criminology, Ed.). Australian Institute of Criminology.

Choo, K.-K. R. (2011). The cyber threat landscape: Challenges and future research directions. *Computers & Security*, *30*(8), 719–731. doi:10.1016/j.cose.2011.08.004

COMESA. (2013). e-Trade. Retrieved April 09, 2013, from http://egov.comesa.int/index.php/en/e-trade/24-e-trade

Commonwealth of Australia. (2009). *Cyber Security Strategy* (p. 38). Retrieved March 1, 2013, from http://www.ag.gov.au/RightsAndProtections/CyberSecurity/Documents/AG%20Cyber%20Security%20Strategy%20-%20for%20website.pdf

Condron, S. M. (2007). Getting It Right: Protecting American Critical Infrastructure in Cyberspace. *Harvard Journal of Law & Technology*, *20*(2), 404–421.

Conklin, A., & White, G. B. (2006). e-Government and Cyber Security : The Role of Cyber Security Exercises. In *Proceedings of the 39th Hawaii International Conference on System Sciences* (Vol. 4, pp. 1–8).

Conti, J. A., & O'Neil, M. (2007). Studying power: qualitative methods and the global elite. *Qualitative Research*, *7*(1), 63–82.

Cooper, D. R., & Schindler, P. S. (2003). *Business Research Methods* (p. 857). McGraw-Hill School Education Group.

Corbetta, P. (2003). *Social research: Theory, methods and techniques*. SAGE Publications Limited.

Daniel, E., & Storey, C. (1997). On-line banking: Strategic and management challenges. *Long Range Planning*, *30*(6), 890–898. doi:10.1016/S0024-6301(97)00074-5

David, M., & Sutton, C. D. (2004). *Social research: The basics*. SAGE.

Davinson, N., & Sillence, E. (2010). It won't happen to me: Promoting secure behaviour among internet users. *Computers in Human Behavior*, *26*(6), 1739–1747. doi:10.1016/j.chb.2010.06.023

Davis, L. M., Golinelli, D., Beckman, R., Cotton, S. K., Anderson, R. H., Bamezai, A., & Steinberg, P. (2008). *The National Computer Security Survey (NCSS)*. US.

De Joode, A. (2011). Effective corporate security and cybercrime. *Network Security*, *2011*(9), 16–18. doi:10.1016/S1353-4858(11)70097-6

Dennis, J. (2010, April 28). SA seventh in global cyber crime list. *Times Live*. South Africa. Retrieved May 5, 2012, from http://www.timeslive.co.za/local/article423649.ece/SA-seventh-in-global-cyber-crime-list

Department of Broadband Communications and Digital Economy. (n.d.). Stay Smart Online. Retrieved June 30, 2013, from http://www.staysmartonline.gov.au/

Department of Homeland Security. (2012a). Stop.Think.Connect. Retrieved May 05, 2013, from http://www.dhs.gov/stopthinkconnect

Department of Homeland Security. (2012b). Stop.Think.Connect. Cyber Awareness Coalition. Retrieved May 03, 2013, from http://www.dhs.gov/stopthinkconnect-cyber-awareness-coalition

Department of Homeland Security. (2012c). Stop.Think.Connect. Friends of the Campaign Program. Retrieved June 05, 2013, from http://www.dhs.gov/stopthinkconnect-friends-campaign-program

Department of State Security. (2012). Statement on the approval by Cabinet of the Cyber Security Policy Framework for South Africa. Retrieved June 05, 2012, from http://www.info.gov.za/speech/DynamicAction?pageid=461&tid=59794

Dlamini, I. Z., Taute, B., & Radebe, J. (2011). Framework for an African Policy Towards Creating Cyber Security Awareness. *Security*. Retrieved February 20, 2012, from http://researchspace.csir.co.za/dspace/handle/10204/5163

Dlamini, Z., & Modise, M. (2012). Cyber security awareness initiatives in South Africa: a synergy approach. In *7th International Conference on Information Warfare and Security*. USA: Academic Conferences International. doi:10.1007/978-3-8349-4134-3_3

Duderstadt, J. J., Atkins, D. E., & Van Houweling, D. E. (2002). *Higher education in the digital age: Technology issues and strategies for American colleges and universities*. Rowman & Littlefield Publishers.

Duggan, M., & Brenner, J. (2013). *The Demographics of Social Media Users — 2012*. Washington, D.C. Retrieved March 20, 2013, from http://pewinternet.org/Reports/2013/Social-media-users.aspx

Embar-Seddon, A. (2002). Cyberterrorism: Are We Under Siege? *American Behavioral Scientist*, *45*(6), 1033–1043. doi:10.1177/0002764202045006007

Expert Program Management. (2009). *The Plan, Do, Check, Act Cycle (The Deming Cycle)*. Retrieved April 25, 2013, from http://www.expertprogrammanagement.com/2010/10/the-plan-do-check-act-cycle-the-deming-cycle/

Eynon, R. (2005). The use of the internet in higher education: Academics' experiences of using ICTs for teaching and learning. *Aslib Proceedings*, *57*(2), 168–180. doi:10.1108/00012530510589137

Fallows, D. (2004). The Internet and Daily Life. Retrived April 20, 2013, from http://www.pewinternet.org/2004/08/11/the-internet-and-daily-life/

Fallows, D. (2005). *How Women and Men Use the Internet* (p. 54). Washington, D.C. Retrieved May 13, 2013, from http://www.pewinternet.org/2005/12/28/how-women-and-men-use-the-internet/

Fletcher, N. (2007). Challenges for regulating financial fraud in cyberspace. *Journal of Financial Crime*, *14*(2), 190–207.

Furling, A. L., & Digman, L. . (2000). The Impact of Electronic Commerce on Business Level Strategies. *Journal of Electronic Commerce Research*, *1*(1), 13–23.

Furnell, S. (2008). End-user security culture: a lesson that will never be learnt? *Computer Fraud & Security*, (April). Retrieved August 20, 2012, from http://www.sciencedirect.com/science/article/pii/S1361372308700642

Futcher, L., Schroder, C., & von Solms, R. (2010). Information security education in South Africa. *Information Management & Computer Security*, *18*(5), 366–374. doi:10.1108/09685221011095272

Gascoyne, R. J., & Ozcubukcu, K. (1997). *Corporate Internet Planning Guide: Aligning Internet Strategy with Business Goals*. New York NY: Van Nostrand Reinhold Co. Retrieved August 20, 2012, from http://dl.acm.org/citation.cfm?id=550585

Gentile, B., Twenge, J. M., Freeman, E. C., & Campbell, W. K. (2012). The effect of social networking websites on positive self-views: An experimental investigation. *Computers in Human Behavior*, *28*(5), 1929–1933. doi:10.1016/j.chb.2012.05.012

Get Safe Online. (2012). Get Safe Online Partners. Retrieved June 20, 2013, from https://www.getsafeonline.org/partners-and-supporters/

Ghernouti-Hélie, S. (2010). A National Strategy for an Effective Cybersecurity Approach and Culture. In *2010 International Conference on Availability, Reliability and Security* (pp. 370–373). Ieee. doi:10.1109/ARES.2010.119

Gordon, S., & Ford, R. (2002). Cyberterrorism? *Computers & Security*, *21*(7), 636–647.

Gorge, M. (2007). Cyberterrorism: hype or reality? *Computer Fraud & Security*, *2007*(2), 9–12.

Government of Canada. (2010a). *Action Plan 2010-2015 for Canada ' s Cyber Security Strategy* (p. 15). Canada: Canada. Retrieved August 20, 2012, from http://www.securitepublique.gc.ca/cnt/rsrcs/pblctns/ctn-pln-cbr-scrt/index-eng.aspx

Government of Canada. (2010b). *Canada 's Cyber Security Strategy*. Canada. Retrieved August 20, 2012, from http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/index-eng.aspx

Grobler, M., Dlamini, Z., Ngobeni, S., & Labuschagne, A. (2011). Towards a cyber security aware rural community. Retrieved May 20, 2013, from http://researchspace.csir.co.za/dspace/handle/10204/5183

Grobler, M., van Vuuren, J., & Leenen, L. (2012). Implementation of a Cyber Security Policy in South Africa: Reflection on Progress and the Way Forward. *ICT Critical Infrastructures and Society, p* 215–225. Retrieved May 20, 2013, from http://link.springer.com/chapter/10.1007/978-3-642-33332-3_20

Healy, D. (1997). Cyberspace and place: The Internet as middle landscape on the electronic frontier. *Internet Culture*, 2–3. Retrieved March 8, 2013, from https://services.exeter.ac.uk/cmit/media/texts/porter1996/healy1997_cyberspace_and_place.pdf

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design science in information systems research. *MIS Quarterly*, *28*(1), 75–105.

Hildreth, S. A. (2001). *CRS Report to Congress : Cyberware* (p. 19). Retrieved from http://heinonlinebackup.com/hol-cgi-bin/get_pdf.cgi?handle=hein.tera/crser0010&section=1

Ho, A. T. (2002). Reinventing Local Governments and the E-Government Initiative A Paradigm Shift of Public Service. *Public Administration Review*, *62*(4), 434–444.

Hochschild, J. (2009). Conducting intensive interviews and elite interviews. In *Workshop on Interdisciplinary Standards for Qualitative Research*. Retrieved February 6, 2013, from http://scholar.harvard.edu/jlhochschild/publications/conducting-intensive-interviews-and-elite-interviews

Hofstee, E. (2006). *Constructing a good dissertation: A practical guide to finishing a master's, MBA or PhD on schedule*. Johannesburg, South Africa: EPE.

Holewa, R. (2004). Strategies for Writing a Conclusion. Retrieved August 20, 2013, from http://leo.stcloudstate.edu/acadwrite/conclude.html

House of Representatives. (2010). *Hackers, Fraudsters and Botnets: Tackling the Problem of Cyber Crime*. Canberra: Commonwealth of Australia. Retrieved February 6, 2013, from https://www.ncjrs.gov/App/Publications/abstract.aspx?ID=253374

Hua, J., & Bapna, S. (2012). The economic impact of cyber terrorism. *The Journal of Strategic Information Systems*, 1–12. doi:10.1016/j.jsis.2012.10.004

Hunton, P. (2011). A rigorous approach to formalising the technical investigation stages of cybercrime and criminality within a UK law enforcement environment. *Digital Investigation*, *7*(3-4), 105–113. doi:10.1016/j.diin.2011.01.002

International Telecommunication Union. (2008). *Global Security Report*. Retrieved February 6, 2013, from http://www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/global_strategic_report.pdf

International Telecommunication Union. (2012). *Measuring the information society*. Geveva Switzerland: International Telecommunication Union. Retrieved February 6, 2013, from http://stile.be/conference/PROGRAMMA website.pdf

Introduction to the new old world of netspionage. (2000). *Computer Fraud & Security*, *2000*(2), 18–19.

ISO/IEC 27000. (2009). *ISO/IEC 27000: Information technology — security techniques — information security management systems — overview and vocabulary* (Vol 2003).

ISO/IEC 27002. (2005). *INTERNATIONAL STANDARD ISO / IEC 27002: Information technology — Security techniques — Code of practice for information security management* (Vol. 2005, p. 128).

ISO/IEC 27032. (2012). *INTERNATIONAL STANDARD ISO / IEC: Information technology — Security techniques — Guidelines for cybersecurity* (Vol. 2012, p. 58).

Jabareen, Y. (2009). Building a conceptual framework: philosophy, definitions, and procedure. *International Journal of Qualitative Methods*, *8*(4), 49–62. Retrieved September 12, 2012, from http://ejournals.library.ualberta.ca/index.php/IJQM/article/viewArticle/6118

Jefferies, P., & Hussian, F. (1998). Using the Internet as a teaching resource. *Education + Training*, *40*(8), 359–365.

Jenik, A. (2009). Cyberwar in Estonia and the Middle East. *Network Security*, *2009*(4), 4–6. doi:10.1016/S1353-4858(09)70037-6

Jones, A. (2008). Industrial espionage in a hi-tech world. *Computer Fraud & Security*, *2008*(1), 7–13.

Kajornboon, A. B. (2005). Using interviews as research instruments. *E-Journal for Research Teachers*, *2*(1).

Kim, C., & Renée, M. (2007). ITIL v3: The use of Resources and Capabilities. Retrieved April 20, 2012, from http://itilblues.wordpress.com/2007/11/20/itil-v3-the-use-of-resources-and-capabilities/

Kim, W., Jeong, O. R., Kim, C., & So, J. (2011). The dark side of the Internet: Attacks, costs and responses. *Information Systems*, *36*(3), 675–705.

Kirstein, P. (1999). Early experiences with the Arpanet and Internet in the United Kingdom. *Annals of the History of Computing, IEEE*, 1–7. Retrieved from http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=759368

Klimburg, A. (2012). National cyber security framework manual. NATO CCD COE Publications.

Kortjan, N., & von Solms, R. (2012). Fostering a cyber security culture: a case of South Africa. In A. Koch & P. A. van Brakel (Eds.), *Proceedings of the 14th Annual Conference on World Wide Web Applications*. Durban: Cape Peninsula University of Technology. Retrieved June 20, 2013, from http://www.zaw3.co.za/index.php/ZA-WWW/2012/paper/view/730

Kovacich, G. L. (2000). Netspionage — The Global Threat to Information, Part I: What is it and Why I Should Care? *Computers & Security*, *19*(4), 326–336. doi:10.1016/S0167-4048(00)04020-7

Kritzinger, E., & von Solms, S. H. (2010). Cyber security for home users: A new way of protection through awareness enforcement. *Computers & Security*, *29*(8), 840–847. doi:10.1016/j.cose.2010.08.001

Krone, T. (2004). *A typology of online child pornography offending*. (T. Makkai, Ed.) (p. 6). Australia: Australian Institute of Criminology.

Labaree, R. (2013). Theoratical Framework -Organizing Your Social Sciences Research Paper. Retrieved June 28, 2013, from http://libguides.usc.edu/content.php?pid=83009&sid=618409

Lehr, W., & McKnight, L. W. (2003). Wireless Internet access: 3G vs. WiFi? *Telecommunications Policy*, *27*(5-6), 351–370. doi:10.1016/S0308-5961(03)00004-1

Leiner, B. M., Cerf, V. G., Clark, D. D., Kahn, R. E., Kleinrock, L., Lynch, D. C., Wolff, S. (2009). A brief history of the internet. *ACM SIGCOMM Computer Communication Review*, *39*(5), 22. doi:10.1145/1629607.1629613

Leurdijk, A. A., Slot, M., Nieuwenhuis, O., Jean, E., & Simon, P. (2012). *Statistical , Ecosystems and Competitiveness Analysis of the Media and Content Industries : The Newspaper Publishing Industry* (p. 127). Spain. doi:10.2791/79486

Li, Q. (2007). New bottle but old wine: A research of cyberbullying in schools. *Computers in Human Behavior*, *23*(5), 281–282.

Lieberman, C., & Carper, T. (2011). *Protecting Cyberspace as a National Asset Act of 2010* (pp. 1–9). Retrieved September 20, 2013, from http://www.centerfornphosting.org/policy/cyberbill_draft060710.pdf

Livingstone, S., & Helsper, E. J. (2007). Taking risks when communicating on the internet: The role of offline social-psychological factors in young people’s vulnerability to online risks. *Information, Communication & Society*, *10*(5), 619–644.

Lu, W., Tavallaee, M., Rammidi, G., & Ghorbani, A. (2009). BotCop: An Online Botnet Traffic Classifier. In *2009 Seventh Annual Communication Networks and Services Research Conference* (pp. 70–77). IEEE. doi:10.1109/CNSR.2009.21

Mansfield-devine, S. (2012). Estonia: what doesn’t kill you makes you stronger. *Network Security*, *2012*(7), 12–20. doi:10.1016/S1353-4858(12)70065-X

Marshall, A. M., & Tompsett, B. C. (2005). Identity theft in an online world. *Computer Law & Security Review*, *21*(2), 128–137.

Marshall, C., & Rossman, G. (2011). *Designing qualitative research* (5th ed.). SAGE Publications.

McDowell, L. (1998). Elites in the City of London: some methodological considerations. *Environment and Planning*, *30*(12), 2133–2146.

Mikecz, R. (2012). Interviewing elites addressing methodological issues. *Qualitative Inquiry*, *18*(6), 482–493.

Miles, M. B. A., & Huberman, M. (1994). *Qualitative data analysis: An Expanded source Book* (p. 338). SAGE.

Mills, M., van de Bunt, G., & de Bruijn, J. (2006). Comparative Research: Persistent Problems and Promising Solutions. *International Sociology*, *21*(5), 619–631. doi:10.1177/0268580906067833

Milne, G. R., Rohm, A. J., & Bahl, S. (2004). Consumers’ protection of online privacy and identity. *Journal of Consumer Affairs*, *38*(2), 217–232.

Mitnick, K. D., & Simon, W. L. (2002). *The Art of Deception: Controlling the Human Element of Security*. Wiley Publishing.

Molander, R. C., Riddile, A., Wilson, P. A., & Williamson, S. (1996). Strategic information warfare: A new face of war. Rand Corporation.

Moore, T. (2010). The economics of cybersecurity: Principles and policy options. *International Journal of Critical Infrastructure Protection*, *3*(3-4), 103–117. doi:10.1016/j.ijcip.2010.10.002

Mullen, P. E., Pathé, M., Purcell, R., & Stuart, G. W. (1999). A study of stalkers. *American Journal of Psychiatry*, *156*, 1244– 1249.

Murithi, T. (2006). Practical peacemaking wisdom from Africa: Reflections on Ubuntu. *The Journal of Pan African Studies*, *1*(4), 25–35. Retrieved September 12, 2012, from http://www.jpanafrican.com/docs/vol1no4/PracticalPeacemakingWisdomFromAfrica_JPASvol1no4.pdf

NICE. (2012). *National Initiative for Cybersecurity Education Strategic Plan* (p. 26). USA. Retrieved April 16, 2013, from http://csrc.nist.gov/nice/documents/nicestratplan/nice-strategic-plan_sep2012.pdf

Nicholson, A., Webber, S., Dyer, S., Patel, T., & Janicke, H. (2012). SCADA security in the light of Cyber-Warfare. *Computers & Security*, *31*(4), 418–436. doi:10.1016/j.cose.2012.02.009

O’Connor, C. (2013). Wal-Mart Vs. Amazon: World’s Biggest E-Commerce Battle Could Boil Down To Vegetables. *Forbes*. Retrieved April 16, 2013, from http://www.forbes.com/sites/clareoconnor/2013/04/23/wal-mart-vs-amazon-worlds-biggest-e-commerce-battle-could-boil-down-to-vegetables/

OECD. (n.d.). The Organisation for Economic Co-operation and Development (OECD). Retrieved June 06, 2013, from http://www.oecd.org/about/

OECD. (2002). *Recommendation of the Council Concerning Guidelines for the Security of Information Systems and Networks - Towards a Culture of Security*. Retrieved

June 06, 2013, from http://acts.oecd.org/Instruments/ShowInstrumentView.aspx?InstrumentID=116&Lang=en&Book=False

Ogilvie, E. (2001). Cyberstalking. *Crime & Justice International*, *17*(50), 9–10.

Ophardt, J. (2010). Cyber Warfare and the Crime of Aggression: The Need for Individual Accountability on Tomorrow's Battlefield. *Duke Law & Technology Review*, *29*(3). Retrieved from http://heinonlinebackup.com/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/dltr2010&section=7

Paget, F. (n.d.). *Financial Fraud and Internet Banking: Threats and Countermeasures*.

Paulsen, C., McDuffie, E., Newhouse, W., & Toth, P. (2012). NICE: Creating a Cybersecurity Workforce and Aware Public. (June), 76–79. Retrieved May 20, 2013, from http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6226542

Peffers, K., Tuunanen, T., Gengler, C., Rossi, M., Hui, w, Virtanen, V., & Bragge, J. (2006). The design science research process: a model for producing and presenting information systems research. In *Proceedings of the first international conference on design science research in information systems and technology* (pp. 83–106). Retrieved May 20, 2013, from http://6a.1b.7aae.static.theplanet.com/sites/default/files/documents/000designscresearchproc_desrist_2006.pdf

Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2008). A Design Science Research Methodology for Information Systems Research. *Journal of Management Information Systems*, *24*(3), 45–78.

PEW Internet. (2012). *Internet activities*. Washington, D.C. Retrieved May 20, 2013, from http://www.pewinternet.org/Static-Pages/Trend-Data/~/media/Infographics/Trend Data/Winter 2012/Online_Activities_all.xls

Pew Research Center. (2011). *How people learn about their local community*. (p. 81). Retrieved May 20, 2013, from http://scholar.google.com/scholar?hl=en&btnG=Search&q=intitle:How+people+learn+about+their+local+community#4

Philips, F., & Morrissey, G. (2004). Cyberstalking and Cyberpredators: A Threat to Safe Sexuality on the Internet. *Convergence: The International Journal of Research into New Media Technologies*, *10*(1), 66–79. doi:10.1177/135485650401000105

Public Safety Canada. (2013). Get Cyber Safe. Retrieved June 26, 2013, from http://www.getcybersafe.gc.ca/cnt/bt/index-eng.aspx

Purcell, K. (2011). *Search and email still top the list of most popular online activities* (p. 15). Washington, D.C. Retrieved May 20, 2013, from http://pewinternet.org/~/media//Files/Reports/2011/PIP_Search-and-Email.pdf

Purcell, K., Rainie, L., Buchanan, J., Friedrich, L., Jacklin, A., & Zickuhr, K. (2012). *How Teens Do Research in the Digital World* (pp. 1–115). Washington, D.C. Retrieved from http://www.pewinternet.org/files/old-media/Files/Reports/2012/PIP_TeacherSurveyReportWithMethodology110112.pdf

Radicati, S. (2012). *Email Statistics Report , 2012-2016* (Vol. 44, p. 4). LONDON. Retrieved May 20, 2013, from http://www.radicati.com/wp/wp-content/uploads/2012/04/Email-Statistics-Report-2012-2016-Executive-Summary.pdf

Rantala, R. R. (2008). *Cybercrime against businesses, 2005* (Vol. 15, p. 20). US.

Riem, A. (2001). Cybercrimes Of The 21st Century. *Computer Fraud & Security*, *2001*(3), 13–15.

Roberts, L. G. (1978). The evolution of packet switching. *Proceedings of the IEEE*, *66*(11), 1307–1313. doi:10.1109/PROC.1978.11141

SA Government Gazette. (2010). *Draft Cybersecurity Policy of South Africa*. *Prevention* (pp. 1–16). Pretoria. Retrieved June 20, 2013, from http://www.pmg.org.za/files/docs/100219cybersecurity.pdf

SA Government Gazette. (2011). Draft National Cybersecurity Policy Framework for South Africa. Retrieved May 20, 2013, from http://www.cyanre.co.za/national-cybersecurity-policy.pdf

Savetz, K. (1994). *Your Internet consultant: The FAQs of life online* (p. 600). Sams Publishing.

Schudel, G., & Wood, B. (2000). Modeling behavior of the cyber-terrorist. RAND National Security Research Division Workshop.

Selwyn, N. (2008). Safe haven for misbehaving? An investigation of online misbehaviour amongst university students. *Science Computer Review*, *26*(4), 446–465.

Smith, K. (2006). Problematizing power relations in elite interviews. *Geoforum*, *37*, 643–653.

Stop.Think.Connect. (2012). Cyber Tours Program. Retrieved June 05, 2013, from http://stopthinkconnect.org/get-involved/homeland-security-campaign/cyber-tours-program

Swartz, M. K. (2009). Cyberbullying: an extension of the schoolyard. *Journal of Pediatric Health Care*, *23*(5), 281–282.

Tansey, O. (2007). Process tracing and elite interviewing: A case for non-probability sampling. *Political Science and Politics*, *40*(4), 765-772.

The White House. (2003). *The National Strategy to Secure Cyberspace*. Washington, D.C. Retrieved July 30, 2013, from http://www.dhs.gov/xlibrary/assets/National_Cyberspace_Strategy.pdf.

The White House. (2009a). Cyberspace Policy Review. Washington, D.C.: The White House.

The White House. (2009b). Remarks by the president on securing our nation's cyber infrastructure. Retrieved February 10, 2013, from http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure

Thomson, K.-L., & von Solms, R. (2005). Information security obedience: a definition. *Computers & Security*, *24*(1), 69–75. doi:10.1016/j.cose.2004.10.005

Thomson, K.-L., von Solms, R., & Louw, L. (2006). Cultivating an organizational information security culture. *Computer Fraud & Security*, *2006*(10), 7–11.

Von Solms, R., & van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, (2013), 1–6. doi:10.1016/j.cose.2013.04.004

Von Solms, R., & von Solms, S. H. (2006). Information Security Governance: A model based on the Direct–Control Cycle. *Computers & SecurityComputers*, *25*(6), 408–412.

Wall, D. S. (2010). The Internet as a Conduit for Criminal Activity. SAGE Publications. Retrieved February 10, 2013, from http://ssrn.com/abstract=740626

Wamala, F. (2011). *ITU National Cybersecurity Strategy Guide*. *Chemistry & …* (p. 122). Geneva, Switzerland. Retrieved October 10, 2013 from http://onlinelibrary.wiley.com/doi/10.1002/cbdv.200490137/abstract

Williams, C. (2011). BlackBerry services collapse. Retrieved February 05, 2013, from http://www.telegraph.co.uk/technology/blackberry/8818094/BlackBerry-services-collapse.html

Wolak, J., Finkelhor, D., & Mitchell, K. (2005). *Child-pornography possessors arrested in internet-related crimes: findings from the National Juvenile Online Victimization Study* (p. 64). Alexandria.

Wolf Pack. (2012). *2012/13 The South African Cyber Threat Barometer* (p. 70). Johannesburg. Retrieved May 12, 2012, from www.wolfpackrisk.com

World Economic Forum. (2012). *Risk and Responsibility in a Hyperconnected World Pathways to Global Cyber Resilience*. Retrieved May 12, 2012, from http://www3.weforum.org/docs/WEF_IT_PathwaysToGlobalCyberResilience_Report_2012.pdf

Yakhlef, A. (2001). Does the Internet compete with or complement branches ?. *International Journal of Retail & Distribution Management, 29*(6), 272–281.

Young, K. (1998). Internet addiction: The emergence of a new clinical disorder. *CyberPsychology & Behavior*, *1*(3), 237–244. Retrieved from http://online.liebertpub.com/doi/abs/10.1089/cpb.1998.1.237

Young, K. (1999). Internet Addiction : Symptoms , Evaluation , And Treatment,. *Innovations in Clinical Practice: A Source Book*, *17*, 19–31. Retrieved March 12, 2013 from http://www.netaddiction.com/articles/symptoms.pdf

Zuckerman, H. (1972). Interviewing an ultra-elite. *The Public Opinion Quarterly*, (36), 159–175.

APPENDIX A1: ZA-WWW PRESENTED AND PUBLISHED

PROCEEDINGS OF THE 14th ANNUAL CONFERENCE ON WORLD WIDE WEB APPLICATIONS

7-9 November 2012
Durban
South Africa

Editors:

A. Koch
P.A. van Brakel

Publisher:

Cape Peninsula University of Technology
PO Box 652
Cape Town
8000

Proceedings published at
http://www.zaw3.co.za

ISBN: 978-0-620-55590-6

TO WHOM IT MAY CONCERN

The full papers were refereed by a double-blind reviewing process according to South Africa's Department of Higher Education and Training (DHET) refereeing standards. Before accepting a paper, authors were to include the corrections as stated by the peer-reviewers. Of the 72 full papers received, 64 were accepted for the Proceedings (acceptance rate: 89%).

Papers were reviewed according to the following criteria:

- Relevancy of the paper to Web-based applications
- Explanation of the research problem & investigative questions
- Quality of the literature analysis
- Appropriateness of the research method(s)
- Adequacy of the evidence (findings) presented in the paper
- Technical (e.g. language editing; reference style).

The following reviewers took part in the process of evaluating the full papers of the 14th Annual Conference on World Wide Web Applications:

Prof RA Botha
Department of Business Informatics
Nelson Mandela Metropolitan University
Port Elizabeth

Mr AA Buitendag
Department of Business Informatics
Tshwane University of Technology
Pretoria

Prof AJ Bytheway
Faculty of Informatics and Design
Cape Peninsula University of Technology
Cape Town

Mr A El-Sobky
Consultant
22 Sebwih El-Masry Street
Nasr City, Cairo

Prof M Herselman
Meraka Institute, CSIR
Pretoria

Mr EL Howe
Institute of Development Management
Swaziland

Dr A Koch
Department of Cooperative Education
Faculty of Business
Cape Peninsula University of Technology
Cape Town

Dr DI Raitt
Editor: The Electronic Library (Emerald)
London

Mr PK Ramdeyal
Department of Information and Communication Technology
Mangosuthu University of Technology
Durban

Prof CW Rensleigh
Department of Information and Knowledge Management
University of Johannesburg
Johannesburg

Prof A Singh
Business School
University of KwaZulu-Natal
Durban

Prof JS van der Walt
Department of Business Informatics
Tshwane University of Technology
Pretoria

Prof D van Greunen
School of ICT
Nelson Mandela Metropolitan University
Port Elizabeth

Further enquiries:

Prof PA van Brakel
Conference Chair: Annual Conference on WWW Applications
Cape Town
+27 21 469 1015 (landline)
+27 82 966 0789 (mobile)

Fostering a cyber-security culture: a case of South Africa

N. Kortjan
Institute for ICT Advancement
Port Elizabeth
South Africa
noluxolo.kortjan@live.nmmu.ac.za

R. von Solms
Institute for ICT Advancement
Port Elizabeth
South Africa
rossouw.vonsolms@nmmu.ac.za

Abstract

Cyberspace has altered the way in which people do things today. It has allowed people from all ends of the globe instant communication and unlimited sharing of information. Conversely, this limitless world – cyberspace – is not without risks. A new spectrum of cyber threats has surfaced contrary to the advantages. In attempting to mitigate these threats, the promotion of cyber security has emerged. As an attempt to address cyber security, countries have drafted policies, awareness campaigns, training programmes, and suchlike. South Africa (SA) envisages in its draft National Cyber Security Policy Framework a cyber-security culture (Department of Communications, 2010). Through this culture, amongst its population, the South African government envisages safer and more secure cyber-citizens. It is argued in this paper that education is core in establishing such a culture. This is done by analyzing what constitutes a cyber security culture. Using SA as the case of a developing country, this paper argues towards a set of guidelines that should assist any developing country in creating a cyber-security culture.

Keywords: South Africa, cyberspace, cyber security culture, cyber security education

1. Introduction

When computers were stand-alone devices, security was seldom an issue (Batteau, 2011). However, as technology has evolved, computers were networked in creating a new world. “This world – cyberspace – is a world that we depend on everyday (White house, 2009)”. Cyberspace has allowed life-changing innovations, and continues to impact lives in a way beyond imagination. One of the major contributions of cyberspace is communication. Cyberspace has allowed people from all ends of the globe instant communication and unlimited sharing of information (Digital Britain, 2009).

Today, nations are becoming more and more reliant on cyberspace to govern properly (Choo, 2011). Similarly, businesses have seen an opportunity to transact online, whilst individuals also benefit personally and professionally (Maignan & Lukas, 1997). Enjoying all these benefits, cyberspace is not without risks, however. New risks have emerged; and new ways to commit old crimes have also developed (Selwyn, 2008). These risks render all users of cyberspace unsafe whilst online. Such risks comprise botnets, identity theft, phishing, malware, cybercrime, social engineering and cyber bullying (Choo, 2011).

Cyber threats are apparent worldwide, including in countries which appear to have low internet usage rates. Although this is the case, the extent to which each country promotes secure online behaviour differs. As a result, countries like the United States (US) and the United Kingdom (UK) have already implemented national policies, strategies, campaigns and other mechanisms, in order to counter the ever-increasing cyber risks (Cabinet Office, 2011; White house, 2009). Whilst developing countries, such as South Africa (SA) and Morocco, still find it cumbersome to develop means to secure cyberspace (Cole, Chetty, LaRosa, Reitta, Schmitt, & Goodman, 2008). Most African countries have not yet even considered drafting such policies and strategies.

Cybercrime is one of the leading threats faced by SA today. This dates back to the year 2010, when SA was seventh in the global cyber crime list (Dennis, 2010). This increase in crime has resulted from the 2010 Soccer World Cup event, which was held in SA (Dennis, 2010). Since 2010, SA persistently ranks high in cybercrime to date (Deloitte, 2012). In addition, the recent increase of bandwidth has also contributed to the increase in cybercrime. However, cyber security efforts have not strengthened in step with cyberspace reliance.

1.1. Research problem and objectives

South Africa is still to publish its final National Cyber Security Policy Framework. Envisaged in this policy is a cyber-security culture (Department of Communications, 2010). The problem addressed in this paper is the apparent lack of emphasis that SA has on cyber-security education. Thus, the objective of this paper is to prove that education is core in establishing such a culture, as envisaged in the draft National Cyber Security Policy Framework, amongst South African cyber citizens.

1.2. Methodology

The paper will be using the following research methods. Firstly, extensive literature studies was conducted, according to Hofstee (2006), to attain insight on what a cyber-security culture should entail, and also to identify what is critical to such a culture. Secondly, evidential and interpretive argumentation techniques as discussed by Masson (1996) was used to demonstrate that SA can learn valuable lessons from its highly successful Human Immunodeficiency Virus (HIV) awareness campaigns. As a result this paper aims to provide guidelines for developing a successful cyber security awareness and education campaign, based on a critical analysis performed on an existing HIV awareness campaign. This research method is used to abstract a subjective interpretation on the HIV campaign, so as to extrapolate key principles that can be identified in this campaign.

The paper structure is as follows. In the second section, the literature on a cyber security culture is provided. In the third section, an assessment on HIV awareness and education is presented as an analogy to the topic at hand. In the forth section, a contrast of HIV and cyber security is provided and the proposed guidelines are presented, followed by some concluding remarks.

2. Cyber security culture

“Cyber security needs the development of a cyber-culture and acceptable user behaviour in the new reality of cyberspace, but it is also based on norms of correct behaviour and the capacity to pursue wrong-doers and bring them to justice, albeit in the online world (International Telecommunication Union, 2008)”. The growing dependency on cyberspace and other digital resources has introduced its own set of security issues. Consequently, this dependence has added cyber security to the nation’s list of security concerns (Choo, 2011).

Realising this, SA over a period of two years has been fine tuning its national cyber security strategy. Concerning the awareness and education domain, SA is aiming at fostering a cyber security culture. However, this policy fails to expand on how it intends to promote this culture (Department of Communications, 2010). This section will attempt to elaborate on what should constitute a cyber-security culture.

2.1. What constitutes a cyber security culture?

The International Telecommunications Union (ITU) defines the creation of a cyber security culture as the “best guarantee” for cyber security (International Telecommunication Union, 2008). Moreover, according to Ghernouti-Helie (2010) one of the pillars of such a culture is awareness and education. This pillar is also perceptible in the guidelines provided by the UN General Assembly Resolution 57/239 on the Creation of a Global Culture of Cyber Security, and the OECD’s Guidelines for the Security of Information Systems and Networks. These guidelines have a number of aims which depict what a cyber security culture should encompass. These aims are as follows (Organisation for Economic Co-Operation and Development, 2002):

- Promoting a secure digital environment amongst all users of cyberspace;
- Raising awareness about the risks that are apparent online, and also the counter measures to these risks;
- Increasing the confidence of all users in information systems and networks, and the way in which they are provided and used;
- Serving as a general frame-of-reference for the development and implementation of cyber security measures;
- Promoting co-operation and information sharing, as appropriate, amongst all the participants in the development and implementation of security policies, practices, measures and procedures.
- Promoting the consideration of security as an important objective amongst all participants involved in the development or implementation of standards.

With the aims defined above, one should be able to use these guidelines as an outline for fostering a cyber-security culture. These guidelines reflect the aforementioned aims (Organisation for Economic Co-Operation and Development, 2002). The guidelines are listed and explained below; and they refer to all users of cyberspace as “participants”. These include governments, businesses, other organizations and individual users:

(1) *Awareness.* Participants should be well informed about the necessity of cyber security and the steps they can take to promote security;

(2) *Responsibility*. All participants should assume responsibility for the security information systems and networks. Hence cyber security is a shared responsibility amongst all the participants;
(3) *Response*. There has to be a central point for information sharing for participants, to facilitate appropriate and joint prevention, detection and response to security incidents.
(4) *Ethics*. Participants need to be respectful towards one another and also to act in a manner that is appropriate.
(5) *Democracy*. Security measures should be implemented in such a way that the rights of participants are not infringed.
(6) *Risk assessment*. All participants should conduct periodic risk assessments that identify threats and vulnerabilities; they should be sufficiently broad-based to encompass key internal and external factors, such as technology, physical and human factors, policies and third-party services with security implications; allow determination of the acceptable level of risk; and assist in the selection of appropriate controls to manage the risk of potential harm to information systems and networks in the light of the nature and importance of the information to be protected.
(7) *Security design and implementation*. Participants should incorporate security as an essential element in the planning and design, operation and use of information systems and networks.
(8) *Security management*. Participants should adopt a comprehensive approach to security management based on risk assessment that is dynamic, encompassing all levels of participants' activities and all aspects of their operations.
(9) *Reassessment*. Participants should review and reassess the security of information systems and networks and should make appropriate modifications to security policies, practices, measures and procedures that include addressing new and changing threats and vulnerabilities.

It is important to note that '*awareness*' is the first guideline, implying that in fostering a cyber-security culture, one has to firstly realise that need for security; and secondly, one needs to be informed on how to apply the needed security. Educating the users of cyberspace is a proactive effort, and one that has great benefit.

In addition to the above mentioned guidelines, ITU has compiled eight definite steps that should be taken in order to promote a cyber security culture. These steps are listed below (International Telecommunication Union, 2008):

(1) Implement a cyber security plan for government-operated systems.
(2) Security awareness programs and initiatives for users of systems and networks.
(3) Encourage the development of a culture of security in firms.
(4) Support outreach to civil society.
(5) Promote a comprehensive national awareness programme.
(6) Enhance Science and Technology (S&T) and Research and Development (R&D) activities.
(7) Review existing privacy regime and update it to the online environment.
(8) Develop awareness of cyber-threats and available solutions.

Considering the guidelines and the above-mentioned steps it becomes clear that education and awareness are elements underpinning cyber security as a whole. However, "*awareness-raising and the availability of resources are cross-cutting issues that need to be dealt with separately* (International Telecommunication Union, 2008)". It is clear in the aforementioned guidelines and steps presented by ITU, that awareness and education both play a vital role in cyber security as a whole. They play an even more vital role in the harnessing of a cyber security culture. Therefore, for SA to succeed in its attempts in promoting this culture, it should have a rather steady, well-defined educational plan. Most importantly, the government must take charge and lead this venture. In addition, every user of cyberspace has a duty; but this responsibility can only be appreciated when the users are well informed, through effective education and awareness campaigns.

SA has had extensive and expensive campaigns on HIV, and could surely learn from these. The following section will provide an analysis of the HIV awareness campaign.

3. The HIV analogy

HIV is an epidemic that in its course requires human behaviour and attitudes to change. Apprehending this, the change in human behaviour and attitude has been pursued by a number of awareness campaigns, aimed at shifting how the society relates to HIV, and how our society perceives HIV (Kylie, 2004). Although everyone is targeted in the campaigns, different programmes are tailor-made to reach certain audiences. One of SA's leading awareness campaigns is loveLife (SANAC, 2011).

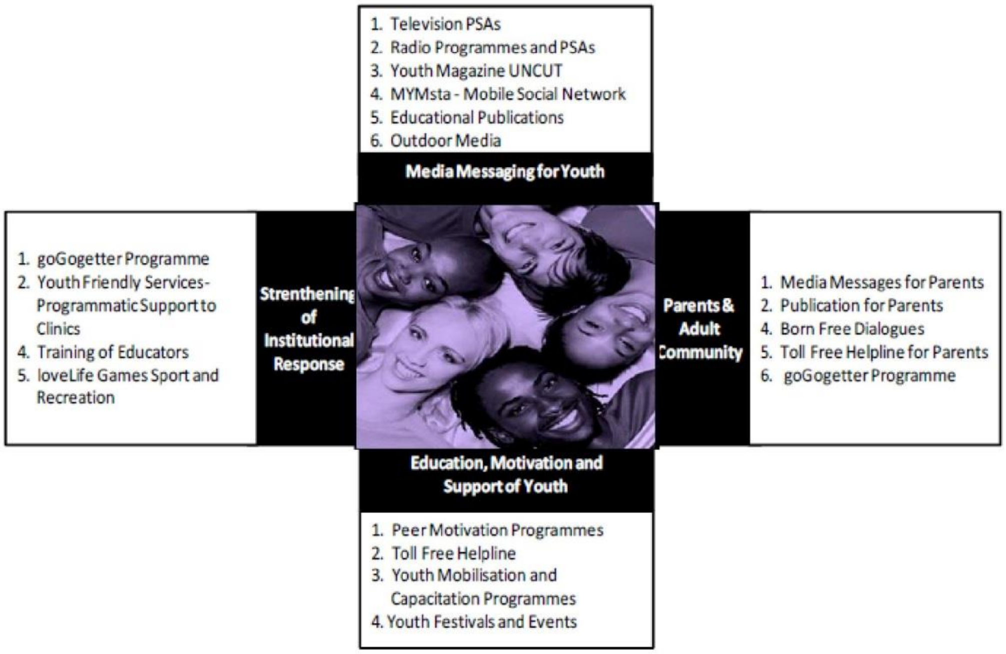
LoveLife is a comprehensive HIV campaign with the focus on South African youth (Love Life, 2008). This non-governmental campaign was launched in 1999. It is, however, funded by the SA government with the support of the SA private sector. This campaign aims "*to substantially reduce the rate of new infection in young people, in order to help reduce the overall prevalence of HIV in South Africa (*Love Life, 2008)".

The way in which loveLife is constructed is based on its four objectives, which are (Love Life, 2008):

- Getting South African citizens to talk about HIV and the basic dynamics of sexuality;
- Inspiring the youth of SA, to possess a sense of purpose, belonging and identity within an HIV-free future;
- Making the youth of SA aware of the risk of HIV, to also understand this risk, to be able to decide against the risk, along with equipping them with the necessary proficiency to avoid the risk;
- Implanting loveLife's communication in institutional responses to young people – including youth development and leadership, educational and sports development, and access to appropriate health services.

A number of key messages are crucial to loveLife. One of these messages is that HIV is the responsibility of everyone living. Moreover, everyone is, in fact, affected by the virus, regardless of whether or not one is infected. How loveLife reaches the public is illustrated in Figure 1 below.

Figure 1: LoveLife Contact-points with South African Young People (Love Life, 2008)


1. Television PSAs
2. Radio Programmes and PSAs
3. Youth Magazine UNCUT
4. MYMsta - Mobile Social Network
5. Educational Publications
6. Outdoor Media
Media Messaging for Youth
1. goGogetter Programme
2. Youth Friendly Services-Programmatic Support to Clinics
4. Training of Educators
5. loveLife Games Sport and Recreation
Strenthening of Institutional Response
Parents & Adult Community
1. Media Messages for Parents
2. Publication for Parents
4. Born Free Dialogues
5. Toll Free Helpline for Parents
6. goGogetter Programme
Education, Motivation and Support of Youth
1. Peer Motivation Programmes
2. Toll Free Helpline
3. Youth Mobilisation and Capacitation Programmes
4. Youth Festivals and Events

The above diagram also illustrates the key-elements of the loveLife HIV prevention campaign, together with all the programmes included in the campaign. This is described in more detail below:

(1) A countrywide community-level HIV prevention peer education and youth mobilization programme led by a national corps of 18 to 25 year olds, known as LoveLife groundBREAKER (gB) and volunteer peer motivators ('Mpintshis') recruited annually for one year.

(2) A comprehensive youth leadership development programme: The gB's programme provides approximately 1 200 young people a year with the opportunity for personal and skills development through extensive training courses.

(3) Youth Friendly Services training for public clinic staff as well as provision of educational training and management resources.

(4) Two nationally accessible toll free HIV/Aids telephone help lines for young people and parents providing specialized sexual health information, HIV prevention counselling and referrals.

(5) A national network of loveLife hubs where peer educators are based, including youth centres, franchises, youth friendly public clinics and outlets. The Y-Centres provide comprehensive HIV prevention education as well as recreational and skills training programmes for youth.

(6) The LoveLife Games, the largest school sports competition in South Africa, promoting HIV prevention through healthy living, self-motivation and personal achievement to school students annually.

(7) A sustained multi-media HIV and Aids education and awareness campaign including television, radio, outdoor media and print - educating young people about HIV; promoting dialogue about sexual health issues, and pointing them to the help lines and other face-to-face services.
(8) The development of a new generation of young leaders is essential to loveLife and this goal is achieved through our gB and Mpintshi programs.

There are various principles that can be abstracted from loveLife. The most crucial point to note is that loveLife is aimed at changing human behaviour and perception of the risk. With that said, if one is to look at what loveLife is doing to achieve the intended change, the following may be deduced:

- Making everyone aware of the existence of the risk
- Making everyone understand the nature of the risk
- Making everyone assume responsibility for the risk
- Educating everyone regarding ways to detect, prevent and live with the risk
- Strategically choosing one's target audience
- Identifying key messages to communicate
- Creating unique programmes to portray particular messages
- Identifying all possible mediums available to communicate the message
- Identifying which medium is best suited for a particular message and target audience
- Coordinating training programmes
- Holding awareness events with particular themes
- Publishing information through various channels.

These are the principles that have contributed to the success of the loveLife campaign. Moreover, these principles could serve as a blueprint in creating a successful cyber security awareness campaign for SA. The following is a map of the adapted principles to cyber security education. In addition, the proposed guidelines will be introduced.

4. Cyber security awareness campaign guidelines

The sceneries of HIV and cyber security are similar in many ways. This section expands on the similarity between these concepts – by providing the similar elements. This section, furthermore, introduces the proposed guidelines that should add value to establishing a cyber security awareness campaign – a campaign that could contribute to promoting a culture of cyber security.

Similar to HIV, cyber risks are threats that need to be addressed from a national point of view. Cyber risks require a strengthened cyber security strategy that includes awareness and education (Ghernouti-Helei, 2010). If one is to use the HIV analogy and consider the nature of the awareness campaigns held for the purpose, the key messages displayed in this analogy also apply in cyber security. For example, "prevention is better than cure" holds in the case cyber security because it is better to prevent cyber ills than to remedy them. This includes the fact that HIV is the responsibility of all citizens (SANAC, 2011); it is just so, even in cyber security, because cyber security is the responsibility of all cyber citizens (Stay Safe Online, 2012). This expands to the notion that everyone is affected by

HIV, regardless of whether or not one is infected (Love Life, 2008); this also applies to cyber security, as all cyber citizens are affected directly or indirectly.

It is also pivotal to note that the nature of a cyber security awareness campaign, similar to that of HIV, has the ultimate goal of altering human behaviour and perceptions. For that reason, it is fitting to use the key principles defined as a blue print when creating a cyber security awareness campaign. The proposed guidelines are as follows:

(1) Make everyone aware of the existence of the cyber risks
(2) Make everyone understand the nature of these risks
(3) Making everyone assume responsibility to play his/her part in the solution
(4) Educate everyone regarding ways to detect, prevent and respond to cyber risks
(5) Strategically choose target audiences to address
(6) Identify key cyber security messages to communicate
(7) Create unique programmes to convey particular messages
(8) Identify all possible mediums available to communicate the message
(9) Identify which medium is best suited for a particular message and target audience
(10) Coordinate training programs
(11) Hold awareness events with particular themes
(12) Publish information through various channels.

Applying these guidelines would enable SA, and any developing country, to co-ordinate a comprehensive awareness campaign that would reach users of cyberspace and change the way they relate to cyber security. It would furthermore draw the attention of those users who were not previously aware of how vulnerable they are online. The following are concluding remarks.

5. Conclusion

While we grow more reliant on cyberspace, more cyber threats surface. These cyber threats have an adverse effect on all the users of cyberspace. As a result, there is a great need for an effective cyber security campaign. Governments have attempted to promote a cyberspace that is resilient to crime, or any misbehaviour. Furthermore, to produce a nation that is well informed of the risks apparent online; thus, a nation that is educated on how to detect, prevent and respond to cyber risks. Security has become a pivotal consideration to every nation in this mordent day and promoting a cyber security culture is SA's ultimate weapon in preparing its citizens.

Critical to fostering a cyber-security culture are awareness and education. Therefore, a comprehensive awareness campaign would contribute to such a culture. Using the loveLife campaign as an analogy to abstract the key principle of a successful awareness campaign could assist SA in its endeavour. Thus, the proposed guidelines are to contribute towards co-ordinating a cyber security awareness campaign that could change the behaviour of South Africans towards a cyber secure culture. These guidelines are only part of the solution; however, they are a significant part thereof.

6. References

Batteau, A.W. 2011. Creating a Culture of Enterprise Cybersecurity. *International Journal of Business Anthropology*, pp.36 - 47.

Cabinet Office. 2011. [Online] Available at: http://www.cabinetoffice.gov.uk/news/protecting-and-promoting-uk-digital-world. [Accessed 4 September 2012]

Choo, K.K.R. 2011. The cyber threat landscape: Challenges and future. *Computers & Security*, pp.719 -731.

Cole, K. et al. 2008. [Online] Sam Nunn School of International Affairs Available at: http://www.cistp.gatech.edu/publications/files/AnAssessmentofAfricanCybersecurity.pdf [Accessed 1 August 2012].

Deloitte. 2012. *World Economic Forum*. [Online] Available at: http://www3.weforum.org/docs/WEF_IT_PathwaysToGlobalCyberResilience_Report_2012.pdf [Accessed 4 September 2012].

Dennis, J. 2010. *SA seventh in global crime list*. [Online] Available at: http://www.timeslive.co.za/local/article423649/SA-seventh-in-global-cyber-crime-list [Accessed 4 September 2012].

Department of Communications. 2010. [Online] Available at: http://d2zmx6mlqh7g3a.cloudfront.net/cdn/farfuture/mtime:1266829764/files/docs/100219cybersecurity.pdf. [Accessed 4 September 2012]

Digital Britain. 2009. [Online] Available at: http://webarchive.nationalarchives.gov.uk/+/http://www.culture.gov.uk/images/publications/digital_britain_interimreportjan09.pdf. [Accessed 4 September 2012]

Ghernouti-Helei, S. 2010. A national strategy for an effective cybersecurity approach and culture. In *International Conference on Availability, Reliability and Security.*, 2010. IEEE Computer Society.

Hofstee, E. 2006. *Constructing a good dissertation*. EPE.
International Telecommunication Union, 2008. *ITU*. [Online] Available at: http://www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/global_strategic_report.pdf [Accessed 2 September 2012].

Kylie, T. 2004. A Better Life for Some: The Lovelife Campaign and HIV/AIDS in South Africa. *Agenda*, pp.29-35.

Love Life. 2008. *Fact Sheets*. [Online] Available at: http://www.lovelife.org.za/corporate/files/8613/3848/3246/Annual_Report_2008.pdf [Accessed 8 September 2012].

Maignan, I. & Lukas, B.A. 1997. The Nature and Uses of the Internet: A qualitative Investigation. *Journal of Consumer Affairs*, 31(2), pp.346-71.

Mason, J. 1996. *Qualitative researching*. SAGE Publications.

Obama, B. 2009. *The White House*. [Online] Available at: http://www.whitehouse.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure [Accessed 5 September 2012].

Organisation for Economic Co-Operation and Development, 2002. *Decisions, Recommendations and other Instruments of the OECD*. [Online] Available at: http://acts.oecd.org/Instruments/ShowInstrumentView.aspx?InstrumentID=116&Lang=en&Book=False [Accessed 2 September 2012].

SANAC. 2011. *Resources*. [Online] Available at: http://www.sanac.org.za/files/uploaded/World%20AIDS%20Day%202011%20Messaging%20Booklet.pdf [Accessed 5 September 2012].

Selwyn, N. 2008. A Safe Haven for Misbehaving?An Investigation of Online Misbehavior Among University Students. *Social Science Computer Review*, 26(4), pp.446-65.

Stay Safe Online. 2012. *National Cyber Security Month*. [Online] Available at: http://www.staysafeonline.org/ncsam/about [Accessed 1 September 2012].

Whine, M. 2001. Cyberspace-A New Medium for Communication, Command, and Control by Extremists. *Studies in Conflict & Terrorism*, pp.231-45.

Acknowledgements

The financial assistance of the following institutions towards this research is hereby acknowledged:

- National Research Foundation (NRF)
- Vodacom/NMMU scholarship.

Opinions expressed and conclusions arrived at are those of the authors and not necessarily to be attributed to these sponsors.

APPENDIX A2: AFRICOMM PRESENTED AND PUBLISHED

Cyber Security Education in Developing Countries: A South African Perspective

Noluxolo Kortjan, Rossouw von Solms

PO Box 77000, Nelson Mandela Metropolitan University, Port Elizabeth
6031, South Africa

{Noluxolo.Kortjan,Rossouw.VonSolms}@nmmu.ac.za

Abstract. Cyberspace has become significant to the wellbeing of the individuals, organisations and general economy of a country. It is for this reason that a country should play a leading role in securing cyberspace. However, in the face of the inherent challenges, the awareness of and education on cyber security cannot be overlooked. This paper aims to determine the current situation regarding cyber security in South Africa (SA) as a case of developing countries, specifically from an awareness and educational point of view. This will be achieved by providing a comparative analysis between two well-advanced countries and South Africa in order to abstract key points from a policy and policy implementation point of view to the actual execution of cyber security education initiatives. From the identified key points, some aspects are highlighted that a developing country should perhaps consider in engineering its cyber security education plan.

Keywords: cyberspace; cyber security; cyber security education

1 Introduction

In modern technology, the internet has become one of the most significant inventions to date [1]. Over the years the internet has developed immensely, providing billions of individuals and enterprises across the globe with digital communication [2]. In the modern way of doing business, enterprises use the internet to meet their aims and to enable business processes [1]. Over and above its communication value, people use the internet for financial and entertainment purposes [3]. As a result, large numbers of enterprises and individuals have become dependent on the technology.

Although the internet offers numerous advantages, it is constantly threatened by many risks. These risks can have serious adverse effects on both enterprises and individuals making use of the internet. One of these risks is online crime [4]. The internet has given criminals a platform on which to grow and proliferate [5]; further, it is easy for criminals to go unpunished because of the abstract nature of the internet and the difficulty involved in tracing the origins of such crime [1]. Core to criminal activities on the internet is the exploitation of personal and corporate information [6]. As a result, every person or enterprise using the internet is at risk of having such information compromised.

Not only has the internet become critical to the wellbeing of many people and organisations; but it has also become part of several components that are critical to the wellbeing of national economies and society at large [7]. Accordingly, in light of the increasing adoption of the internet, developing countries and Africa, in particular, lack general safety and security measures in terms of this resource. This is due in part to a number of unique factors. However, with the continuous rise in the adoption of the internet measures should be put in place to address the security risks.

Many developed countries, such as the United States of America (USA) and the United Kingdom (UK), have developed and implemented cyber security protocols, standards and implementations for internet security and policing. Education in this regard is critical to cyber security implementation. Realising this, these countries have taken the initiative in educating society at large, including enterprises, on the threats related to the internet and to cyberspace. This includes how to recognise and avoid the threats, as well as how to recover from them.

In contrast with developed countries, many developing countries do not, as yet, have comprehensive cyber security initiatives in place [8]. These countries include Egypt, Libya and Morocco in the northern region of Africa. In addition, in other parts of Africa, such as Central Africa, the concept of cyber security is still vague [8].

Using South Africa as a case, this paper aims to explore the current situation as it pertains to cyber security education in developing countries. It furthermore aims to identify criteria that should be considered when creating a comprehensive cyber security educational plan for a typical developing country. These criteria are an attempt to contribute to education on cyberspace security in developing countries and underline the role education plays in it. This will be achieved by conducting a comparative analysis between South Africa and two advanced countries in terms of cyber security, namely, the UK and the USA.

2 A snapshot of the United Kingdom's and United States of America's efforts regarding cyber security

The UK and the USA have taken definitive steps towards securing cyberspace. These entail a complete suite of aspects that need to be addressed and implemented, including drafting policies and implementing cyber security protocols. This section will assess what is currently in place concerning cyber security education. The cyber security efforts of these two countries are studied merely because a great deal of relevant information is available in this regard.

2.1 Cyber security education in the United Kingdom

Six and a half million pounds has been has been allocated by the UK government to educate UK citizens on cyber security awareness [9]. An education scheme "Get Safe Online" has been developed to assist organisations and the general population with cyber-related issues [10]. This scheme provides advice on cyber threats and ways in which to recognise and recover from the threats. "Get Safe Online" provides cyber safety tips for teachers, parents and young people. Moreover, its knowledge base comprises information on protecting both individuals and businesses. The UK intends to expand the scope of the scheme to include more innovative ways of disseminating cyber security education. The UK has also launched the Cyber Security Challenge which aims to groom young cyber specialists to fill the skills gap in IT security [11].

Therefore, it would seem that, from a UK perspective, objectives have been set for cyber security education, funds have been set aside, and well-planned, coordinated activities are taking place to educate all levels of cyber users.

2.2 Cyber security education in the United States of America

The USA has formed the National Initiative for Cyber Security Education (NICE) [12]. The NICE initiative aims to improve the cyber behaviour, skills, and knowledge of the US population, enabling a safer cyberspace. One of the major goals of NICE is "to strengthen the future cyber security environment by expanding cyber education; coordinating and redirecting research and development efforts across the Federal Government; and working to define and develop strategies to deter hostile or malicious activity in cyberspace" [12].

This initiative is currently active and has awareness campaigns that include the "Stop.Think.Connect" online educational scheme [13]. This scheme underpins the notion that cyber security is the responsibility of everyone who benefits from using cyberspace. Therefore, everyone should take a moment to **stop** and **think** carefully about the risks associated with using cyberspace. Once the risks are considered one can make an informative choice and continue to **connect** and enjoy cyberspace [13]. "Stop.Think.Connect" has also spawned another online education scheme "OnGuardOnline.gov" with a similar intention. Moreover, the USA holds a National Cyber Security Awareness month in October every year, which is intended to remind American citizens that cyber security is a shared responsibility [14].

The NICE cyber security workforce structure consists of the US Federal workforce, the government and the private sector. In addition, the US Department of Homeland Security has formed partnerships with the private and public sector in its quest to mitigate cybercrime against critical infrastructure [12]. The USA also has a Computer Emergency Response Team (CERT) aimed at improving the nation's cyber security.

The CERT serves as a point of contact for the US nation to share and communicate directly with the US government about cyber-related threats and incidents [15].

The UK and the USA have positioned cyber security alongside other governmental priorities, consequently taking the initiative in securing cyberspace. Steps have been taken to develop policy and strategy in this regard, as well as with regard to the educational facet of cyber security. However, cybercrime is still an issue and there are calls for more innovative ways to secure cyberspace. Therefore, constantly improving cyber security protocols should also be a concern. The following section will explore cyber security from a South African perspective.

3 South Africa's efforts towards cyber security

Cyber security issues are not unique to the UK and the USA. As South Africa becomes ever more reliant on cyberspace to govern and to conduct business, it is increasingly being affected by threatening cyber issues [16]. As with the previous section, this section will provide a brief summary of the key points addressed in South Africa's Draft National Cyber Security Policy Framework. It will evaluate the vision of this policy together with that way in which its objectives are to be achieved. Further, it will assess what is currently implemented in South Africa in terms of cyber security education.

3.1 South African cyber security policies and strategies

In the year 2010, the South African government released a draft cyber security policy [17]. This draft policy implied that South Africa is not currently in a position to deal effectively with cyber-related threats. In addition, the draft stated that South Africa lags behind other countries in the development of cyber security protocols and standards, as well as in the implementation of such protocols and standards. The objectives of this policy document include developing structures that would be capable of adequately supporting cyber security, as well as establishing and promoting a cyber security culture, and encouraging compliance with certain security standards. However, this policy remained stagnant for a period of two years.

This draft has, nevertheless, led the way to the recently published National Cyber Security Policy Framework. Articulated in this policy is the intent to secure cyberspace and to ensure that the protection of South Africa's national critical information infrastructure is not hindered. This policy aims to create a knowledgeable society that understands cyber-related threats. Moreover, it intends to provide a cyber security approach that is holistic and, in doing so, it requires the support of all role-players. These role-players include the state, the public and private sector and society at large [17]. This policy addresses the following:

- developing and implementing an integrated approach to cyber security that will be led by the government
- creating a Cyber Security Response Committee dedicated solely to coordinating cyber security measures
- synchronising effective departmental resources in order to ensure uniform cyber security goals
- promoting partnerships with all role-players in cyber security
- creating an environment that has well-coordinated approaches, plans, manpower and infrastructure
- strengthening the legal sphere to incorporate cyber crime prevention
- promoting a cyber security culture that subscribes to minimum cyber security measures
- establishing a comprehensive framework to govern cyberspace
- establishing a partnership with public and private entities to coordinate action plans that correspond with the intents of this policy.

Currently, South Africa merely has a vision; as yet there have been no concrete developments.

3.2 Cyber security education in South Africa

The policy at hand says little regarding cyber security education. This is only “hinted” at in terms of the idea of promoting a cyber security culture; a culture that is not elaborated on in detail.

Further, the policy fails to provide a clear vision on how South Africa plans to implement the objectives expressed and no resources have been set aside to fund their implementation. Seemingly, apart from the Electronic Communications and Transactions (ECT) Act, the Draft Cyber Security Policy and the recently published National Cyber Security Policy Framework, South Africa is still in the infancy stages of preparing to secure cyberspace. Moreover, there are no known cyber security awareness initiatives, as would seem to be the case in a number of developing countries. As education plays a core part in introducing any cyber security-related policy or strategy, the next section will propose some aspects that need to be addressed in this regard.

4 Bridging the gap between South Africa and its counterparts in the United Kingdom and the United States of America

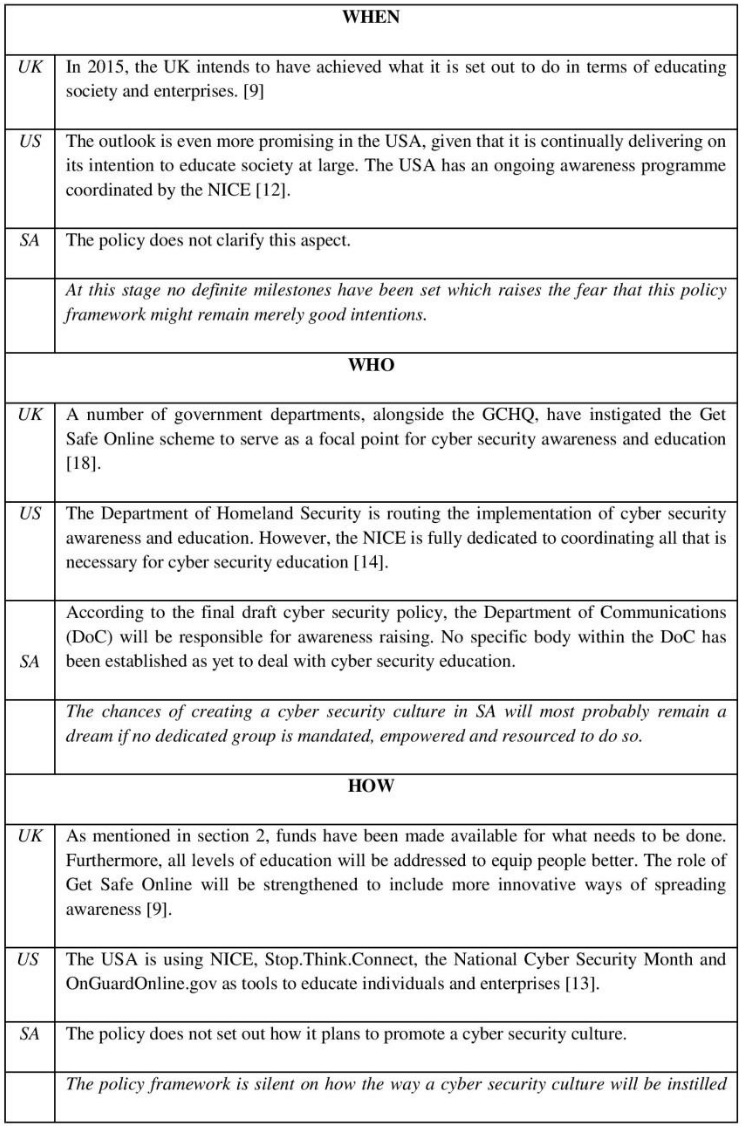
Cyber security has become a burning issue worldwide. In the attempt to mitigate this issue, education has been identified as an important tool. As mentioned in the previous section, the UK and the USA have taken definitive steps in implementing cyber security education. However, South Africa is still in the preparation stage in this regard. This section provides a brief summary of what is envisioned and has been implemented in the UK, the USA and South Africa. This summary is intended to highlight what is "missing" from South Africa's national cyber security policy as regards education, and proposes some aspects that South Africa should consider when engineering its cyber security education plan.

4.1 What has been said and done in the United Kingdom, the United States of America and South Africa

It is important to note that the UK and the USA are improving initiatives that are already in place, while South Africa is still struggling to lay the foundations of cyber security education. This point is expanded on in the summary in Table 1. The information provided in Table 1 is grouped according to four categories. Firstly, **what** each country wants to achieve in terms of cyber security education, namely, its **objective**. Secondly, **when** is the **outcome** pertaining to the objective expected? Thirdly, **who** is **responsible** for certain tasks? Lastly, **the way in which** each country plans to achieve the expected outcome is stated.

Table 1: Cyber security education overview of the United Kingdom, the United States of America and South Africa

WHAT	
UK	Concerning cyber security education, the UK wants to create a knowledgeable society and commercial world that is able to protect itself from cyber-related threats [9].
US	The USA is also working towards educating the general public on cyber-related threats [12].
SA	SA, on the other hand, is set on creating a cyber security culture [17]. As mentioned in the previous section, the policy does not go into detail on what this "culture" entails.
	SA has indeed embarked on securing cyberspace; albeit, years after other countries and therefore with a very big deficit.



	WHEN
UK	In 2015, the UK intends to have achieved what it is set out to do in terms of educating society and enterprises. [9]
US	The outlook is even more promising in the USA, given that it is continually delivering on its intention to educate society at large. The USA has an ongoing awareness programme coordinated by the NICE [12].
SA	The policy does not clarify this aspect.
	At this stage no definite milestones have been set which raises the fear that this policy framework might remain merely good intentions.
	WHO
UK	A number of government departments, alongside the GCHQ, have instigated the Get Safe Online scheme to serve as a focal point for cyber security awareness and education [18].
US	The Department of Homeland Security is routing the implementation of cyber security awareness and education. However, the NICE is fully dedicated to coordinating all that is necessary for cyber security education [14].
SA	According to the final draft cyber security policy, the Department of Communications (DoC) will be responsible for awareness raising. No specific body within the DoC has been established as yet to deal with cyber security education.
	The chances of creating a cyber security culture in SA will most probably remain a dream if no dedicated group is mandated, empowered and resourced to do so.
	HOW
UK	As mentioned in section 2, funds have been made available for what needs to be done. Furthermore, all levels of education will be addressed to equip people better. The role of Get Safe Online will be strengthened to include more innovative ways of spreading awareness [9].
US	The USA is using NICE, Stop.Think.Connect, the National Cyber Security Month and OnGuardOnline.gov as tools to educate individuals and enterprises [13].
SA	The policy does not set out how it plans to promote a cyber security culture.
	The policy framework is silent on how the way a cyber security culture will be instilled

	as well as the target audience that is to be made aware and educated in this regard.

4.2 Bridging the gap

After comparing the criteria from these countries, one can clearly identify the areas in which South Africa lags behind. Using South Africa as a typical example of a developing country, the objective is to address the shortfalls from an awareness and educational point of view. In doing so, we list some of the aspects that should be considered by developing countries in this regard:

- setting an undisputable objective
- identifying definite milestone dates
- creating, empowering and resourcing a responsible group
- defining a reasonable action plan
- allocating resources

It would be a good start for developing countries to have clear-cut **goals** for cyber security education. This would make it easy for such a country to rate its performance in this regard [19]; in addition, it essential that performance be monitored against **targets**. Accordingly, once South Africa knows exactly what it wants to achieve and when, it will be easier to benchmark its progress. As vital as this is, identifying who is responsible for what is just as important. Merely assigning responsibility for awareness and education to the Department of Communication is not enough; if a definite grouping **is made responsible** for awareness and education, delivery will be assured.

It is all very well to abstract that which the UK and the USA have in place; however, it is crucial to be aware that these countries are different to Africa. The difference lies in how technologically advanced the UK and the USA are. Having considered that, the responsible party could coordinate a tailor-made **action plan** that would be suitable for a developing country. Finally, resource allocation is crucial; for example allocating a budget will play a major role in tying the all the aspects together.

Table 1 summarised the areas in which South Africa lags behind in cyber security. In mitigation, some suggestions have been made to ensure that South Africa does indeed embark effectively on the road to "create a cyber security culture" in SA.

5 Conclusion

The reliance on cyberspace to live, to conduct commerce and to govern has placed cyber security alongside other global concerns. Hence, cyber security education should be viewed in the same important light. The UK and the USA are well on their way to educating their citizens to behave in a safe, secure manner when connected to cyberspace. Such safe and secure behaviour will be beneficial to the individual, businesses and, eventually, for the entire country. By contrast, developing countries are barely armed, owing to a number of unique factors. However, as there is a continuous rise in the adoption of the internet globally, every country should be preparing to create a secure virtual environment. With the evidence and arguments that have been provided, one can ask and answer the questions posed below:

1. Are the enterprises and individuals in developing countries as dependent on the internet as their US and UK counterparts?

   Developing countries are becoming increasingly as dependant on the internet, particularly in the areas of governance and economics.

2. Are developing countries equally prepared to educate enterprises and individuals on how to protect themselves in cyberspace?

   No.

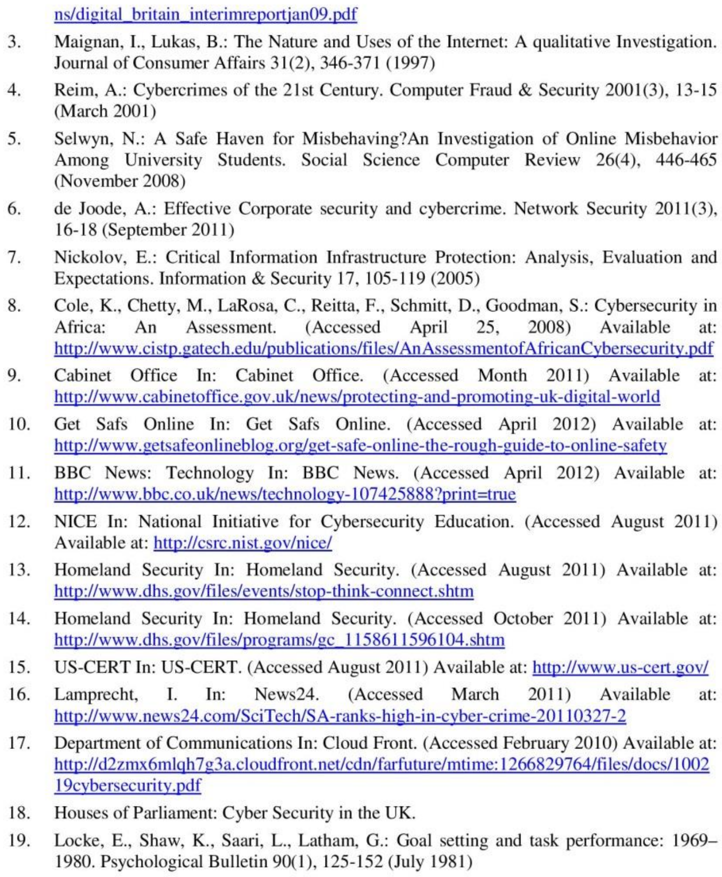
The suggestions made are intended to assist developing countries in their endeavours to derive a strategy for solidifying an envisaged cyber security culture. It is acknowledged that the suggestions are only part of the eventual solution.

6 Acknowledgement

The financial assistance of the National Research Foundation (NRF) in this research is hereby acknowledged. The opinions expressed and the conclusions arrived at are those of the authors and are not necessarily to be attributed to the National Research Foundation.

7 References

1. Hunton, P.: A rigorous approach to formalising the technical investigation stages of cybercrime and criminality within a UK law enforcement enviroment. Digital Investigation 7(2011), 105-113 (January 2011)
2. Digital Britain In: Digital Britain the interim report. (Accessed January 2009) Available at: http://webarchive.nationalarchives.gov.uk/+/http://www.culture.gov.uk/images/publicatio



ns/digital_britain_interimreportjan09.pdf

3. Maignan, I., Lukas, B.: The Nature and Uses of the Internet: A qualitative Investigation. Journal of Consumer Affairs 31(2), 346-371 (1997)

4. Reim, A.: Cybercrimes of the 21st Century. Computer Fraud & Security 2001(3), 13-15 (March 2001)

5. Selwyn, N.: A Safe Haven for Misbehaving?An Investigation of Online Misbehavior Among University Students. Social Science Computer Review 26(4), 446-465 (November 2008)

6. de Joode, A.: Effective Corporate security and cybercrime. Network Security 2011(3), 16-18 (September 2011)

7. Nickolov, E.: Critical Information Infrastructure Protection: Analysis, Evaluation and Expectations. Information & Security 17, 105-119 (2005)

8. Cole, K., Chetty, M., LaRosa, C., Reitta, F., Schmitt, D., Goodman, S.: Cybersecurity in Africa: An Assessment. (Accessed April 25, 2008) Available at: http://www.cistp.gatech.edu/publications/files/AnAssessmentofAfricanCybersecurity.pdf

9. Cabinet Office In: Cabinet Office. (Accessed Month 2011) Available at: http://www.cabinetoffice.gov.uk/news/protecting-and-promoting-uk-digital-world

10. Get Safs Online In: Get Safs Online. (Accessed April 2012) Available at: http://www.getsafeonlineblog.org/get-safe-online-the-rough-guide-to-online-safety

11. BBC News: Technology In: BBC News. (Accessed April 2012) Available at: http://www.bbc.co.uk/news/technology-107425888?print=true

12. NICE In: National Initiative for Cybersecurity Education. (Accessed August 2011) Available at: http://csrc.nist.gov/nice/

13. Homeland Security In: Homeland Security. (Accessed August 2011) Available at: http://www.dhs.gov/files/events/stop-think-connect.shtm

14. Homeland Security In: Homeland Security. (Accessed October 2011) Available at: http://www.dhs.gov/files/programs/gc_1158611596104.shtm

15. US-CERT In: US-CERT. (Accessed August 2011) Available at: http://www.us-cert.gov/

16. Lamprecht, I. In: News24. (Accessed March 2011) Available at: http://www.news24.com/SciTech/SA-ranks-high-in-cyber-crime-20110327-2

17. Department of Communications In: Cloud Front. (Accessed February 2010) Available at: http://d2zmx6mlqh7g3a.cloudfront.net/cdn/farfuture/mtime:1266829764/files/docs/100219cybersecurity.pdf

18. Houses of Parliament: Cyber Security in the UK.

19. Locke, E., Shaw, K., Saari, L., Latham, G.: Goal setting and task performance: 1969–1980. Psychological Bulletin 90(1), 125-152 (July 1981)

APPENDIX A3: SOUTH AFRICAN COMPUTER JOURNAL (SUBMITTED)

A conceptual framework for cyber security awareness and education in SA

Noluxolo Kortjan[1], **Rossouw von Solms**[2]

School of ICT, Nelson Mandela Metropolitan University, South Africa

ABSTRACT

The Internet is becoming increasingly interwoven in the daily life of many individuals, organisations and nations. It has, to a large extent, had a positive effect on the way people communicate. It has also introduced new avenues for business and has offered nations an opportunity to govern online. Nevertheless, although cyberspace offers an endless list of services and opportunities, it is also accompanied by many risks that many Internet users are not aware of. As such, various countries have developed and implemented cyber security awareness and education measures to counter to the perceived ignorance of the Internet users. However, there is currently a definite lack in South Africa (SA) in this regard, as there are currently no government-led cyber security awareness and education initiatives. The primary research objective of this paper, therefore, is to propose a cyber security awareness and education framework for SA that will assist in creating a cyber secure culture in SA among all of its users of the Internet.

CATEGORIES AND SUBJECT DESCRIPTORS

KEYWORDS

South Africa, cyber security, cyber security awareness and education

1. INTRODUCTION

In modern technology, the Internet has become one of the most significant inventions to date [1]. Over the years the Internet has developed immensely, providing billions of individuals and organizations across the globe with endless opportunities such as digital communication [2]. Although the Internet offers numerous advantages, it is constantly threatened by many risks that often have serious adverse effects on those who use the Internet. One of these risks is online crime [3]. The Internet has given criminals a platform on which to grow and proliferate [4].

Core to criminal activities on the Internet is the exploitation of private information [5]. Thus, Internet users are at risk of having their private information compromised and misused. According to Thomson, von Solms and Louw [6], many users are unaware and ignorant of the concept of protecting their personal and confidential information. Moreover, users online behave in an unsecure manner which makes them easy targets of exploitation. Consequently, humans are deemed as "a severe threat to each other's security" [7]. Moreover, users are not only pose as a threat to each other, but to also to national security [8].

In this context, it is the role of the government to empower all levels of society by providing the necessary knowledge and expertise to act securely online. However, there is currently a definite lack in South Africa (SA) in this regard, as there are currently no government-led cyber security awareness and education initiatives [9]. The primary research objective addressed in this paper, therefore, is to propose a cyber security awareness and education framework for SA that will assist in creating a cyber secure culture in SA among all of its users of the Internet. The following section will briefly discuss current cyber security efforts in SA.

2. CYBER SECURITY EFFORTS IN SOUTH AFRICA

SA becomes ever more reliant on cyberspace to govern and to conduct business; it is increasingly being exposed to cyber threats [10]. In the year 2010, the South African government released a Draft Cyber Security Policy [11]. This draft policy implied that SA is not currently in a position to deal effectively with cyber-related threats [11]. Additionally, the draft policy stated that SA lags behind other countries in the development of cyber security protocols and standards, as well as in the implementation of such protocols and standards.

Articulated in this draft policy framework is the intent to secure cyberspace and to ensure that the protection of SA's national critical information infrastructure. This draft policy framework aims to create a knowledgeable society that understands cyber-related threats. Moreover, it intends to provide a cyber security approach that is holistic and, in doing so, it requires the support of all role-players such as the state, the public and private sector and society at large [12].

This draft policy framework envisages that SA wishes to cultivate a cyber security culture amongst its citizens and society. As such, cyber security awareness and education is a critical component towards such a culture [10]. Conversely, the

[1] Noluxolo.Kortjan@nmmu.ac.za

[2] Rossouw.VonSolms@nmmu.ac.za;

draft policy framework at hand is silent regarding cyber security awareness and education. Moreover, as yet, SA does not have government-initiated cyber security awareness and education initiatives in place [9]. Although there are currently existing cyber security awareness and education initiatives in SA, they are offered by academic institutions and industry [9]. The proposed framework for cyber security awareness and education for SA will, if implemented and used, contribute in creating the envisaged cyber secure culture in SA amongst its citizens and users of the Internet. Following is a comparative analysis of similar awareness and educational efforts in other developed countries.

3. CYBER SECURITY AWARENESS AND EDUCATION KEY FACTORS

Placing A comparative analysis on the awareness and educational components, as part of the cyber security efforts of United States of America (US), United Kingdom (UK), Australia, and Canada was performed. These countries were chosen because all of them have national cyber security strategies, have at least one national cyber security education and awareness initiative and are listed in the Organization for Economic Co-operation and Development (OECD). Being a member of the OECD is of relevance to the study because this organization promotes the development of policies that improve a country's economic and social well-being [13]. The analysis was based on the following thematic questions:

1. Why is cyber security awareness and education important to the country?
2. What is the country's foremost aim regarding cyber security awareness and education?
3. Who is assigned the duty to oversee cyber security awareness and education related tasks?
4. How is the country planning to work towards cyber security awareness and education?
5. When is the implementation of cyber security awareness and education initiatives expected?

Based on the arguments, deductions and conclusions from the analysis, key factors were extrapolated for the purpose of constructing the basis of the proposed awareness and education framework for South Africa. The key factors are listed below.

- Cleary articulated **goals** should be defined.
- A **dedicated team** should be appointed.
- An **action plan** should be outlined.
- A **national cyber security awareness and education campaign** should be defined.
- **Partnerships** should be established.
- **Resources** should be in place.
- **Monitoring techniques** should be defined.

The above listed key factors form the basis of the proposed awareness and education framework. The resultant framework is presented in the following section.

4. THE CYBER SECURITY AWARENESS AND EDUCATION FRAMEWORK

The previous section presented the key factors identified that should form the basis of the proposed cyber security awareness and education framework. Moving forward, this section will introduce the proposed framework and discuss its elements individually.

The proposed framework is divided into five layers and one overarching component as listed below:

- The Strategic Layer – this layer reflects the overall vision of the government concerning cyber security awareness and education.
- The Tactical Layer – this layer suggests the schemes that SA should employ to realize its cyber security awareness and education goals.
- The Preparation Layer – this layer prepares the contents of the scheme identified in the tactical layer.
- The Delivery Layer – this layer defines the recipients of the preparations made in the preparation layer, namely the target audience.
- The Monitoring Layer – this layer examines the progress made by the scheme towards fulfilling the governments' vision.
- Resources – this component defines the resources which should be inputs in all the aforementioned layers.

Respectively, the abovementioned layers illustrate six themes embodied in the cyber security awareness and education framework. Firstly, the cyber security awareness and education 'dream' of the government; secondly the proposed strategies to be used to fulfill the dream; thirdly, the preparations necessary towards realizing this dream, fourthly, the heirs of the dream; fifthly, the monitoring of the progress towards the dream and finally the necessary resourcing. A graphical illustration of the framework is presented in Figure 1 below. The remainder of this section will provide a detailed discussion of the respective layers of the framework.

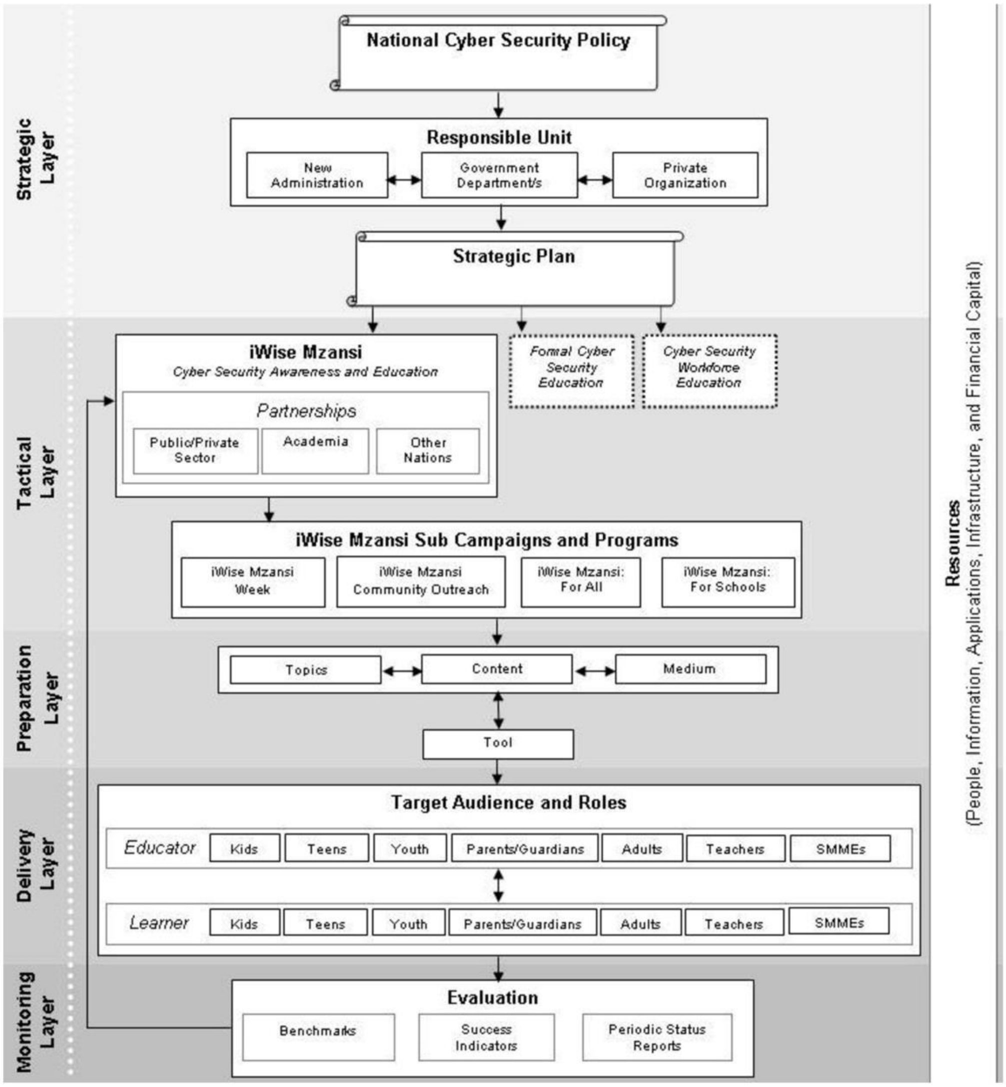


Figure 1. Cyber security awareness and education framework

4.1 The strategic layer

The strategic layer reflects the overall vision (the dream) of the government concerning cyber security awareness and education. It is known, from the draft Cyber Security Policy, that SA's overall vision is a cyber security culture. In this layer, this vision is delineated into three components, the national cyber security policy, responsible unit and strategic plan.

The first component is the national cyber security policy detailing the primary objective of each country concerning cyber security awareness and education. The second component is a responsible unit, a dedicated administration for cyber security awareness and education. The responsible unit component proposes three ways in which this administration can be formed. These ways are listed below:

- Forming a new administration;
- Using one or multiple government departments; and/or
- Delegating to a private organization

The framework recommends that once an administration is appointed, a comprehensive strategic plan should be drafted hence the last component, the strategic plan. This plan should clearly articulate how a country will approach cyber security awareness and education. It was, however, beyond the scope of this study to elaborate on every aspect that the strategic plan should comprise of. Yet from the analysis performed it was gathered that the strategic plan should make known the schemes that the country should employ to realize the cyber security goals. Such schemes will fall into the next layer which will be discussed in the following subsection.

4.2 The tactical layer

The tactical layer lies below the strategic layer. As stated, this layer continues where the strategic plan defined in the strategic layer left off. In this layer, the suggested elements to drive cyber security awareness and education are stated.

The tactical layer has four components which are proposed in the framework. The first component is a national cyber security awareness and education campaign. This suggestion was confirmed by the fact that all the countries analysed have one or more cyber security awareness and education initiatives. The proposed name for the South African campaign is iWise Mzansi. iWise Mzansi suggests an informative SA, hence the "i", and cyber wise SA, hence the name Mzansi. "Mzansi" is an accepted name that refers to SA.

The findings from the performed analysis indicate a variety of aspects which should be considered in such a campaign. One of those aspects is the establishment of partnerships with public/private Sector, academia and other nations. These partnerships would allow industry, academia and other nations to contribute to a country's cyber security awareness and education. Such partnerships, particularly with other nations, would promote the alignment of cyber security awareness and education among nations. Moreover, in partnership with academia, iWise Mzansi would benefit current research that would help to align what the campaign has to offer with the specific needs of South African citizens. It is proposed that iWise Mzansi could reach the people of SA through the below mentioned campaigns:

- iWise Mzansi Week
- iWise Mzansi Community Outreach
- iWise Mzansi : For All
- iWise Mzansi: For Schools

iWise Mzansi week is intended to be an annual event aimed at all South African citizens. This week should serve as a reminder that cyber security is a shared responsibility and should also induce and spread awareness of current and anticipated cyber security practices and issues. With all these campaigns, a South African 'flavour' should be adopted, meaning the South African context should be taken into consideration.

iWise Mzansi Community Outreach is intended to give everyone an opportunity to lend a helping hand. This programme will allow any member of society to be part of iWise Mzansi by volunteering to participate in spreading the cyber security awareness and education message to communities. This programme is closely linked with the well-known philosophy of ubuntu (humility) in SA [14].

It is proposed that iWise Mzansi: For All should be an all-encompassing website addressing the general public in SA. Finally, it is proposed that iWise Mzansi: For Schools should target primary and secondary schools.

Since cyber security education is broad in nature, a national cyber security awareness and education campaign is not the only end to cover. Alongside iWise Mzansi, are two more proposed components; these encompass formal cyber security education for students and cyber security education for those in the workforce. However, providing insight on what these two components should comprise of falls outside of the scope of this paper. Thus, students together with people in the workforce are also part of society; therefore they will be included in iWise Mzansi.

The major facet of the tactical layer is the cyber security awareness and education campaign, iWise Mzansi, and also the suggested subordinate campaigns and programmes that should be used to reach South African citizens. Having said this, one may wonder about the following:

- What topics will iWise Mzansi cover?
- What communication tools will be employed?

The following subsection will introduce another layer that will answer the questions posed above.

4.3 The preparation layer

The preparation layer concerns itself with defining the cyber security awareness and education resources that iWise Mzansi will offer to the people of SA. The preparation layer comprises of four components; topics, content, medium and tools. With regard to topics, from the analysis of cyber security awareness and education initiatives, a number of topics that are common throughout the initiatives may be identified. Such topics include, but are not limited to, cyber bullying, cyber stalking, identity theft, fraud, phishing, securing personal and private information online and secure behaviour. These topics and more could be covered by iWise Mzansi. However, further research has to be done in order to find out the particular needs of South African citizens.

Figure 1 suggests a particular relationship between content and topics in the preparation layer. This relationship is guided by the target audience that the material will be offered to. For example, if material on cyber bullying is offered to children, the content may include how to report a cyber bully. However, the same topic, offered to a different target audience such as a parent, may include such content as the warning signs of a cyber bullied child. Thus, there is a definite link between topic and content.

The preparation layer as shown in Figure 1 further presents a link between content and medium. This relationship suggests that based on the defined topic together with the content, a suitable medium of communication should be chosen. There are two acknowledged mediums, that is, paper based and electronic. Once these elements are clear, the tools that will be used must be defined. These tools include websites, videos, games, quizzes and so forth. Thus, a suitable tool should be chosen based on the topic, content and medium. From this layer one further question arises:

- To which target audience will iWise Mzansi deliver cyber security awareness and education?

This question will be addressed in the following subsection.

4.4 The delivery layer

The delivery layer concerns itself with the process of defining the target audience to which iWise Mzansi will deliver awareness and education. In addition, it will also define the roles that this audience will play within iWise Mzansi and amongst each other. There can possibly be seven different target audiences defined, namely:

- Kids younger than 13 years
- Teenagers
- Youth
- Parents/Guardians
- Adults

- Teachers
- Small, Medium and Micro-sized Enterprises (SMMEs)

It is proposed in this layer that iWise Mzansi delivers cyber security awareness and education to the above mentioned audiences as they represent the nation at large. In addition, this layer identifies two roles that these audiences should play, a Learner Role and an Educator Role.

It is well known that cyber security is the responsibility of everyone who enjoys the benefits offered by cyberspace. Therefore, it is recommended that the defined target audience take up the responsibility of using the resources that iWise Mzansi will offer to educate them, thus assuming the role of a learner. Moreover, it is also recommended that everyone passes on what they have learnt to one another, thus assuming the role of an educator.

Once the target audiences and roles in iWise Mzansi are clear what is left is defining the manner in which the progress towards achieving the primary cyber security awareness and education will be monitored. The monitoring component will be discussed in the following subsection.

4.5 The monitoring layer

The Monitoring Layer is the final layer of the cyber security awareness and education framework. It was gathered from the analysis that there should be monitoring and evaluation of the progress made in the cyber security awareness and education efforts. In addition, the effectiveness of the campaign should be evaluated. As such, the framework suggests the following:

- Benchmarks must be declared
- Success indicators must be defined
- Periodic status reports must be generated

It is suggested that the feedback from the evaluation should inform iWise Mzansi in the tactical layer. In so doing this national cyber security awareness and education campaign should be adapted on the basis of the feedback from the evaluation. For instance, if a declared benchmark or certain success indicator fails to materialise, iWise Mzansi may possibly need to make some changes in the Preparation Layer. Consequently, the topics, content or tools in this layer may be adapted in order to get the expected results.

The monitoring layer serves as the last layer of the framework. The following subsection will discuss the resources component.

4.6 Resources

TIn order for all the components identified in the framework within each layer to be addressed, certain resources have to be in place. The framework identifies five types of resources that will be needed as input in all the layers of the framework. These resources are as follows:

- People – The people needed to carry out a certain function.
- Information – The information required to carry out function.
- Applications – Computer application such as software programs which will be needed.
- Infrastructure – The physical hardware such as desktops and servers.
- Financial Capital – Monetary resources that will be needed.

These resources are adopted from the Information Technology Infrastructure Library (ITIL) and have been identified as being essential to delivering an information technology service [15]. In the context of this framework, cyber security awareness and education is the service which will be delivered. Therefore, within the five layers of the framework, appropriate resources have to be identified.

Each and every layer of the cyber security awareness and education framework will need one or more resources in order for components within each layer to be in place. Hence, the government has the duty to ensure that these resources are in place. This subsection marks the last component of the proposed framework.

The proposed framework was developed in such a manner that its layers are in line with the Plan-Do-Check-Act (PDCA) cycle presented by figure 2.

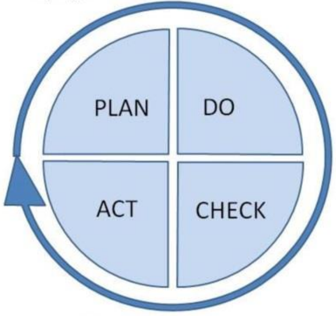


Figure 2. PDCA cycle

Figure 2 depicts the iterative four-step process of the PDCA Cycle. According to ISO/IEC 27000 these steps signify the following [16]:

- Plan – establishing objectives and processes which are necessary in order to deliver certain outcomes.
- Do – implementing the outlined plan.
- Check – monitoring and measuring progress against particular requirements.
- Act – taking action in accordance to the feedback obtained from the monitoring.

These steps overlap well with the layers of the proposed framework, as the "planning" step can be recognised in the strategic and tactical layers, and the "doing" step can be seen in the preparation and delivery layers. In addition, the checking step can be recognised in the monitoring layer. Finally, the feedback from the monitoring layer triggers the acting step, as elaborated in subsection 5.5 of this paper.

The use of this proposed framework will enable SA to define a national cyber security awareness campaign, here proposed as iWise Mzansi. This campaign will serve as a means for providing SA citizens with the necessary cyber security understanding and knowledge, and will therefore contribute to the creation of the envisaged culture.

5. CONCLUSION

Cyberspace had humble beginnings. Over time it has progressed immensely providing individuals with endless opportunities. Imbedded in these opportunities, however, are risks that compromise the safety and security of the individuals that participate in cyberspace. It would seem that people are largely unaware of these risks; and so they put themselves, as well as businesses and governmental assets and infrastructure, at risk.

In recognition of this, SA wishes to promote a culture of cyber security among its citizens. Cyber security awareness and education plays a big role in cultivating such a culture.

Accordingly, this paper proposes a cyber security awareness and education framework that will assist SA in promoting its envisaged cyber security culture.

The implementation of this framework will afford SA a national cyber security awareness campaign, iWise Mzansi. Furthermore, making use of its subsidiary campaigns will mean that South African citizens will be the recipients of cyber security awareness and education that is suitable for a South African audience.

REFERENCES

[1] P. Hunton, "A rigorous approach to formalising the technical investigation stages of cybercrime and criminality within a UK law enforcement environment," Digital Investigation, vol. 7, no. 3–4, pp. 105–113, Apr. 2011.

[2] S. Livingstone and E. J. Helsper, "Information , Communication & Society Taking risks when communicating on the Internet : the role of offline social- psychological factors in young people ' s vulnerability to online risks," Information, Communication & Society, vol. 10, no. 5, pp. 619–644, 2007.

[3] A. Riem, "Cybercrimes Of The 21st Century," Computer Fraud & Security, vol. 2001, no. 3, pp. 13–15, 2001.

[4] N. Selwyn, "safe haven for misbehaving? An investigation of online misbehaviour amongst university students," Science Computer Review, vol. 26, no. 4, pp. 446–465, 2008.

[5] A. de Joode, "Effective corporate security and cybercrime," Network Security, vol. 2011, no. 9, pp. 16–18, Sep. 2011.

[6] K.-L. Thomson, R. von Solms, and L. Louw, "Cultivating an organizational information security culture," Computer Fraud & Security, vol. 2006, no. 10, pp. 7–11, 2006.

[7] K. D. Mitnick and W. L. Simon, The Art of Deception: Controlling the Human Element of Security. Wiley Publishing, 2002.

[8] M. Grobler, Z. Dlamini, S. Ngobeni, and A. Labuschagne, "Towards a cyber security aware rural community." 2011.

[9] Z. Dlamini and M. Modise, "Cyber security awareness initiatives in South Africa: a synergy approach," in 7th International Conference on Information Warfare and Security, 2012.

[10] N. Kortjan and R. von Solms, "Fostering a cyber security culture: a case of South Africa," in Proceedings of the 14th Annual Conference on World Wide Web Applications, 2012, no. November.

[11] SA Government Gazette, "Draft Cybersecurity Policy of South Africa," Pretoria, 2010.

[12] SA government gazette, "Draft National Cybersecurity Policy Framework for South Africa." p. 33, 2011.

[13] OECD, "The Organisation for Economic Co-operation and Development (OECD)." [Online]. Available: http://www.oecd.org/about/. [Accessed: 06-Jun-2013].

[14] T. Murithi, "Practical peacemaking wisdom from Africa: Reflections on Ubuntu," The journal of Pan African studies, vol. 1, no. 4, pp. 25–35, 2006.

[15] C. Kim and M. Renée, "ITIL v3: The use of Resources and Capabilities," 2007. [Online]. Available: http://itilblues.wordpress.com/2007/11/20/itil-v3-the-use-of-resources-and-capabilities/.

[16] ISO/IEC 27000, "ISO/IEC 27000: Information technology — security techniques — information security management systems — overview and vocabulary," 2009.

APPENDIX B: INTERVIEW BRIEF

A Cyber Security Awareness and Education Framework

Dear Interviewee

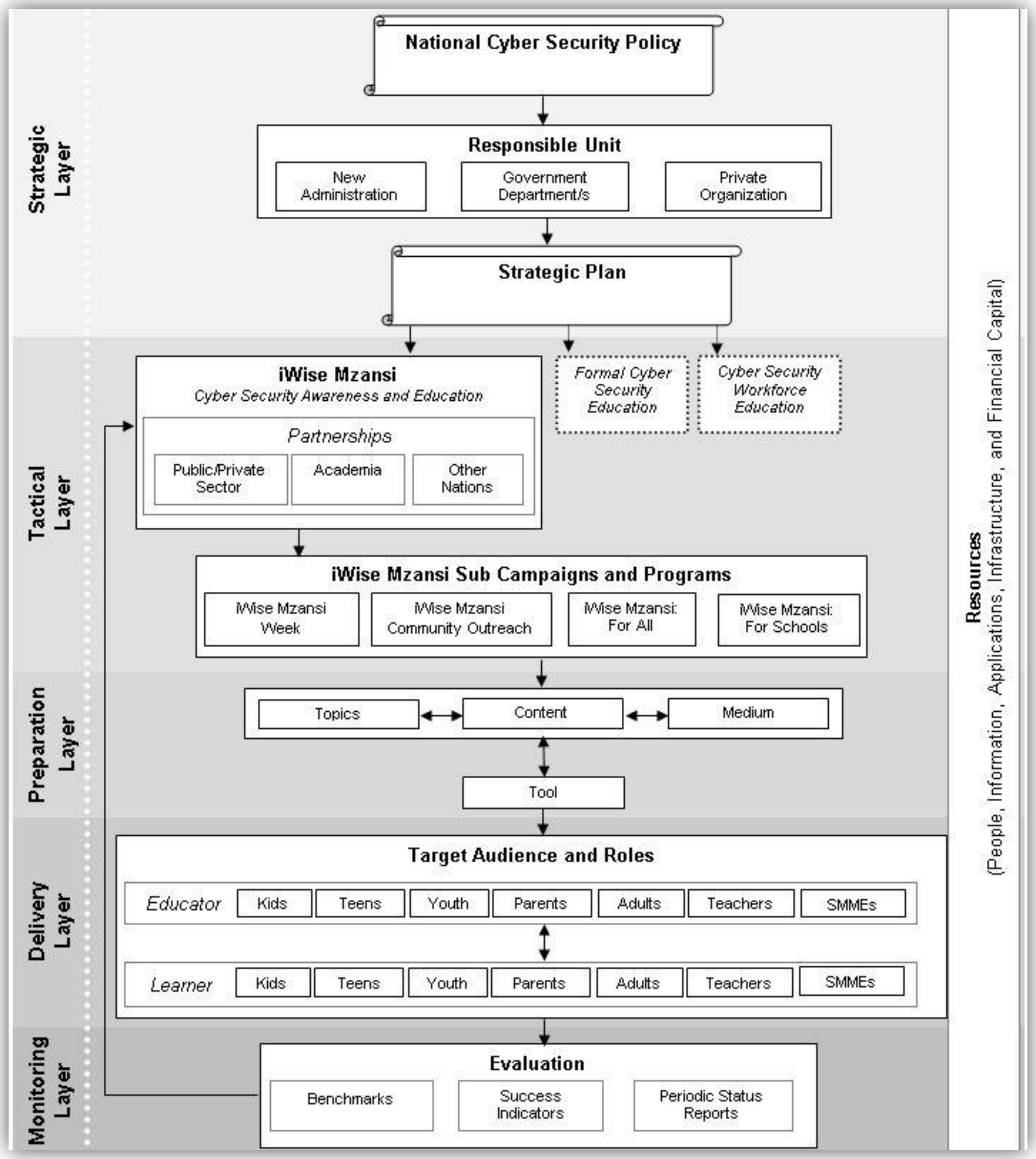
Thank you for being keen to assist me with my research project in being willing to act as elite interviewee. Please find below a brief to the methodological background of such an interview. The process I will follow in conducting the interview will begin with a brief presentation by me to introduce the project which will then be followed by short semi-structured interview. All in all, the entire interview should not last longer than 45 to 60 minutes.

Background:

“It is only through evaluation that designers come to understand the nuances of their design and add to the body of knowledge for other future designers to learn from” (Hevner & Chatterjee, 2012). For that reason evaluation is deemed as a very important component in the research process. Amongst other effects, the use of well executed evaluation methods demonstrates the quality of a research contribution. Owing to that, the verification method chosen for the proposed cyber security awareness and education framework is an elite ‘interview’.

An elite interview is formally defined as “a discussion with someone knowledgeable about a problem or its possible solution” (Cooper & Schindler 2003). According to Cooper and Schindler (2003), this method of interviewing is used to discuss a subject with a knowledgeable person, the ‘elite’. Thus, the aim of this interview is to gain as much feedback from you as the designated elite in order to improve the proposed cyber security awareness and education framework. The proposed framework is presented in the diagram below.

The Framework:



Cyber Security Awareness and Education Framework

The proposed framework is divided into five layers and one overarching component as listed below:

- The Strategic Layer – this layer reflects the overall vision of the government concerning cyber security awareness and education.
- The Tactical Layer – this layer makes known the schemes that the country will employ to realize the cyber security awareness and education goals.
- The Preparation Layer – this layer prepares the contents of the scheme identified in the tactical layer.
- The Delivery Layer – this layer defines the recipients of the preparations made in the preparation layer.
- The monitoring Layer – this layer examine the progress made by the scheme in the recipients towards fulfilling the governments vision.
- Resources – this component defines the resources which should be inputs in all the aforementioned layers.

Respectively, the abovementioned layers illustrate six themes embodied in the cyber security awareness and education framework. Firstly, the cyber security awareness and education dream of the government; secondly the strategies to use to fulfil the dream; thirdly, the preparations necessary towards realizing this dream, fourthly, the heirs of the dream; fifthly, the monitoring of the progress towards the dream and finally the necessary resourcing in each of the layers.

As mentioned more detail of the proposed framework will be presented in the beginning of the interview, however should you have any pressing queries regarding the framework please feel free to contact me.

Warm Regards,

Noluxolo Kortjan

APPENDIX C: INTERVIEW GUIDE

INTERVIEW GUIDE

1) Do you agree with the layers of the proposed framework?

2) Do you agree on the components of the proposed framework?

3) Is the framework comprehensive enough?

4) Do you think the framework will contribute to the cultivation of the suggested culture?

5) Are there any other frameworks that you are aware of which you can refer me to?

6) Any other comments and suggestions?

APPENDIX D: INTERVIEW TRANSCRIPTS

Interview Transcript: Elite no. 1

1. Do you agree with the layers of the proposed framework?

“Yes, I do agree with the layers of the framework, one of the phases of any awareness that we always have, which I have picked up from various studies that, others have 3 and others they have 2. These phases are preparation phase, followed by the design phase, and then you have implementation phase and your review phase for your monitoring.

So, those four phases are cyclic, you make sure that the awareness is the continuous thing, simply because as you mentioned there are always threats, the more we use the internet the more we come across these threats. So, those phases will make your framework to…. I don’t know… It will ensure that each and every layer is revisited annually to check how did it go and where they can improve. That will make your framework more right, I mean more alive. So I agree with it, it does look like it has all of them.

If you look at the strategic and preparation layer, they both fall under the preparation phase. The tactical layer is the design while the delivery layers fall under the implementation phase and the monitoring layer is under the review phase. So your framework has all these phases and that is why I agree with the layers but you have to mention that it has to be revisited annually”

Interviewer: Where should I note that?

“**In the line that indicates the feedback from the monitoring layer to the tactical layer. So you should write ‘continuously’**”.

2. Do you agree on the components of the proposed framework?

“The relationship between monitoring and iWise Mzansi can be specified by stating that the feedback must be continuous.

From the strategic layer I prefer personally if you would call it a strategic implementation plan so that as soon as it comes to the tactical layer, although they are still designing it [strategic plan] they are busy with its implementation.”

“In the delivery layer, I suggest you **add guardians as a target audience** because speaking from a professional’s point of view, when I am at work it is the guardians who are with the children and helping them with homework and all”

“In the preparation layer, the tools and the **medium both falls under delivery methods**, therefore I suggest you group them together.”

3. Is the framework comprehensive enough?

“I would say it’s comprehensive, because for any awareness campaign these must be these components: goal/purpose, objective of the campaign, the need of the campaign, campaign name, target audience, delivery methods, and evaluation”

4. Do you think the framework will contribute to the cultivation of the suggested culture?

“I definitely think so, because you mentioned that there would be partnering with other nations. If you look at the countries that you have studied and more they always reference each other. And we must it our own but also show SA that cyber security is an international issue.”

5. Are there any other frameworks that you are aware of which you can refer me to?

I know that the DOC is still working on coming up with something like this. I’m not sure how far that is, since you know that the cyber security framework is still pending.

6. Any other comments and suggestions

a) “I do feel that giving kids the responsibility to educate others is too much of a responsibility. Also, depending on the culture of the audience that your framework targets having a child educate a parent might not work out well. Please do consider such factors”

b) “Also the child might not pass the correct information to the next person so an issue of the integrity of the information is introduced.”

c) “In any awareness we normally try to have a conducive transformation from physical world to cyberspace, so if you ask a kid to teach a mother that might not be acceptable”

d) “I like the word ‘iWise Mzansi, but you elaborate on it in your framework definition. It makes more sense to if you link back to iWise Mzansi for the educator role in the delivery layer not the target audience’”

e) “All in all I like your work; your framework is very much into detail and looks like something that can work.”

Interview Transcript: Elite no. 2

1. Do you agree with layers of the framework?

“Yes, I totally agree with the layers, they are interestingly similar by what is set out by other people. The one thing is from the delivery layer, if you look at schools you will have a problem with awareness being the responsibility of the DOC as opposed to schools being the responsibility of the Department of Basic Education. So I think you should make reference to the two governments, the interrelationship between the government departments. That means, **your framework must make provision for the interrelatedness of cyber security between different government departments**”

2. Do you agree with components of the proposed framework?

“The components are fine as they are, as long as you show in the strategic layer interrelationship between the government departments. See it as a matrix structure.”

3. In your opinion, is the framework comprehensive enough?

“The framework is comprehensive, yes, it can be even more so if it cater for the interrelatedness of the responsible unit.”

4. How do you see that this framework will be a contribution?

“The framework will contribute to cyber security awareness and education because it structures things that people are currently a little bit there and there, things that people don’t see as a full blown framework. The framework nicely links all these facets”.

5. Are there other frameworks which you can refer me to?

There are not any other frameworks, which I am aware of.

6. Other comments and suggestions?

a) “In the comparative analysis you did to come up with the key factors, you did not mention Estonia. The reasons I suggest you **include Estonia** are that it was the first the country to react to a cyber attack. Estonia is the only country with the highest governance and integration of IT, you will see if you read that in Estonia you pay for almost everything with electronically. That means if their banking systems go down the economy goes down. They had a DDos attack in their banking systems, and that is the reason why Estonians are leaders in to setting the drive in cyber security in Europe and in the world.”

b) “I totally agree with your key factors for the framework, more especially the monitoring techniques. When the USs did its reevaluation after three years, they said monitoring was their biggest problem because no monitoring techniques where defined in the initial stages.”

c) “Propose a **month for iWise Mzansi** because most countries have a month and a week is too short”.