Creating a Cyber Skills Framework for South Africa

Elizabeth Phillips

Abstract—In this paper, we set out to argue the case for a cybersecurity curriculum for South Africa and identified distinct users of cyberspace in South Africa and the skills training they require in order to safely navigate across cyberspace.

1 Introduction

The invention of the internet and the speed of it's adoption has been helped by the boom of Web 2.0. The growth has reduced the barriers of time, distance, language and culture and has enabled developing countries to become further connected to information that was previously inaccessible[14]. The relatively low level of skill and resources required to participate in this digital revolution provides an accessible entry barrier to the World Wide Web (WWW) and enables information to be created and shared by anyone at a global scale[17].

However, with the expansion of cyberspace comes new difficulties and challenges as we embrace this revolution. Just as the industrial revolution led to health and safety training and the invention of auto-mobiles preceded the invention of the common "rules of the road", users are navigating through cyberspace without appreciating the hazards that also exist in this uncharted domain.

2 Need for a curriculum

In developed nations, the adoption of digital technologies has been a steady process, individuals have seen the transition from computers that occupy the size of whole rooms involving limited processing capabilities to portable computers, through to personal computers, laptops and now smartphones and tablets. The limited processing capabilities of these early machines and the transparency of the programs run resulted in a small number of qualified specialists being able to operate the machines. With the dawn of the internet, in developed nations, individuals began to appreciate the need for antivirus protection and appropriate security settings.

With the development of operating systems and the increase in the variety of applications capable of running on personal computers, security settings have become more difficult to locate and the creation of new user interfaces (UI) has led to users being unaware of the exact workings of applications and the information/applications that the software interacts with. The initial deployment of Microsoft's MS-DOS operating system contained in the region of 4,000 lines of code but their latest operating system, Windows 8 shipped with over 40 million lines of code. This dramatic increase in complexity provides obscurity that attackers exploit to conduct malicious operations without raising the user's suspicions.

Meanwhile in developing nations, for many users, due to the difficulties in laying the infrastructure required to deliver underground cables across South Africa, their only access to the internet is through mobile internet and is usually done on smartphones or on portable devices. As such, many of the internet users in South Africa have missed stages in their cyber training leaving them more susceptible to generic attacks than those in developed nations.

This gap in the skill straining for the individuals has led to an increase in a new type of targeted attacks in this new territory and a new breed of cybercriminals has emerged.[1] In 2013, Lloyds TSB ranked Cyber Crime as 3rd

1. http://www.news24.com/Technology/News/Lack-of-SA-skills-leads-to-cyber-attack-risk-firm-20130927

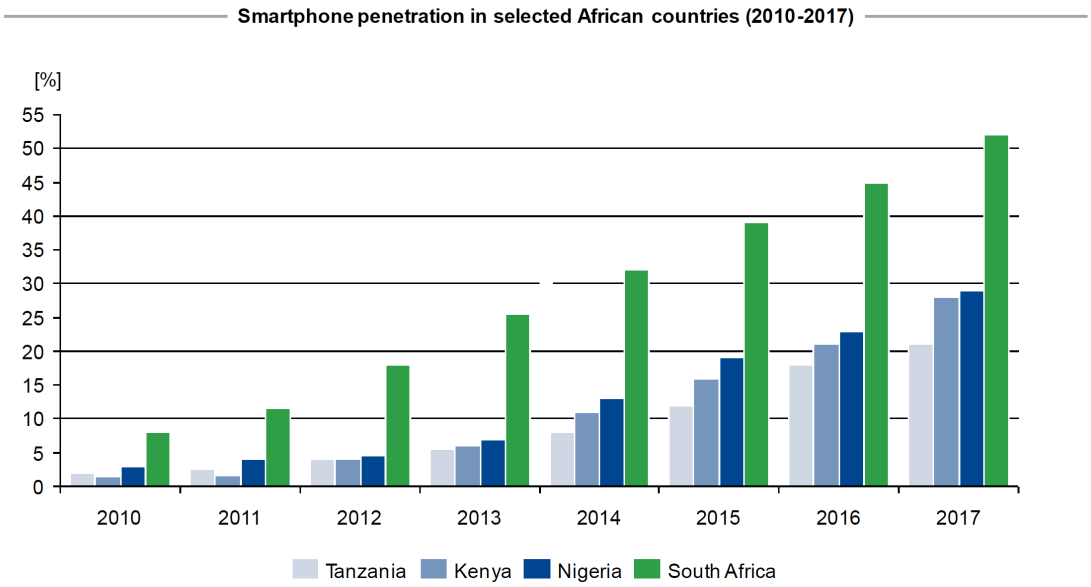

Fig. 1. The adoption of smartphones in Africa and a prediction of the continued growth of the uptake of smartphones through to 2017

in their Risk register. Many of the successful attacks can be mitigated by introducing basic training for all users so that they are more confident operating in cyberspace. Given the ubiquitous nature of computing and IT, and the need for cybersecurity to be considered in all aspects of the profession, the knowledge and skills required of an cyber security practitioner are not limited to a specific country, job role, career path, industry or application of IT; rather they are pervasive and range from broad generalist skills to very deep specialist skills. As such cyber security skills are needed in the profession at all levels and throughout society in general, since we are all personally responsible for the security of information with which we are entrusted.

Whilst a Cyber skills framework and curriculum will help provide a framework for providing effective training for users, individuals must also be responsible for developing their own personal cyber knowledge and skills. With the connected nature of cyberspace, an attacker need only exploit one single vulnerability left inadvertently by an untrained user to act as a springboard from which to launch an attack at an organisation/individual. Therefore in order to successfully protect against such an attack, we need to create a curriculum that is society wide and is not solely aimed at technology professionals similar to that of the "Cyber Streetwise" campaign in the UK.

2.1 The importance of non-technical approaches

An effective cyber security strategy must therefore employ not just the reactive and defensive measures that can be offered from technical solutions; it must also encourage proactive and anticipatory measures borne of understanding human behaviour and motivations of those intent on doing us harm.

3 Current state of Cyber Security in South Africa

In 2011, South Africa was ranked 5th in the World Mobile Data Rankings compared to the USA who came 7th in the same ranking[11] in terms of mobile data usage. Figure 1 shows the predicted increase in the adoption of smartphones up to 2017 which shows the continued increase in smartphone use across Africa and shows South Africa's continuous lead in the use of smartphones compared to other similar countries.

According to the world bank[3] by 2013, only 3.06% of South Africans had a fixed broadband

internet connection compared to 35.73% of UK citizens and 9.48% of the world overall. This reliance on smartphones to access the internet brings with it its own challenges and difficulties for varying users.

3.1 Private internet users

With the rise of web 2.0, the increase in the number of smartphones and tablet PCs across South Africa and the progress towards greater mobile internet access and broadband access across South Africa, a fast growing number of private users are becoming victims of increasingly sophisticated cyber threats. These private internet users use cyberspace to conduct everyday tasks such as online banking, social networking, email communication and other daily tasks.

In order to cope with the increasing adoption of cyberspace, a nat]ional strategy needs to be set up to help create cybersecurity education programs and broad public awareness campaigns. These campaigns need to cover behavioural training (e.g. informing users not to click on unknown email attachments) as well technical guidance (e.g. password strength and encryption standard for WIFI networks). When creating a curriculum, we need to ensure that the it is designed in such a way that it is accessible for all users regardless of disability, and it needs to be accessibly remotely over the limited bandwidth available in large parts of South Africa.

3.2 Business users

Within South Africa, many of the small and medium enterprises (SMMEs) are in a similar position to individual users and are restricted to low bandwidth internet connections and limited resources which leaves them incapable of dealing sufficiently with cyber threats. Their skills level is on average slightly higher than that of a private internet user but a modular curriculum is required in order to improve their skills and allow them to tackle the developing cyber threats.

For large corporations where many include offices oversees, many of them have established processes and experienced/skilled personnel in order to comply with Information Security Standards (ISO 27xxx series) and allow the organisation to act as a third party supplier for other large ISO compliant organisations. The close links with other large organisations also allows for a transfer of knowledge between organisations and allow the security professionals in an organisation to gain insight into any new developments in Cyber Security.

3.3 Critical Infrastructure

As far back as South Africa's National Security Intelligence Act 1994[7], South Africa has identified the need to protect critical infrastructure (including water, electricity etc.) essential to the day-to running of the nation. Newer legislation such as the Defence Act (Act 42) of 2002[5] have helped to prioritise further the protection of these essential services.

Chapter XV of the Electronic Communication and Technology ACT (ECTA) in South Africa provides clear outlines as to the protection of such CI and outlines the disclosure process required after an attack on CI and allows the minister to prescrive minimum standards surrounding the protection of CI. The act also provides the ability for the minister to clearly classify what qualifies as CI.

In addition to ECTA, the State Information Technology Act (SITA) act also refers to the protection of "Critical Electronic communications infrastructure"

3.4 Cyber Security Policy

On the 19th February 2010, Gen (Tet) Siphiwe Nyand, South Africa's Minister of Communications issued a governement notice indicating a *"notice of intention to make South African national cybersecurity policy"*. This noticed set out some of the essential issues that needed to be prioritised in order to address the issue of cybersecurity in South Africa. Their four main policy objectives were:-

- Facilitate the establishment of relevant structures in support of Cybersecurity.
- Ensure the reduction of Cybersecurity threats and vulnerabilities.
- Foster cooperation and coordination between government and the private sector.

- Promote and strengthen international cooperation on Cybersecurity.
- Build capacity and promoting a culture of Cybersecurity.
- Promote compliance with appropriate technical and operational Cybersecurity standards.

Whilst the completed cyber policy is still currently unavailable, in March 2012, Cabinet's approval of the Cyber Security Policy Framework[12] and some of the key components of the initial policy such as the establishment of a CSIRT and a National Cybersecurity Advisory Council (NCAC) have been met [6]. The creation of the NCAC has enabled policy decisions about cyber security to be discussed at government level in order to provide a swift and effective response to any potential cyber incident.

3.5 Cyber incident response

Complementing the national cybersecurity policies, Computer Emergency Response Teams (CERTs) and Computer Security Incident Response Teams (CSIRTs) at a national/regional level. These CSIRTs are designed to coordinate planned and adhoc acticities against cybersecurity threats and are often the point of contact for international cooperation. These CSIRTs may be public funded (such as ...) or private CSIRTs (as in ...). The national cyber policy helps the CSIRT develop operational plans in response to cyber incidents.

Prior to 2012, South Africa had worked with the Tunisian National Computer Security Agency (ANSI) and Finland to establish a national CERT. By 2012, the CSIRT in South Africa was completed and was known as ECS-CSIRT. On the completion of the CSIRT, Uchenna J.Orji concluded that *"Despite the existence of ECS-CSIRT there still appears to be a lack of awareness and local reports on cybersecurity incidents; poor coordination of incident responses and shortage of skilled incident-response experts. It is noted that this state of affairs has exposed the country's National Critical Infrastructures to major cybersecurity risks"*. Despite the initial increased risk for South Africa after their CSIRT was initially launched, as the nation begins to address cyber incidents, their cyber policy and cyber responses from the CSIRT have increased their ability to tackle cyber incidents[4].

3.6 Education in South Africa

In 2012, van Vuuren et al. conducted a survey into the levels of cyber security awareness were calculated in South Africa. They found the levels to be 69% for urban areas, 53% for semi-rural areas, and 40% for rural areas. A cumulative extrapolation of total awareness in South Africa based on the overall awareness of the sample group is estimated at 51% [9]. This aspect still requires a lot of attention in South Africa.

Education aspect Ranking	Ranking(out of 144 countries)
Quality of maths and science education	143
Quality of primary education	132
Primary education enrolment	115

TABLE 1

A table showing South Africa's position in the World Economic Forum's Ranking of 144 countries in terms of education quality.

One potential reason for the comparatively low cyber literacy levels is the quality of primary education in general across South Africa. In a study conducted by the world economic forum in 2013 on Global Competitiveness, South Africa was placed 143rd out of the 144 countries assessed in terms of Maths and science education and only 115th in terms of primary education enrolment in general[13]. Table 1 shows a breakdown of some of the key areas which need to be addressed in order to implement an effective cyber curriculum.

If users have not had a sufficient background knowledge of literacy and numeracy, then some of the users may find it difficult to cope with some of the content of a new curriculum. As such we need to be cautious in the way our curriculum is designed so that it is accessible to all. Current work in South Africa has helped to create a suite of educational material aimed at students aged 3 to 16 which is available in English, Sesotho and IsiZulu [16] in a user-friendly way in order to gain maximum uptake of the course material. A similar set of documents need to be tailored for those individuals

that have not had this training as part of their education at school and wish to pick up these skills later on in life.

4 Existing International Frameworks

4.1 Cyber Professionals

Currently a variety of different skills frameworks are available for cyber professionals to obtain certification of their expertise in various domains of Cyber Security. The most common cyber frameworks are:-

- **The Institute of Information Security Professionals (IISP) Skills Framework**
- **The UK Governments Communications-Electronics Security Group (CESG) Information Assurance Role Definitions** based upon the IISP framework
- **The US National Initiative for Cyber Education (NICE) Cybersecurity Workforce Framework**
- **The e-skills UK National Occupational Standards for Cyber Security**
- **The joint initiative between two US-based professional bodies: the Association for Computing Machinery (ACM) and the Institute of Electrical and Electronic Engineers (IEEE)** Computing Societys programme for undergraduate Computer Science degrees (CS2013) includes cyber security concepts
- **(ISC)2** provides a range of qualifications emphasising different aspects of cyber security skills

4.2 Difficulties with existing frameworks

These models tend to be influenced by the security priorities of the countries in which they are developed leading to the various models emphasising different aspects of cyber security, sometimes in context of wider IT professionalism but in most cases treating cyber security either as a distinct and separate discipline or only loosely coupled to IT.

Most of the frameworks are designed to be taught in countries where high-speed broadband access is readily accessible and most users interact with their daily tasks such as internet banking via a laptop. However, due to the high reliance of smartphones and mobile internet in South Africa, many of the frameworks do not cover the differences in the use of cyber devices between nations.

None of these frameworks fully address the need for a model that identifies progressive levels of competence from foundation to the most senior levels in business. Neither do they integrate with other IT/computing skills in any consistent manner; rather they treat cyber security as if it were a specialist skill, set apart from the wider IT profession.

Similarly, existing cyber policies from South Africa have been heavily focused on Confidentiality, Integrity and Availability of data. Whilst this criteria is applicable to crititcal infrastructure, we need to also consider other factors such as human aspects of cyber security in order to create a holistic approach.

5 Skills required

Despite the dynamic nature of Cyberspace, there are several skills that if mastered would allow individuals to adapt to the latest technological and sociological advances and allow them to keep themselves protected. In this paper, we set out to identify some of these key knowledge components for Cyber professionals and typical end users.

5.1 Cyber professional

For the purpose of the paper, we define a cyber professional as an individual with technological whose role in an organisation includes the maintenance and upkeep of IT infrastructure/software in an organisation. This role includes system administrators, Chief Technology Officers (CTO), Chief information Officer (CIO) etc. These individuals require specialist technical training and often undergo professional certification after several years of experience in the role in order to demonstrate a core knowledge of cyber security. These certifications are often done in a modular fashion using the frameworks defined in section 4.

In order to tackle not only the technological aspects of cyber security, but also the policy and

human aspects of cyber security, the desirable skills for a cyber professional includes (but is not limited to):-

- **consulting**
- **cyber ethics**
- **digital forensics**
- **compliance, governance and regulation**
- **cyber Assurance methodologies and testing**
- **cyber hygiene** (best practice for all in the information society e.g. effective patching regime and access control etc.)
- **implementation of secure systems** (including physical security)
- **incident management**
- **information risk management**
- **operational management**
- **research and development** (to ensure we have security and privacy by design)

If a cyber professional has the skills mentioned above, then not only will they have the technical knowledge required to swiftly detect any potential cyber attack, they will also be able to have the necessary skills required to inform the relevant people in a timely fashion in order to resolve the incident swiftly to minimise any potential damage caused as a result of an attack.

Their knowledge of the policy and human aspects of cyber security will also allow them to help create effective cyber policies and best practices for the organisation (by introducing cyber exercises, introducing new and effective access control mechanisms etc.) in order to help try to create a defence in depth approach within the organisation and help reduce the reliance on technological solutions. This in turn will help move the position of their organisation from a reactive stance to a more proactive stance in order to prevent as many of these incidents occurring in the first place as possible.

Despite the fact that cyber security frameworks are currently in existence, many of the existing qualifications, frameworks and professional bodies emphasise different aspects of cyber security. One thing they all share in common is the perspective of cyber security being a specialist domain of IT practice. Existing qualifications fall into three broad categories:

- those emphasising deep technical consulting skills
- those focusing on cyber security management and governance
- those segmenting cyber security into narrowly defined functional tasks

Two aspects of cyber security that are poorly served by existing qualifications are:

- technical operations and support staff
- generalist knowledge of cyber security for the wider IT profession

The inclusion of information risk management, incident management and digital forensics into a unified framework will help fill the gap for small and medium-sized enterprises to develop their own capabilities in-house. The skills framework will also help fill the gap left by poor cyber hygiene, aided by initiatives such as the BCS Cyber to the Citizen campaign. This, in combination with effective risk management techniques, will help professionals identify key vulnerabilities in their systems and respond effectively.

5.2 End User

Whilst a typical home user would not require the in-depth knowledge expected of a cyber professional, in order to maintain cyber hygiene, it is necessary for an end user to have a basic understanding of cyber security so that they can protect themselves from common attacks and are able to respond effectively to any successful attack in order to help increase the cyber hygiene of a nation.

Just as only one dangerous/inexperienced driver is needed to cause an Road traffic incident on the road network which may also affect innocent drivers, only one dangerous/inexperienced driver is needed to cause an incident in cyberspace which may effect several innocent users. As such, in order to reduce the likelihood of such an incident occurring in the first place, users should have to undertake the equivalent of the Highway Code of Cyberspace in order to protect themselves and others online. This highway code would include:-

- **Password Management**
- **Social Engineering**
- **Cyber Fraud**

- **Cyber Stalking**
- **Malware, worms and spyware**
- **Spam**
- **Phishing**
- **Backing Up**
- **Card payment devices**
- **On-line Bullying**
- **SmartPhone Security**
- **Internet Banking**
- **Digital Footprints**
- **Wireless Networks**

Just as seatbelts cannot protect an individual from a collision but can reduce the damage to the individual, informing end users how to correctly configure antivirus and firewalls will help minimise the damage from any cyber incident.

Whilst having the core knowledge above will not protect from sophisticated attacks, the skills and knowledge obtained from the elements above will help users safely conduct their daily tasks online with added confidence and will help reduce the amount of cybercrime online.

The inclusion of modules such as SmartPhone Security and Internet Banking are essential for end users if the users are to keep their confidence in cyberspace in order to help stimulate growth in the economy and introduce more facilities to developing nations. In order to cope with the demands of busy working lives, the course content for end users needs to be bitesize so that users can work on one module at a time around their other commitments. A modular curriculum similar to the newly created digital security modules with the UK exam board OCR can be used as a template of a short modular component.

5.3 Policy Makers

With the increasingly borderless expansion of cyberspace, the need for effective compliance and regulatory control is essential in order to maintain the security of our systems. This is not covered in many IT skills frameworks. By introducing compliance, governance and regulation into a unified framework, it will help cyber security practitioners increase their awareness of current procedures as well as helping them implement such systems in their organisations.

In an era where computers are becoming more and more entwined in our everyday lives, it is insufficient for security/technology professionals to be the only members within an organisation to have a knowledge of cyber security. Currently, South Africa are working on creating a skills framework for the judicial sector from the senior judges to the clerks and all roles in-between in order to establish what level of cyber literacy is required for each role. This will help to distinguish between the digital forensic evidence collection training required for police officers from the technical knowledge required by the judge in order to process the evidence in a similar way to the way that they might handle medical evidence.

Similarly, within an organisation, it is important that senior members of the organisation have a core knowledge of cyber security in order to protect their critical business processes and in order to help them design effective cyber policies that will be implemented by the technologists and undertaken by the employees on a daily basis. In order to help them in their decision making process, their knowledge would need to include (but not be limited to):-

- **cyber ethics**
- **compliance, governance and regulation**
- **cyber Assurance methodologies and testing**
- **implementation of secure systems** (including physical security)
- **incident management**
- **information risk management**
- **operational management**
- **strategic planning** (extra-national, national and organisational levels)

With the blurring of the boundaries of Cyberspace, the skill level required for a policy maker within an organisation overlaps with that of a cyber professional due to the need for common knowledge of incident management and the implementation of secure systems is common to both roles. However the level of knowledge required for a policy maker is different to that of a cyber professional.

For example, a system administrator would need to know how to deal with an incident from a technical solution and will need training in how to stop such an attack, whereas

a policy maker would need to concentrate on the resources and funding required to create an effective response to an incident and any legislation that may influence his decision but will still require some knowledge of the capabilities of the technical solutions on offer by the system administator.

Not only will the skills training above allow the policy makers to create effective policies, they will also have the technical knowledge to understand the consequences of an incident should one occur and will have a better understanding of the cost and resources required to resolve the situation as well as the consequences of a slow reaction and the impact that this can have on the reputation of the organisation.

5.4 Implementation

Whilst there may be some agreement about some of the initial modules required for the different professions, there are still huge differences as to the depth each module should cover and a modular approach is required. Similarly the skill level required for an individual in an SMME in comparison to a system administrator in a large multinational corporation is vastly different. As such, a levelled curriculum such as that of the newly adapted SFIA framework is required in order to allow individuals to have the knowledge at the required level for the individual to carry out their daily tasks.

Once a core content is approved, the next step would be to begin to introduce these schemes further along the education chain and increase the amount of cyber security university courses in South Africa in order to help train the next level of Cyber Security professionals in a similar manner to the degree courses available in the UK[10] and the US[15].

6 Conclusion

We have identified three distinct levels of skills training required for an effective cyber curriculum in a developing nation and propose a levelled modular curriculum consisting of key topics that will allow individuals to tailor the curriculum and specialise in areas specific for their role whilst still maintaining a base knowledge. It is also important that the focus of the curriculum expands from the traditional CIA model and incorporates behavioural aspects of cyber security in order to allow the curriculum to cope with the dynamic and evolving nature of cyberspace.

Whilst the equivalent of a "driver's licence" is not yet required to navigate across cyberspace, in order to help increase the level of cyber awareness globally, it is important that we create a framework of critical knowledge for users to help tackle the infections in cyberspace in a similar way that an increase in hygiene globally has helped to minimise the spread of infectious diseases.

Whilst the cost of the course content for policy makers and cyber professionals is placed with the individual/organisation it is vital that the costs for the end user and the introductory courses are kept to a minimum and are ideally free in order to maintain cyber hygiene nationally and in order to get maximum uptake.

Appendix A
Adoption of the internet across Sub-Saharan Africa

Figure 2 shows the adoption of internet across Sub-Saharan Africa from 1993 to 2013. From 1993 to 1999 South Africa was an early adopter of the internet and invested in infrastructure to enable internet access to be delivered easily to South Africa. This initial uptake was helped by the support of American initiatives such as the Leland Initiative [8] and help from the ITU[1] and other organisations [2].

As of 2011, the sharp increase in the uptake of internet use across South Africa has led them to overtake the world average number of internet users per country. Their sharp increase has been closely followed by that of Kenya, Equador and Nigeria which has led to an increase in the gap between these nations and other sub-saharan African nations.

As the uptake of internet usage across South Africa increases, so does our need to create a skills framework capable of providing resilience to this increasing domain.

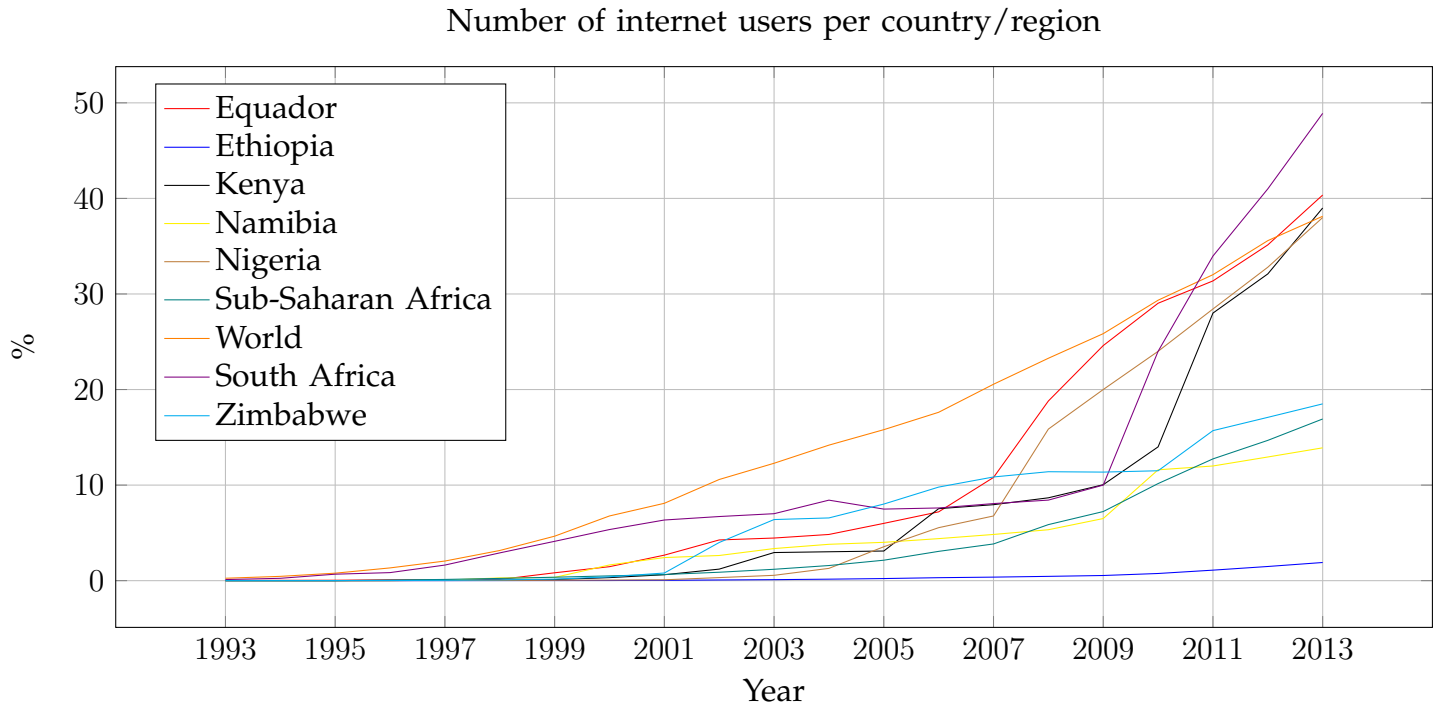

Fig. 2. A comparison of the percentage of users per country/region with internet access across Sub-Saharan Africa

REFERENCES

[1] Balancing Act. ITU launches multipurpose community telecenter initiative in Africa | balancingact-africa.com.

[2] MN Amutabi and MO Oketch. Experimenting in distance education: the african virtual university (avu) and the paradox of the world bank in kenya. *International Journal of Educational Development*, 23(1):57–73, 2003.

[3] World Bank. Fixed broadband internet subscribers (per 100 people) http://data.worldbank.org/indicator/IT.NET.BBND.P2, *accessed on 2014-09-19*, 2013.

[4] ECS-CSIRT. ECS CSIRT newsletter *volume 1*, 2012.

[5] South African Government. Defence act 42 of 2002.

[6] South African Government. Minister inaugurates national cyber security advisory council, http://www.doc.gov.za/mediaroom/media-statements/247-minister-inaugurates-national-cyber-security-advisory-council.html.

[7] South African Government. National strategic intelligence act, 1994.

[8] ITU. Leland initiative, http://www.itu.int/ITU-D/ict_stories/themes/case_studies/leland.html, *accessed on 2014-09-17*.

[9] J. Jansen van Vuuren, M. Grobler, and J. Zaaiman. *The influence of cyber security levels of South African citizens on national security*. Academic Conferences Limited, March 2012. Copyright: 2012 Academic Conferences Limited. Proceedings of the 7th International Conference on Information Warfare and Security, Center for Information Assurance and Cybersecurity University of Washington, Seattle, USA, 22-23 March 2012.

[10] BBC News. BBC news - GCHQ accredits UK master's degrees for 'cyber spies', http://www.bbc.co.uk/news/uk-28623365 *accessed on 2014-09-19*.

[11] Nielsen. Mobile phones dominate in south africa | nielsen. Technical report, September 2011.

[12] Government of South Africa. state security on national cyber security policy framework for south africa, http://www.gov.za/speeches/view.php?sid=25751&tid=59794, March 2012.

[13] Klaus Schwab on behalf of the World Economic Forum. The global competitiveness report 2012 - 2013.

[14] Ben Petrazzini and Mugo Kibati. The internet in developing countries. *Communications of the ACM*, 42(6):31–36, 1999.

[15] Education Portal. List of top cyber security schools and colleges in the u.s., http://education-portal.com/articles/List_of_Top_Cyber_Security_Schools_and_Colleges_in_the_US.html, *accessed on 2014-09-19*.

[16] UNISA. Cybersafe workbook, http://eagle.unisa.ac.za/elmarie/index.php?option=com_content&view=category&layout=blog&id=3&Itemid=4 *accessed on 19/09/2014*.

[17] Alexander Van Deursen and Jan Van Dijk. Internet skills and the digital divide. *new media & society*, 13(6):893–911, 2011.