IST-Africa
IST-Africa 2012 Conference Proceedings
Paul Cunningham and Miriam Cunningham (Eds)
IIMC International Information Management Corporation, 2012
ISBN: 978-1-905824-34-2

Global Cyber Trends a South African Reality

Marthie GROBLER[1], Zama DLAMINI[2]
Council for Scientific and Industrial Research, Pretoria, 0001, South Africa
University of Johannesburg, Auckland Park, 2001, South Africa
[1]*Tel: +27 12 841 3262, Email: mgrobler1@csir.co.za*
[2] *Tel: +27 12 841 4441, Email: idlamini@csir.co.za*

Abstract: Cyber trends are a reality across the globe. Not only are technology and electronic devices and media used more regularly in easing everyday activities, but these technological advances are also used in sophisticated criminal activities. Regardless of the global innovation and development ranking of a country, all countries tend to show the same global trends, either on a more or lesser scale. Some of the more prominent global trends are identified and discussed. This paper aims to show that these global cyber trends are also a reality in South Africa, by addressing some of the most prominent global trends. Based on the statistics available to support the presence of high cyber trends, as present in high ranked countries across the globe, this article shows that technology within South Africa has advanced to such an extent that the country is not unduly hurdled by large scale lack of connectivity and bandwidth, computer illiteracy, low Internet penetration and inadequate cyber crime related legislation. The discussion within this paper places South Africa on par with first world countries in terms of cyber trends.

Keywords: cyber trends, global, Africa, South Africa.

1. Introduction

Cyber trends are a reality across the globe. Although a number of global factors and developments impact the general direction that cyber trends take, all countries tend to show the same global trends, either on a more or lesser scale. These trends are independent of the global innovation and development ranking of a country.

Africa has recently seen explosive growth in information and communication technologies, making cyber trends more of a reality [6]. Some of the factors that make African countries more vulnerable include increasing bandwidth, increasing use of wireless technologies and infrastructure, high levels of computer illiteracy, ineffective or insufficient legislation to deal with cyber attacks and threats, as well as increasing Internet penetration rates. All these issues expose countries' crucial infrastructures to cyber risks.

In terms of phishing attacks, South Africa has been ranked amongst developed countries (such as the United Kingdom and United States) as one of the most attacked countries in the world [8] [12]. This paper aims to show that other global cyber trends are also a reality in South Africa, by addressing some of the most prominent global trends. The objective is to show that South Africa is not only on par with first world countries in terms of cyber attack statistics, but also on par with the presence of a number of cyber trends that are normally associated with higher ranked countries.

2. Approach

The current information age comes with an aggressive technological growth to which there is no foreseeable end. In order to show the impact of global cyber trends in Africa,

especially South Africa, this paper analyses and cites some of the more recent cyber trends and recent South African incidents.

These trends were selected from publicly available trend related literature [2] [5] [7] [8] [9] [11] [15] [16] [19] to shows that South Africa is comparably advanced with regard to cyber developments. The paper aims to show that South Africa is not far behind top ranked countries in terms of trends, and can in most instances, relate to trends and figures more prevalent in higher ranked countries. Africa as a continent is also placed into perspective when specific statistical data are available for a particular trend. The article presents South Africa's standing in terms of cyber trends mapped against the rest of the world.

3. Cyber Trends and Effects

Although trends tend to be consistent on a global scale, many countries will show variations of trends based on the country's specific social economic status at a specific point in time [6]. The next subsections show some of the more omnipresent cyber trends and their impacts in Africa and South Africa.

3.1 Data Driven World

Both businesses and individuals are largely dependent on data. This dependence relates not only to the physical data, but also to the means of getting access to the data at any time, i.e. interconnectedness via smart devices. According to Eric Schmidt [15], user-generated content such as digital pictures, tweets and emails are fast tracking the data driven world. *"Every two days now we create as much information as we did from the dawn of civilization up until 2003"*. Everywhere, the quantity of data and the visual representation of information are multiplying at an alarming rate.

With the strong digital component that forms part of modern day businesses, the multiplicity of cyber security is becoming more prominent [5]. In addition, more people work towards an automated environment where outputs can be maximised and human error is minimised. Although this is beneficial in terms of outputs, computerised automation has a negative impact on labour productivity. According to Adcorp Employment Index, South Africa's labour productivity fell to its lowest level in 40 years during October 2011, as calculated by output per worker [13]. Although this is not solely due to automation, this does have an impact on the actual human productivity levels since computer output cannot necessarily be translated directly to output per worker. The presence of this trend in South Africa shows that many actions are automised, and not solely dependent on individuals doing the work. Automation is generally associated with higher ranked countries with adequately computerised systems.

3.2 Bandwidth and Internet Penetration

The rate of bandwidth consumption or utilisation in South Africa increases daily. In 2007/ 2008, South Africa’s overall online activity was estimated to be 67% of overall online activity in Africa, whilst its population accounted for only 5% of the entire continent’s population. The remaining percentage of online activity was assigned to Morocco and Egypt [10]. In 2007, the total number of wireless broadband subscribers overtook the number of fixed line broadband subscribers. These numbers are still increasing [17].

According to Internet World Stats, South Africa currently has 6.8 million Internet users and an Internet penetration rate of 13.9% (refer to Figure 1). South Africa's Internet user base is foreseen to reach nine million users by the year 2014, as a result of the arrival of five new undersea telecommunications cables, one of which is already in place [17].

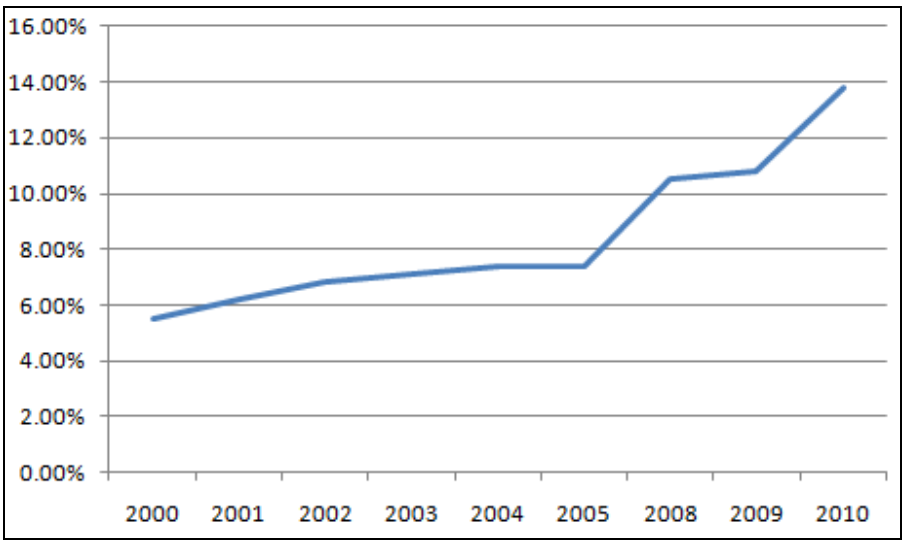

Figure 1: Internet Users in South Africa [7]

South Africa is currently ranked fourth in the 'Africa Top Internet Countries', led by Nigeria ranked first. South Africa's total international bandwidth is estimated to be more than 10 Gbit per second; its continued increase is being driven primarily by the uptake of broadband and lowering of tariffs. In South Africa alone, there are more than 433 Internet Service Providers [7]. This enables South Africa to supply up to 60% of Internet traffic to the entire African continent [17]. Since South Africa is ranked quite high within Africa, Internet penetration as an upward trend has a prominent impact on South Africa's global positioning. With regard to bandwidth and internet penetration, South Africa has a major role to play in terms of ensuring the safety of online users to the entire continent.

3.3 Ubiquitous Computing and Separation of Computing from Location

Computing *'anywhere, anytime with any electronic device'* is easily achievable with access that is not dependant on a specific device, place or time, also called ubiquitous computing. Three enablers contribute to ubiquitous computing: wireless, mobile devices and private cloud. These three enablers collectively contribute to the separation of computing from location, and each influences the other positively [4].

- Internet users in South Africa are increasingly changing from Digital Subscriber Line (DSL) connections to wireless connections. Wireless connections offer a mobility advantage that enable users to connect to the Internet anytime, anywhere and with a variety of electronic devices.
- With mobile devices (smart phones, laptops, PDAs, netbooks, etc.) staying connected has shifted from normal connections to Internet access as an option. There are currently more than 26 million mobile phone users in South Africa, 12 million of which have Internet application users. That translates to 39% of Internet users using their mobile devices to access the Internet [11]. These devices enable Internet access anywhere and anytime.
- Private cloud is fragmented from traditional cloud computing and enables better management of software, hardware, data-driven research and resource flexibility. With private cloud, a personalised computing environment with all tools and resources needed is available when accessing Internet via mobile devices, at any location and anytime [4].

While wireless connections are rising in mobile devices, so are the computation, data access, storage services and delivery services that can be performed without the user's explicit knowledge. This is added to the benefits that comes with cloud computing. World

Wide Worx recently interviewed 100 JSE-listed South African corporations. 46% of these corporations are already using cloud computing, 6% is planning to introduce it next year and another 4% the year after, accounting close to 60% by the year 2013 [20]. The corporations who implemented cloud computing are satisfied with it so far. In general, ubiquitous computing and cloud services are associated with more technologically advanced countries. Especially with the increase in mobile phone subscribers, South Africa is on its way to a better global positioning in terms of ubiquitous computing.

In addition, it is the individual's responsibility to ensure that he/she understands all the risks associated with the technology they choose to use. It is also significant to keep up with the updates and patching software that are usually available after the device was purchased.

3.4 Social Aspects

South Africa has more than 49.9 million people of diverse origin, culture, language and religion; people between the ages of 15 and 64 is the largest group, 65.8% (32 259 605 people) [17]. These are the people who are most active in terms of working and studying, as well as using electronic devices and Information Technology in general. In terms of Social Networks, Africa had an estimated 28 million Facebook subscribers by the end of 2011; 3.7 million of these users are from South Africa [2].

The concern regarding social interaction in the cyber domain is that people often forget that they are on a public global domain. Especially with day-to-day human computer interaction, people tend to forget that it is not just a document being typed on a faceless computer, but rather text that is posted on a public forum, to be read by anyone that has the time and understands the language [5]. There are several websites dedicated to these Facebook bloopers, e.g. discussions on drunken escapades, details on body enhancing operations, bad mouthing bosses and jobs, as well as intimate details of romantic endeavours [4].

Another South African example, Thabo Bester earned his nickname of 'Facebook rapist' because he used at least 13 aliases on social media to lure women under false pretences into meeting him, and then raping and robbing them at knife-point. He was sentenced to 50 years' imprisonment [14]. Most social networking sites prohibit the posting of content that is hateful, threatening or violence inciting [3], and an attempt is made to remove these controversial rape pages. This, however, follows an intense debate on freedom of opinion versus advocating rape and violence.

According to Microsoft, traditional cyber crimes are evolving towards social networking. Phishers are moving away from targeting financial sites (35% of identified phishing attempts) and are focusing now more social networking sites (47.8% of identified phishing attempts)[9]. All of these cyber trends show that people in general are becoming more comfortable with using technology.

It is the responsibility of the state to ensure that the users are educated in terms of behaviour on social site or internet use in general. This will not only assist the user to mind their behaviour while online but will further safe-guard the communication infrastructures of the nation.

3.5 Internet Maturity and Living Standards

Over the last decade, many African countries focused on economic growth and overall sustainability. Foreign direct investment increased from US$2.4 billion in 1985 to US$53 billion in 2008, whilst exports from Africa increased significantly. In general, African countries witnessed a period of sustained economic expansion [1].

Similarly, the last decade showed tremendous increase in Internet maturity throughout Africa. Whilst the world average Internet growth between 2000 and 2011 are estimated at

480.4%, Internet growth in Africa has grown by 2527.4% [7]. According to the 2011 Africa Competitiveness Report [16], the three highest-ranked African countries globally in terms of technological readiness are Tunisia (ranked 55th), Mauritius (ranked 61st) and Morocco (ranked 75th). South Africa is ranked 76th. 28 of the 35 African countries are ranked in the lowest-ranked third, and occupy eight of the ten lowest-ranked places overall. These poor rankings are a reflection of the low penetration rates of most ICT tools in Africa. This corresponds largely with the overall global competiveness ranking. Globally, Tunisia is ranked 40th, South Africa 45th and Mauritius 57th. The seven global lowest-ranked countries are from Africa [16], supporting the notion that internet maturity and technological readiness have an indirect impact on rising living standards and sustainability.

3.6 Evolving Targeted Attacks

Since the late 1980s, few mail addresses have not received unsolicited mail from West Africa. Originally, these mails were sent via traditional mechanisms such as post and fax, and later by email. In 2008, about 275 284 complaints with a total loss of US$265 million were received in the United States alone, with victims on average losing about US$931[1]. In 2010, 89.2 billion spam messages were blocked. This number was decreased to 21.9 billion in May 2011, primarily because of takedowns of two major botnets: Cutwailand Rustock [9]. However, criminal attacks are constantly evolving past spam and making advanced use of technology to launch more sophisticated attacks.

Figure 2 shows the different malware threat propagation methods used during the first half of 2011. It is noteworthy that the majority of identified trends (44.8%) require user interaction [9]. These malware types require that the user performs an action for the computer to be compromised, and can relate to Trojan horse infections, common social engineering attack types and inter-fraud schemes.

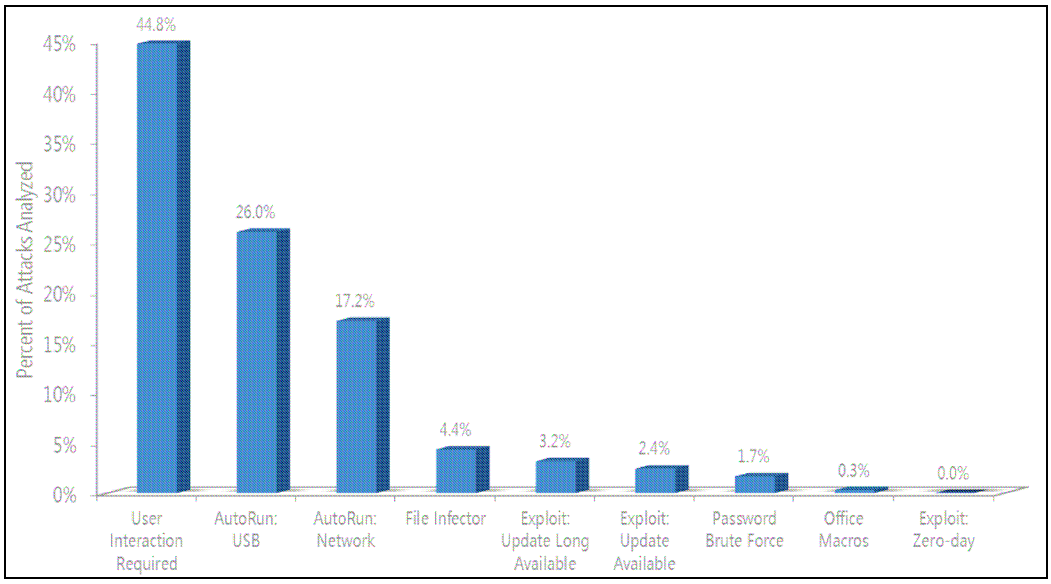

Figure 2: Malware Propagation - First Half of 2011 [9]

In South Africa, more than 4646 online adults fell victim to cyber crime per day in 2010, totalling $573 million in direct financial losses and an additional $995.4 million in time spent resolving the crime. Symantec goes so far to state that cybercrime ($388 billion) costs the world significantly more than the global black market in marijuana, cocaine and heroin combined ($288 billion). Cyber attacks are also evolving into the mobile environment, with an increase of 42% in mobile vulnerabilities from 2009 to 2010 [18].

Table 1 shows the worldwide infection rates for the first and second quarter of 2011. The worldwide average is 9.8 infections per 1000 computers cleaned (CCC). For

comparison, the top 3 ranked countries in the world are compared with the African top 3 ranked countries, and placed against the worldwide infection rate average. The lowest-ranked countries do not have an infection rating due to insufficient data [16] and can thus not be used as part of this comparison. The comparison shows that South Africa is about on par with the global third ranked country, and outperforming the African top ranked country. These figures, however, are not conclusive since many socio-economic factors can have an impact on quarterly figures.

Table 1: Worldwide Infection Rates per CCC [9][16]

Region	Jan – Mar 2011	April – July 2011	Global Ranking
Worldwide	11.0	9.8	Not applicable
Switzerland	3.5	2.8	1st
United States	5.6	5.6	2nd
Singapore	12.6	9.0	3rd
Tunisia	16.0	13.6	40th
South Africa	13.4	10.6	45th
Mauritius	12.0	12.1	57th

Of all the discussed trends, the existence and rate of targeted cyber attacks within a specific can potentially have the greatest impact on a country's global ranking.

4. Recommendations

Despite the impact that each individual trend has on a country's well-being, the combined response to these trends is more significant. This significance arises from the fact that most African countries are classified as developing countries, yet are comparable with the developed countries in terms of digital vulnerabilities, cyber threats and related attacks. In addition, there are many developments and initiatives related to computing (such as bridging digital divides, increasing bandwidth, etc.) that are currently implemented to empower African countries, with less focus on the safety of the users while online. This is one of the areas that increase the exposure of the nation to these cyber threats.

Some of the actions that need to be taken by African countries in response to cyber trends and cyber attacks include the following:

- To conduct cooperative research on these problems with international partners. The direct and effective solution should originate from Africa, in that way it will be easily adapted to the rest of the continent with similar problems.
- Legislation that will monitor the penetration of mobile device needs to be in place.
- Means of empowering and educating the society from all African corners regarding the use of electronic devices and associated risks, and implementing self-defence techniques. This will not only enable the user to mind their behaviour while online, but will further safeguard the communication infrastructures of the nation.
- With regard to bandwidth and internet penetration, South Africa has a major role to play in terms of ensuring the safety of online users of the entire continent. This could be by means of support in security trainings, in preparation to secure users' information and promoting good online behaviour before supplying Internet tariffs.
- Although it is the individual's responsibility to limit the amount of data exposure, it is recommended that all data is treated with integrity, confidentiality and authenticity. All people should be familiarised with the relevant laws and regulations that are associated with electronic data.

It is the responsibility of each country to ensure the security of its citizens. Cyberspace is borderless, therefore, implementing the above recommendations will not only safeguard

users' information and countries' infrastructure, but will be beneficial to all parties involved in cyberspace. Therefore, cooperation, research and appropriate training should be dealt with upfront.

5. Conclusion

This paper has shown that cyber trends are a reality across the globe. Technology, electronic devices and media are used in everyday activities as well as criminal activities. The paper identified and discussed some of the more prominent global trends and showed that these global cyber trends are also a reality in South Africa.

The paper successfully shows that technology within South Africa has advanced to such an extent that cyber trends that are commonly found within higher ranked countries, can also be found within South Africa. It shows that South Africa is not held back in total by traditional technology related hurdles such as lack of connectivity and bandwidth, computer illiteracy, low Internet penetration and inadequate cyber crime related legislation. Rather, South Africa's notable percentage of online activity within the context of the African continent, as well as the drastic increase in Internet penetration in the whole of Africa shows the importance of the cyber domain for Africans. Although some parts of Africa can still claim a clear disadvantage in terms of technology, the Internet and cyber trends, this paper shows that South Africa's specific disadvantage is quickly being diminished. This paper shows that global cyber trends have indeed become a reality in South Africa.

References

[1] Atta-Asamoah, A. 2010. Understanding the West African cyber crime process. African Security Review. 18:4, 105-114.

[2] Blue Magnet. 2011.*South African Internet Statistics 2011 - Put into Global Perspective.* Available from: http://www.bluemagnet.co.za/content/view/87/168/ (Accessed 18 November 2011).

[3] Bosker, B. 2011. *Facebook Pulls A Few Controversional Rape Pages, But Many Remain.* www.huffingtonpost.com/2011/11/09/facebook-controversial-pages_n_1082870.html (Accessed 22 November 2011).

[4] FacebookBloopers. 2011. http://www.facebookbloopers.com/ (Accessed 22 November 2011).

[5] Grobler, M. 2010. Strategic Information Security: Facing the Cyber Impact. http://researchspace.csir.co.za/dspace/bitstream/10204/4507/1/Grobler3_2010.pdf (Accessed 22 November 2011).

[6] Grobler, M. & Jansen van Vuuren, J. 2010. Broadband broadens scope for cyber crime in Africa. http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=5588287 (Accessed 22 November 2011).

[7] Internet World Stats. 2011. *Internet Usage Statistics for Africa.* Available from: http://www.Internetworldstats.com/stats1.htm (Accessed 18 November 2011).

[8] MarkMonitor Security Operations Center.2011. *IP Fraud Intelligence Report.* Available from: https://www.markmonitor.com/download/report/Fraud_Report-Q3_2011.pdf (Accessed 25 November 2011).

[9] Microsoft. 2011. Microsoft Security Intelligence Report. Volume 11. Microsoft Corporation

[10] Muller, R. *State of South Africa's Internet.* MyBroadband.co.za. http://mybroadband.co.za/news/broadband/17987-state-of-south-africa-s-Internet.html, (Accessed 19 November 2011).

[11] OAfrica. 2011.*Mobile Monday's 'Mobile Africa Report 2011'.* Available from: http://www.oafrica.com/mobile/mobile-africa-report-2011/ (Accessed 18 November 2011).

[12] RSA. 2011.*Cyber Security Awareness Month Fails to Deter Phishers.* Available online from: http://www.rsa.com/solutions/consumer_authentication/intelreport/11541_Online_Fraud_report_1011.pdf(Accessed 25 November 2011).

[13] Sapa. 2011. *SA's Labour Productivity At 40-Year Low.* Fin24. www.fin24.com/Economy/SAs-labour-productivity-at-40-year-low-20111110 (Accessed 16 November 2011).

[14] Sapa. 2011. *'Facebook Rapist' appears in Cape Court.* News24. www.news24.com/SouthAfrica/News/Facebook-rapist-appears-in-Cape-court-20111103 (Accessed 22 November 2011).

[15] Schmidt, E. 2010. Eric Schmidt: Every 2 Days We Create As Much Information As We Did Up To 2003. Available from: http://techcrunch.com/2010/08/04/schmidt-data/ (Accessed 22 November 2011).

[16] Schwab, K. 2009. The Global Competitive Report. World Economic Forum: Geneva.

[17] South Africa Web. 2011. *Internet in South Africa*. Available from: http://www.southafricaweb.co.za/page/Internet-south-africa (Accessed 19 November 2011).
[18] Symantec. 2011. *Cybercrime CostSouth Africa $573 Million in 2010*. www.livdigital.co.za/independent/2011/09/08/cybercrime-cost-south-africa-573-million-in-2010/ (Accessed 22 November 2011).
[19] World Bank. 2011. The Africa Competitiveness Report 2011. Available from: www3.weforum.org/docs/WEF_GCR_Africa_Report_2011.pdf (Accessed 17 November 2011).
[20] IT News Africa. 2011. IP Expo: Corporate South Africa looks to the cloud. Available from: http://www.itnewsafrica.com/2011/11/ip-expo-corporate-south-africa-looks-to-the-cloud/ (Accessed 23 November 2011).