CYBERSECURITY IN AFRICA: THE THREATS AND CHALLANGES

Alhassan Tahiru[♣]

Abstract

The world we live in today, has become more complex and more connected than ever before, and this growing complexity and interconnectivity is largely made possible by the forces of modern information, communications and transportation technologies. The world has become a global village mainly because of the rapidity in which socio-economic cleavages are getting interconnected, computers as well as other powerful devices and machines have connected people across oceans. Millions of people all over the world have now become "netizens," a new word coined to denote internet inhabitants. The use of ICTs, and the Internet, has undoubtedly become a matter of strategic importance. Africa's socio- economic political development can be attributed to information communication technology and the "internet of things "(IOT).In as much the internet has been a great pivot and an appetitive drive of all aspects of human life and endeavour, it equally comes with its own associated difficulties, challenges and powerful threats not to only national security but human survival at large.

This paper seeks to critically discuss cyber security in Africa and its accompanied challenges and problems. It further discusses the commanding threats cyber insecurity poses to the Africa as a continent. Relevant analysis is made in other to bring to fore the dire consequences the lack of cyber security mechanism subject a country like Africa, and further plausibly explained the need to protect and guide desirously the internet space of Africa since it is exposed to hazards of many kind.

METHODOLOGY

This paper qualitatively assesses relevant documents and frameworks in relation to this field and other important literatures, to develop an appreciable understanding of both the concepts of Cyber Security and accompanied challenges and threats, to provide a more focused analysis and a basis for this piece of work.

INTRODUCTION

♣ MA Student in Peace and Conflict Studies, Department of International Relations, Ankara Social sciences University, alhassantahir212@gmail.com

The first "electronic mail" was sent in 1971.The children of those scientists now live in a world where almost 40 trillion e-mails are sent a year. The first "website" was made in 1991. By 2013, there were over 30 trillion individual web pages (P. W. and Allan 2014).

Between the space of 40 years, there has been unprecedented participation in the information communication technology in every sphere of our lives. Africa as a continent is indisputably showing good signs of becoming a major player in Information Communication Technology. Possibly because of efforts by governments to cooperate with private and foreign companies in providing ICT infrastructures and digital services to citizens.

This indeed has help Africa to catch up with the rest of the globe in terms of connectivity. The expanding internet user base, fast internet access and the lack of effective cyber security or cybercrime laws is however posing a huge threat to the internet and cyber security space of Africa, which to some has made Africa a new cybercrime harbour. Statistics indicate that Africa is very prone to cyber-related threats due to the high number of domains coupled with very weak network and information security.

This paper discusses the digitalisation of Africa infrastructure systems vis-a-vee the challenges and threats the continent is faced with as far the growing base of internet access is concern. It explores to provide information and depict the clearest picture as to where the African continent stands with regards to cyber security.

For the purposes of comprehensibility, the paper is structured in four major areas, the first part looks at digitisation of State Infrastructures in Africa in which the level of infrastructure and internet connectivity is discussed. The second part encapsulates the phenomena of internet penetration and the expanded user base in Africa in its socio economic and political context.
The subsequent part is the thorough analysis of the challenges and threats the continent faces in cyber space and security, taking a trip into the cyber security documents of African countries coupled with "conventions" made at the continental level. The final part of part of this paper elaborated the strategies to combating cybercrime, and the conclusions part is where he relevancy of this piece of work is reasonably established.

The Digitalization of State Infrastructures in Africa

The African continent has witness a big and tremendous achievements in building ICT infrastructures and internet access in a very rapid pace.From less than 5% in 2007, Internet penetration to 28% in 2015.Substaining this trend means the continent will be comparable and up to par with the develop world in digital connectivity.

Today, wherever one looks, there are new digital resources in Africa: online newspapers, issues of scholarly journals, GIS maps, government documents, archives, and networks bringing online book reviews or e- conferencing. There is a proliferation of online distance learning or "virtual university "packages, some based in Africa. Students everywhere, including in Africa, are embracing new online learning models (Limb 2005; UNESCO 2004) Clearly the Internet Of Things(IOT) has changed the lives of many African citizens relying on the internet to perform daily activities such as education, socializing, communicating or even making money transfers through mobile phones.

In 2007, Africa's first undersea fibre-optic cable infrastructure to connect its eastern and southern parts with the rest of the world was established. Most African countries are now to some extent well-connected, cable wise, giving local ISPs the ability to provide cheaper and faster access types to internet. There is wide range of access services throughout the continent, including dial-up, digital subscriber line (DSL), fibre Enhanced Data rates for GSM Evolution (EDGE), 3G, 4G Long-Term Evolution (LTE), and satellite (cybercrime & cyber security trends in Africa, november,2016).

The West Africa Cable System (WACS), An ultra-high-capacity fibre-optic submarine cable system that links South Africa to Europe, spanning the west coast of Africa and terminates in the United Kingdom was equally developed which seeks to serve majority of western part of Africa.

With the above infrastructures in place, networks have expanded, and thousands of people have join the web of internet. The quest of achieving widespread affordable access to ICT in many parts of Africa is still on course and its excepted to achieve a commanding height in no too distance future. Several other infrastructure development projects are also underway in various parts of the continent. Key Sectors of the African economic infrastructures have been digitalize ranging from transport, energy, manufacturing, communications etc.

In terms of transportation, there has been some important growth of that sector. Transport cooperation's have putting in place digital technologies to ensure safe operations of the transport sectors. Using of advanced digital and software technologies has allowed trains to check the state of rail signals and to intervene when driver acts contrary. In effect, this has given the transport systems a human operators ability to analyse and make informed decisions on time and to anticipate conditions ahead.

For example, in south Africa there has been reshaping in the transport sector with the lunched of a state-of the-art Transport Management Centre (TMC), which is the nerve centre for the management of Bus Rapid Transit (BRT) system. The facility is vital in monitor activities along the transport corridor through CCTV cameras – improving quality of transport and prevent acts of crime. (ADMR,2017).

Kenya is leading the way of making customers and passengers pay transportations through a digital channel. Mobile-money(m-pesa) could be used in paying a taxi ride in Nairobi more easier than it is New York. This is becoming increasingly more accessible and convenience in Kenya causing other countries in Africa to follow suits.

The energy sector has received a fairly face lift of digitization. Electricity supply networks use digital communications technologies like GSM (Global System for Mobile Communications) or PLC (Power-Line Communications) to analyse, detect and react to local changes, are increasingly being incorporated into the African power utilities action plans(Deloitte ,2015) Many African countries have also adopted most efficient payments methods for electricity, ranging from mobile money to internet payments. Ghana, South Africa and other African countries for instance have introduced prepaid metering systems to improve revenue management and financial systems of the energy industries. New technologies have been also introduced to turn wind turbines into more reliable and productive energies. Kenya has the largest wind power project in Africa called the Lake Turkana Wind Power(LTWP), this is to power and distribute generated energies to fulfil diverse needs of citizens.

In the manufacturing industry there has been practical realisation of digitisation. Industries in Africa have resorted to the use of smart technologies, smart plants, smart machines and equipment for efficient processing and supply chain enhancements.

This level of smart technologies has accelerated the overall African Manufacturing Industries, an example of this technology is Siemens' Mind Sphere, which serves as the foundation for digital services such as preventative maintenance, energy data management and resource optimization in many African countries, although awareness of the significance and the potential of this exponential technology is still on a very low rate. (African Digitalization Maturity Report,2017).

The telecommunication sector has seen an explosion of access more than ever before. The number of users has grown tremendously throughout the region, low income countries where telecommunications are hardly accessible are now rapidly catching up with countries with improved communications such as Namibia and South Africa. In 1998, at the begging of telecommunications evolutions, south Africa alone accounted for 86 percent of the regions subscribers by 2008 Nigeria over took south Africa and become the region's biggest telecommunications markets. Networks as it were having been concentrating in urban cities more than rural areas in Africa, as in 2009,90 % of Africa's urban population and 48 % of its rural communities are within the catchments of network coverage.

The internet world statistics reports that; By 2020, about three-quarters of all mobile connections will be on 3G or LTE, and thereafter the impetus will favour LTE as operators are able to make use of spectrum released from the switch to digital TV. Overall forecasts suggest that mobile internet traffic across the region will increase 20-fold by the end of the decade and mobile data revenue in Africa is expected to double by 2019.it is indeed true that the information communications technologies, mobile networks, and internet have been a powerful and essential tool for governments, commerce, civil society and individuals in Africa and in the world as a whole.

Internet Penetration in Africa

In Africa currently more than 650 million unique mobile subscribers, more than 30% of the African population are now using the Internet, more than 120 million people are using Facebook and around 9% are general on social media and is growing each year, with South Africans among the world's leaders in time spent on social networks at 3.2 hours per day . Again, more than 80% of Facebook's users in Africa are visiting the site via mobile devices.

The global share of e-commerce for the Middle East and Africa was expected to rise from 1.6% in 2011 to 2.3% by 2016.

Globally 3.2 billion people are using the Internet by end 2015, of which 2 billion are from developing countries. For every Internet user in the developed world there are 2 in the developing world. (ICT Facts & Figures; the world in 2015) By end 2015, 34% of households in developing countries have Internet access, compared with more than 80% in developed countries. These statistics however show the steadily progress of internet penetration in Africa.in a much such penetration cannot be compared to that of developed country, it is important to note that its quite significant growth than before. Most African countries are still yet to realise high internet penetration, due to political instability or infrastructural challenges Below are the list of African countries with highest internet penetration and biggest internet user base.

The 10 countries with the highest Internet penetration rates are:

1. Morocco
2. Tunisia
3. Nigeria
4. Egypt
5. Kenya
6. Mauritius
7. Senegal
8. South Africa
9. Algeria
10. Uganda

The 10 African countries with the biggest Internet user bases are:

1. Nigeria
2. Egypt
3. Morocco
4. Kenya
5. South Africa
6. Tanzania
7. Algeria
8. Sudan
9. Uganda
10. Tunisia

(Source*; Internet World Statistics: Usage and Population Statistics)*

The high user base and huge internet penetration is good news to Africa. But the lack of effective laws and careful cyber security measures to police the internet space exposes users to several risks and vulnerabilities. Criminals and attackers launch malicious activities without any hesitancy or restrictions since they are unlikely to be apprehended nor prosecuted. Though the wider coverage and faster internet facilities benefit the users and businesses in Africa so it equally benefits attackers and criminals of cyber space.

In the subsequent page we will see the huge and wanton sums of monies Africa countries loose to cybercrime of which these resources could be used in the provision of basic amenities to citizens of the content.

The Threats and Challenges of Cyber Security in Africa

The internet of things (IOT)is becoming reality in Africa, adoption of technology in every sphere of lives continue to grow in a very surprising rate, mobile device ownership and social media use is increasing exponentially. This growing technology and digitization however comes with new risks which potentially undermines growth and achievements made in the internet space. The biggest risks confronting the cyber space is the global rise of cybercrime. The continent's Information Communication Technology's infrastructure has become an attractive target for cyber criminals and hackers.

In 2013, the total global direct cost of cybercrime reached an estimated $113 billion USD. In South Africa alone, 67% of adults reported experiencing cybercrime in the last year, which is estimated to have cost the South African economy $242 million USD. On average, cybercrime cost each cybercrime victim in South Africa US $274 per year. (https://us.norton.com/cyber-security-insights-2016)

Many Africans are still using outdated, or in many cases unlicensed, software. In fact, one of the drivers behind the increasing rates of cybercrime in Africa is the widespread use of outdated or unlicensed software programs. African Countries Lost atleast 2 Billion Dollars to Cyberattacks in 2016.According to the Business Software Alliance's annual Global Software Survey reports that approximately 57% of software used in Africa and the Middle East is unlicensed. Nearly one quarter of users in Africa are currently using the operating system, Microsoft Windows XP which was first released in 2001, and for which software patches were discontinued in 2014.

According to Serianu's Cybersecurity Report 2016, African countries lost at least $2 billion in cyber-attacks in 2016.In East Africa, Kenya recorded the highest losses with $171 million lost to cyber criminals. Tanzania lost $85 million while Ugandan companies lost $35 million. Nigeria lost about $550 million in 2016 alone. Ghana lost $50 million through cybercrime

related issues in 2015.Cote d'Ivoire lost $8,779,070 in 2014 and $ 6,636,530 in 2015., this according to Cisco 2017 Annual Cybersecurity Report.

The figures above shows the alarming and colossal amounts of money the African countries lost and continue to lose to cyber criminals. This by far has some great intended consequences to the economic growth and fiscal stability of many African countries. The continent is somewhat permissive to cybercrime due to poor cyber security capabilities, absence of effective and active legislations as well as lack of general awareness of cyber security measures.

As at September 2012, the top 10 African countries with the biggest number of malware-infections include;

1. South Africa
2. Egypt
3. Tunisia
4. Morocco
5. Comoros
6. Senegal
7. Guinea-Bissau
8. Nigeria
9. Ghana
10. Algeria

South Africa Is reported to be the 3rd highest with respect to cybercrime victims in the world with 80%, after Russia (92%) and China (84%).Findings by the International Data Group Connect; estimates that annually, cybercrimes cost the South African economy USD 573 million. Several commercial banks in Zambia were robbed of more than USD 4 million in the first half of 2013 because of sophisticated cybercrime collaborations between Zambians and foreigners. A 2011 Deloitte Touche survey found that financial institutions in Kenya, Rwanda, Uganda, the United Republic of Tanzania and Zambia had registered losses of up to USD 245 million due to cyber fraud. (Slimani,2016).

The State of Cyber Crime Documents and Legislation in Africa

The Protection of confidentiality, integrity and availability of computer data and systems against cyber-attacks is an essential and critical responsibility of all governments, particularly when ICT has become core potential for human and societal development. Governments cannot remain passive. They have the obligation to protect state structures as well as individuals against cyber crime of any kind.In the light of this, governments are expected to

take active, effective and preventive measures to control, minimize if not totally eliminate cybercrime and its related activities from their respective jurisdiction, though such is far reaching. It is through means of Comprehensive legislation and substantive cyber laws that this could be achieved.

A cursory overview of the 54 countries of Africa in terms of specific criminal law provisions on cybercrime and electronic evidence suggests that by April 2016:
11 States seemed to have basic substantive and procedural law provisions in place (Botswana, Cameroon, Côte d'Ivoire, Ghana, Mauritania, Mauritius, Nigeria, Senegal, Tanzania, Uganda and Zambia) although implementing regulations may still be missing in one or the other country.

A further 12 States seemed to have substantive and procedural law provisions partially in place (Algeria, Benin, Gambia, Kenya, Madagascar, Morocco, Mozambique, Rwanda, South Africa, Sudan, Tunisia and Zimbabwe).

Most of African States (30) did not have specific legal provisions on cybercrime and electronic evidence in force. Draft laws or amendments to existing legislation reportedly had been prepared in at least 15 States (Burkina Faso, Djibouti, Ethiopia, Guinea, Kenya, Lesotho, Mali, Morocco, Namibia, Niger, South Africa, Swaziland, Togo, Tunisia, and Zimbabwe). In some instances, bills had been presented to national parliaments, in others the fate of draft laws is uncertain.

Statistically speaking, 20% of African states have basic legal framework in place.22% have partial legal provisions in place, while 27% have drafts or amendments legislations in place and 31% have no frameworks nor laws in place.

The above statistics is not satisfactory as far as forward match towards combating cybercrime in Africa is concern. This explains the consistent and persistent penetration of cybercrime in the African society, consequently making the continent a haven for cyber criminals. The absence of these laws and practical legislations in majority of African countries only incubate hackers and create fertile grounds for cyber maliciousness to thrive.

Regional and Continental Approach to Cyber Security

African Countries have made attempted efforts to develop a continental and global approach as well as coherent strategy to promote peace and security in the cyber society. Among which include.

1. ***The African Union Convention on Cybersecurity and personal data*** **protection**

This convention seeks to address the legislative challenges and problems African countries are confronted with respect to cyber security, and as well look at the need for Harmonized legislations around Cyber Security and Personal Data Protection in Member States of the African Union. The 23rd African Union Assembly of Heads of State and Government, held in Malabo on 26-27 June 2014 adopted The African Union "Convention *on Cybersecurity and personal data protection"* Which is now known as *The Malabo Convention*.

The Malabo convention calls for the establishment of a Legal Framework for Cyber-security and Personal Data Protection and sets a wide and broad guidelines for subjugation and minimization of cybercrime and its related activities in the continent. It seeks reaffirm commitments of African Union Member States at all levels to build an information society that guarantees a high level of legal and technological security to ensure respect of online privacy and freedoms while enhancing the promotion and development of ICTs in Member States.

2.*Recalling the recommendations of the First Ordinary Session of the STC-CICT-1.*

An Ordinary Session of the Specialized Technical Committee on Communication and Information &Communication Technologies (STC-CICT-1) Was held in Addis Ababa, Ethiopia on August 31ST 31 August to 4 September 2015 to ensure that The African Union Commission follow up of the signing and ratification by Member States of the African Union Convention on Cyber-Security and Personal Data Protection and ; Member states to accelerate the signature and the ratification of the AU Convention, on the development of National Cyber-Security legislations and creation of national and regional Computer Emergency Response Team (CERT) and/or Computer Security Incident Response Team (CSIRT).

These are among others conventions and protocols by the regional body thus Africa Union to engage the attention of African countries to paying attention to the development of measures, policies and strategies to deal with issues of cyber security at regional and continental levels. Even though member states seem to be working on the recommendations but still efforts to win the war on cybercrime in Africa continue to hit a dead end.

CYBER SECURITY AND COMBATING CYBER CRIME IN AFRICA

The threats and risks posed by cybercrime and its related activities threatens the success chopped by Africa as far as the quest to achieve meaningful digitalise heights are concern. Drastic, and calculated measures need to be putting in place in order to nib this teething challenge in the bud minding the fact that significant efforts made.

Cybersecurity and cybercrime cannot be treated as any other rogatory laws particularly when there are clear facts and figures indicating the huge amounts of monies African countries are losing as result of loose measures that has given room and space for cybercrime to thrive. Governments must develop strategies and effective policies to address the emerging security issues associated with the criminal use of the cyber space by way of protecting individual users and critical state infrastructures. Some of these measures needs to be woven into the web of strategies to curtail cybercrime in Africa include.

National Policy

Joint and collaborative measures with stakeholders in cyber industries have the duty to develop a national cyber security policy which recognizes the importance of critical information infrastructures and capable of solving the cyber risks facing the countries as well as outline how objectives of such policies can be achieved.

National Strategy

Adoption of careful and appropriate national strategies towards fighting cybercrime is paramount. African Countries must implement effective national cyber security policy, particularly in the area of legislative reform, development, sensitization and capacity–

building, public -private partnership, and international cooperation among others to achieve the needed results of sanitising the cyber society.

Legislation Against Cybercrime

Effective and efficient legislative and regulatory measures against cybercrime must be enforced by African countries. Clear and substantive criminal offences that affects the confidentiality, integrity, availability and survival of information and communication technology must be encapsulated in legislative instruments.

National Regulatory Authorities

Governments as matter of urgency should confer specific responsibilities on institutions and agencies, either newly established or pre-existing, as well as on the designated officials of the said institutions, with a view to conferring on them an authority and legal capacity to act in all aspects of cyber security issues, including but not limited to response to cyber security incidents, and coordination and cooperation in the field of forensic investigations, prosecution etc. There should be the promotion of technical education and the education of information and communication technology professionals, within and outside government bodies in the area of cyber security and cybercrime protection.

Harmonization

African countries should develop a collaborative and harmonized efforts towards the fight against cyber-crime. such efforts should be woven towards strengthen the possibility of regional harmonization of these measures and strategy. This by far will protect the region in a very broader perspective rather than individual countries taking approaches which is not connected to the general strategy of the continent.

Conclusions

Albert Einstein was quoted as saying "Problems cannot be solved with the same levelA of awareness that created them." The internet has undoubtedly become a matter of strategic importance. A free, open, save and secure cyber space is an engine for economic growth and social development that facilitates communication, innovation, research and business

transformation. The increase in user base, speed internet penetration coupled weak cyber security measures in Africa presents new herculean threats and challenges to the continent.

Cyber security concerns are broader and to some extend complicated national security issue if not carefully handled by duty bearers can planch stable country into many challenges but yet few cybersecurity initiatives and real strategies have been effectively implemented at both regional and continental level.

A strategy and cybersecurity frameworks based on a common approach and common understanding are needed among Member States of the African Union.

The intent and purpose of this paper is to unearth and bring to bear the state of cyber security and cybercrime in Africa. The challenges and threads that is facing the continent which has cause whooping amount of resources going down into the drain due to lack of or loose measures in place as far the protection and preserving the sanctity of the cyber community is concern.

The paper explained the extent of digitisation of state infrastructure in Africa and the level of internet penetration. It gone further to look at the challenges and threats confronting Africa amid growing internet penetration and a transition to a more technology-based continent. Countries with cyber security documents and approach by the regional body thus the African Union in providing solutions to cybercrime is fairly discussed. Lastly measures and possible solutions towards combating cybercrime is equally catalogued and enumerated. Cyber threats represent global problems and they need global frameworks as instruments to promote security and stability in cyberspace

REFRENCES

AU.(2017).*A global approach on Cybersecurity and Cybercrime in Africa* ; retrieved from; https://au.int/sites/default/files/newsevents/workingdocuments/31357-wd-a_common_african_approach_on_cybersecurity_and_cybercrime_en_final_web_site_.pdf on 15th January 2018.

Dall'Omo, S.(2017). *African Digitalization Maturity Report*, Southern and Eastern Africa.

Deloitte (2015). *Sub-Saharan Africa Power Trends: Power disruption in Africa*.Availableat:https://www2.deloitte.com/content/dam/Deloitte/za/Documents/energy-resources/ZA_AfricaPowerTrendsReport_EnergyResources_200515

ICT Facts & Figures, The World 2015 retrieved from; https://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2015.pdf

Kharouni, L.(2013). *Africa A New Safe Harbor for Cybercriminals*? Trend Micro Incorporated Research Paper.

Slimani, M.(2016).*Enhancing Cyber Security in Africa: New challenges for regional Organizations* ?

Symantec.(2017).https://www.symantec.com/about/news/resources/press_kits/detail.jsp?pkid=norton-report-2013

Williams, M.D.J., Mayer, R. and Minges, M.(2016). .*Africa's ICT Infrastructure Building on the Mobile Revolution:*

Yedaly, M. and Wright,B(2016).*Cyber Crime & Cyber Security Trends in Africa*.