International Journal of Social Science Research and Review

http://ijssrr.com
editor@ijssrr.com
Volume 6, Issue 6
June, 2023
Pages: 223-243

Exploring Cybercrime: An Emerging Phenomenon and Associated Challenges in Africa

Witness Maluleke

Associate Professor, Department of Criminology and Criminal Justice, University of Limpopo, South Africa

E-mail: witness.maluleke@ul.ac.za

http://dx.doi.org/10.47814/ijssrr.v6i6.1360

Abstract

This study traces the emergence, highlights the trends, strategies and associated challenges of policing cybercrime in Africa. The researcher also displayed the evolving complexities and escalations of related criminal activities. This qualitative study employed a non-empirical research design: Systematic review methodology to analyse grey literature and primary research studies peer-reviewed and published, restricted from 2002-2021, with non-sequential preference adoption considered. The Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) and Critical Appraisal Skill Programme (CASP) were employed to ensure the trustworthiness of the findings of this study based on reviewed conventional and seminal literature studies on this subject. This study revealed that for a long time in Africa, this crime existed and remains uncoded; however, relevant stakeholders paid limited attention in terms of offering strategies to effectively prevent, combat and investigate this crime, while the documented nature, effects and effects were at maximum scale. Moreover, the associated challenges for policing cybercrime in Africa are currently uncontrollable, as this crime is presently rising beyond unacceptable levels in the cited African countries. The opportunistic organised criminal networks are taking advantage of these existing loopholes. This study concludes and recommends that African countries should realise the importance of efficiently responding to this scourge in the affected countries, the envisaged strategies should be geared towards the African landscape, within a larger global context, while strongly introducing the use of technological advances and improvements, among others. This can aid in the correct usage of computers; staging of the database system; proper facilitation of cybercrime trends; and, surveillance, to eradicate increasing incidences of this crime in African countries. The relevant stakeholders should have access to, and share, information, irrespective of African geographical locations.

Keywords: *Africa; Associated Challenges; Cybercrime; Emerging Phenomenon; Exploring*

1.Introduction

The cited notable researchers (Adams, 2013:29, Bob-Felton, 2006:26, Cassim, 2012:381, Goga, 2014:63, Food Review, 2018:23, Lautier, 2013:71, Kritzinger, 2019:27, Rossouw, 2010:4, Snail & Matanzima, 2014:88 and Young, 2016:32) reached consensus that the world is accustomed to Information Communication Technology (ICT) as it is integrated into individuals' daily lives. The 'cyberspace' is seen as the latest battleground of this digital age. The past three decades, confirms that internet grown into a global network connecting more than 4.5 billion users across the world. These cyber connections are available Twenty-four (24) hours daily, Seven (07) days weekly, while linked through an array of networks, servers and ICT devices. It should be emphasised that cyberspace has no boundaries, laws or enforcement agencies and functions as an independent sovereignty where cyber users (irrespective of their location, culture, language, income or age) are the digital inhabitants. According to African member countries, the most prevalent and pressing cyber threat is online scams.

In particular, banking and credit card fraud is recognised as a serious threat in Africa. It involves the theft of personal data and banking details, which are then used by a threat actor to either purchase goods, siphon funds or sell on markets. Coupled with the Coronavirus disease-2019 (Covid-19) pandemic and its impact on the cybercrime landscape, Africa saw a sustained increase in the volume of cyberattacks, including the 238% rise in cyberattacks on online banking platforms in 2020. At the same time, threat actors in Africa are deploying Trojan information stealers such as Agent Tesla, Lokibot, Fareit and others to commit online scams. Many cybercriminals offer toolkits as a service and training available online has contributed to the continuous operations and development of cybercriminals, considering the broader online scam situation across the African region, data received from the Trend Micro indicates that 27% of its web threat detection in Africa related to online scams in May 2021, International Criminal Police Organisation [INTERPOL] (2021:11). Negatively, the 'cyber space' is becoming a meeting place for criminal groups. This practice as one of the contemporary organised crimes, moreover, cybersecurity concerns are present in all nations, notably; the exact nature of threats differs depending on a country and regional settings. For example; the prevalence of 'cyber espionage' refers to another major threat to national and international cyber security, this threatens various organisations, further branded as a global economic issue, with developing countries such as; South Africa, Zimbabwe and Nigeria often targeted of cybercrimes due to their weak control and security measures (Schoeman, 2017) (in Mpuru, 2017:44).

Mostly, the consulted researchers (Adams, 2013, Bob-Felton, 2006, Cassim, 2012, Goga, 2014, Food Review, 2018, Lautier, 2013, Kritzinger, 2019, Rossouw, 2010:4, Snail & Matanzima, 2014 and Young, 2016) further share that cyber users are spending increasing amounts of time [and money] using internet to connect to cyberspace for work, education, communication and socialising, making a necessity to form part of. However, cybercrime is reported to be spiralling out of control and the extent of losses suffered, coupled with reluctance of companies to take ownership nor responsibilities for security breaches and resultant financial losses to their respective clients, makes a man-in-the street wonder if their monies are safer under his mattress or buried at the bottom of the garden. These practices [Cybercrime and digital espionage] continue to cause massive financial and reputational destruction to many companies. Rarely, a week does not go by without hearing news detailing high profile global firms affected by sophisticated cyberattacks. Certainly, cybercrime in Africa is being taken seriously, however; interception of this crime is not sufficient, calling for law enforcement agencies to proactively prepare for all related method of operations to take a lead in protecting digital assets.

In African context, although the Draft African Union Convention on the Establishment of a Credible Legal Framework for Cyber Security in Africa (AUCLCS) as an African legal framework designed to streamline African cyber security in the 21st century is inducted, it has yet to be seen if this will become another idealistic legal framework that will not be implemented properly. The AUCLCS also

has to overcome lack of consistency with the United Nations Commission On International Trade Law (UNCITRAL) Model Laws as its seems to focus on other aspects of communication regulation such as security and electronic crimes, while failing to cover legal core issues related to and affected by electronic commerce. As a result; different regional developments superseded efforts of African Union (AU) in codifying African cyber law, allowing the public and private sector stakeholders to be exposed to [some] of latest trends in cyber threats from around the world and provides necessary skills, knowledge and insights into some of the technology and expertise required to fight the scourge of cybercrime (Adams, 2013, Bob-Felton, 2006, Cassim, 2012, Goga, 2014, Food Review, 2018, Lautier, 2013, Kritzinger, 2019, Rossouw, 2010:4, Snail & Matanzima, 2014, and Young, 2016). The South African Banking Risk Information Centre (SABRIC) evidenced that "gross fraud losses on South African issued cards increased by 20.5% from 2018 to 2019" with Card-Not-Present (CNP) fraud and banking Malware attacks, behind only Russia. Yet this number fails to take into account the influx of Covid-19 related phishing attempts and the financial, emotional and mental impact they have on victims. Stolen data from carding scams is auctioned off to the highest bidder or sold within underground forums meaning unsuspecting victims of credit card fraud in the African region may have their credit card information misused globally following the breach (INTERPOL, 2011:13).

2. Methods and Materials

This study adopted the non-empirical research design: Systematic review. Dan (2017) states that this research design is adopted to review progress in a specific study field [Exploring cybercrime: An emerging phenomenon and associated challenges in Africa]. While, this research design aim to identify, evaluate and summarise the findings of the reviewed research studies by making available evidence more accessible to decision-makers (Yannascoli, Schenker & Baldwin, 2013) and Bwanga (2020). To develop understanding and obtaining the relevant information on this subject, the collected data stemmed from relevant databases, such as 'Google, Google Scholar, EbcoHost, Emerald Insight, Jstor, ProQuest, Sabinet, Sage Online and Science Direct,' were visited (Maluleke, 2020), this was done following a set of predetermined steps of this research design. The selective keywords retrieved from the research topic were used to obtain relevant information on this subject, using non-probability: Purposefully sampling. The reviewed data were restricted to 2002-2021, not in order of importance and sequence. This was done exercising the exclusion and inclusion criterias of the required data. The PRISMA and CASP were employed to ensure trustworthiness of findings of this study relating to the emergence highlights the trends, strategies and associated challenges of policing cybercrime in Africa.

3. Literature Review and Discussions

3.1 Emergence and Trends of Cybercrime in Africa

In terms of technology and cyber security trends in Africa As in other jurisdictions around the world, Africa is facing a key trend in 'Cyber Security,' namely; the increasing professionalisation of cybercrime. As one of the fastest-growing regions globally, the continent will have 1 billion internet users by the end of 2022. As it is also the world leader in the use of digital money transfers, it is particularly vulnerable to cybercrime, especially as Cyber Security laws and regulations trail those in other countries significantly. According to a report entitled Cyber Crime and Cyber Security Trends in Africa, published by Symantec in 2016, countries throughout Africa are facing massive socio-economic challenges and have neither the time nor the resources to focus on cybercrime. As a result, it is estimated that more than half of the countries in Africa have inadequate Cyber Security laws and regulations, making it a haven for cybercriminals. The rapidly rising number of mobile phones in the region only exacerbates this. Weak and outdated security systems are estimated to cost the continent a staggering United States Dollar [USD]

4 billion [R63 109 640,00] a year, so the time to take planned and concerted action to improve Cyber Security is now (Liquid Cyber Security, 2021).

Furthermore, with internet-connected society upon us, cybercrime is a very real threat to any business or institution, regardless of size or nature of business that has a network, an internet connection and holds sensitive or personally identifiable data (Curtin, 2019:26). The study by (Budhram & Geldenhuys, 2017:9) reveals that the most prevalent economic crimes were asset misappropriation, procurement fraud, bribery, corruption, *cybercrime*, human resources fraud, accounting fraud and money laundering. Apart from cybercrime, the incidence of the other six types was higher than the global average. Cybercrime was on par with the global average. About 60% of participants lost in excess of R500 000 during the reporting period because of economic crime. Accounting and Business Magazine (2019:1), points out that in their rush to embrace the digital future, African entities are leaving themselves dangerously exposed to cyber-attacks. They should join forces to counter the threat. Cybercrimes on businesses and governments are on the rise the world over, and the scale of the problem will only increase as computers and other digital gadgets become more widespread. For African businesses, the risk is potentially even higher. Unfortunately, the rapid increase in internet penetration and digital connectivity, and the enthusiastic embracing of new technologies on the continent, has not been matched by an equivalent commitment to cybersecurity.

In fact, there is evidence on widespread information networks and the development of ICT skills across a broader socio-cultural boundaries open new avenues to prosperity that did not exist many decades ago in many parts of the world, Jegede, Olowookere and Elegbeleye (2016:37). Livingstone (2010) (in Jegede, Olowookere & Elegbeleye, 2016:37) attributed this development to the benefits the new technological order confers on the global community. ICT created new opportunities for self-expression, sociability, community engagement, creativity and new literacies. Nonetheless, it also creates a completely new set of uncertainties for global businesses and other forms of relationship (Salkowitz 2010) (in Jegede, Olowookere & Elegbeleye, 2016:37). Modern technologies exist to target solving all human problems but they still pose enormous threat to the physical and psychological well-being of humans, thereby generating relatively non-predictability of the unfolding scenario (Stivers, 2001) (in Jegede, Olowookere & Elegbeleye, 2016:38). The Advancement in ICT has both positive and negative impacts on society. From the positive standpoint, ICT has contributed to globalisation, with internet becoming central to commerce, entertainment and government. However, despite its benefits, various forms of cyber-related crime, such as identity theft, financial fraud and cyber-bullying, to mention a few have accompanied ICT (Ezeji, Olutola & Bello, 2018:93). These crimes pose enormous threats to several economies and Africa is not an exception (Halder & Jaishankar, 2011:1).

Clearly; cyberspace is emerging as a new battlefield; as cyber-attacks can now complement state conflicts. The recent cyber feud between the United States (US) and Russia, in which the former openly accused the latter of deliberate and orchestrated hacking activities to undermine the integrity of the just-concluded US presidential election, did not come as a surprise. As we witness traditional activities increasingly shifting to this new domain, cyberspace is becoming a focal point, not only for beneficial innovations, enterprises and social networking, but also a site for criminality and warfare. These latter features are reshaping and redefining the digital space as an environment not only for progress and prosperity, but also for cyber threats. Meanwhile, many countries, especially in Africa, are embracing emerging trends in cyber space with little insight as to where certain of the trends may lead. (Ackerman, 2016; and Lewis, 2011) (in Mbanaso, 2016:158).

Expressively, cybercrimes on high profile international companies and organisations are often cited, however, the reality is that there is a steady increase of African organisations falling prey to this crime, frequently motivated by the fact that there is an active and ready black market for data, particularly personal data. Globally, credit card data is worth anywhere between US$20 [R351.62] and USD $45

[791.14] per record [1 US Dollar equals R17,58 South African Rand by the time of compiling this study]. Medical aid information can also be sold, and then used to launch fraudulent medical claims or buy medications to be sold on. The most frequent causes of breaches are accidents and negligence by a company or its third parties, and rogue employees who are looking to gain financially or to damage a company and disrupt its operations (Visser, 2015:1). Considerably, internet is becoming increasingly interwoven in the daily lives of many individuals, organisations and nations. It has largely had a positive effect on the way people communicate. It has also introduced new avenues for business; and it has ordered nations an opportunity to govern online. Nevertheless, although cyberspace offers an endless list of services and opportunities, it is also accompanied by many risks, of which many internet users are not aware. As such, various countries have developed and implemented cyber-security awareness and education measures to counter the perceived ignorance of the internet users (Kortjan & von Solms, 2014:29).

Similarly, criminals have long leveraged the advances of new and evolving technology for gain or profit. The internet, and its emerging information communication technologies, are no different. Both have changed the world of unlawful activity, providing it with a global reach that can touch anywhere in the world. Barriers to illegal cyber enterprises are limited only by access to a computer [or internet] service (Baken & Mantzikos, 2012:27). Likewise, the conceptualisation of cybercrime emerged from a combination of the inception of the internet and the consistent expansion of new technology. Cybercrime has thus resulted in the challenge of addressing old and new crimes facilitated by the use of new technology (Lucks, 2004:34). As clarified by Schell and Martin (2004:225), cybercrime is allied to technology, computers and the internet that causes harm to property and persons. The nature of cybercrime therefore creates opportunities for the relatively effortless commission of covert illicit online activities.

Significantly, Cassim (2011:123) highlights that cybercrime is thriving on the African continent. The increase in broadband access has resulted in an increase in internet users. Thus, Africa has become a ‘safe haven’ for online fraudsters. African countries are pre-occupied with pressing issues such as poverty, the Aids crisis, the fuel crisis, political instability, ethnic instability and traditional crimes, such as murder, rape, and theft. As a result, the fight against cybercrime is lagging behind. The lack of Information Technology (IT) knowledge by the public and the absence of suitable legal frameworks to deal with cybercrime at national and regional levels have compounded the problem. (Snail, 2015:63) states that cybercrime (computer crime) is a new type of criminal activity that started raising its ugly head in the early 1990s, as the internet became a common place for online users worldwide. Computer criminals now have the opportunity to gain access to sensitive information if they have the necessary knowhow. This generally causes huge problems in the economic sphere and results in companies and individuals having to take costly steps to ensure their safety and reduction in commission of cybercrime, it is defined as any criminal activity that involves a computer. It can be divided into two categories:

- The first deals with crimes that can only be committed by computer and that were not possible before the advent of the computer, such as hacking, cracking, sniffing, and the production and dissemination of malicious code.
- The second category is much wider and includes crimes that have existed for centuries but that can now be committed in the cyber environment, such as internet fraud, and the possession and distribution of child pornography. The question then usually arises as to which types of criminal offences may be committed online and which laws one must apply to charge an offender in order to obtain a conviction (Snail, 2015:63).

Additionally, cybercrime is divided into two broad categories of cybercrimes resulting in harm to property and cybercrimes resulting in harm to persons. The former category is commonly carried out using hacking or so-called cracking, for example, computer hacking by criminals, techniques and includes

various crimes such as 'flooding', virus attacks, 'spoofing', 'phishing' and 'phreaking'. These types of crime have a primary goal, which is to cause harm and damage to property by means of destruction, infection, corruption, fraud and theft – all using a computer and the internet as means of perpetration. The latter category deals with the direct harm caused to persons through the commission of illegal activities. These crimes are more personal and often have lasting consequences (Schell & Martin, 2004) (in Sissing & Prinsloo, 2013:15-16).

Correspondingly, Cyber risk (2015:1) shows that the Centre for the Study of Financial Innovation's latest Insurance Banana Skins 2015 survey conducted in association with PricewaterhouseCoopers (PwC), finds cyber risk to be the number one concern for insurers in South Africa, the United Kingdom (UK), and North America. Cyber risk ranked 4th on the combined global survey. Cost of cybercrime suggests that this crime costs Africa billions of dollars annually. For South Africa, it is reported to cost the economy close to R6 billion a year, which is about 0.14% of the national Gross Domestic Product (GDP). The most common threats are from hackers, disgruntled employees, negligence and competitors. *"As recently as 15 years ago, cyber-attacks were fairly rudimentary and typically the work of hacktivists, but with increasing interconnectivity, globalisation and the commercialization of cybercrime there has been an explosion in both frequency and severity of cyber-attacks,"* reveals Allianz Global Corporate and Specialty (AGCS) Africa Chief Executive Officer (CEO), from 2012 to 2017 [Delphine Maïdou]. Cybercrime's footprints across the developing world are getting bigger.

Moreover, due to internet's rapid diffusion and the digitisation of economic activities cyber-crime has gained momentum in developing economies, cybercrimes originating from some developing economies have also opened up new discourses in international relations (Kshetri, 2010:1057). Thus, cybercrime is ubiquitous; companies, governments, banks and even social media have increasingly become the target of data breaches, fraud, malicious communication, cyber pornography and phishing. As security measures are put in place, criminals find more innovative ways to neutralise them. Access to personal data is also used in the run-up to national elections, as the recent use of personal data by 'Cambridge Analytica' from Facebook has underlined. It affected millions of internet users and was one of the biggest privacy violations in social media history (Desai, 2018:150).

Subsequently, Kshetri (2019:77) shares that Africa has been among the fastest growing regions in terms of cybercrime activities. The continent is also a source of significant cyberattacks targeting the rest of the world. However, a number of measures have been taken to address cyber-threats and improve cybersecurity in the continent. Specifically, many countries in the continent have developed legislation to fight cyber-threats. They have also strengthened enforcement measures. Private sector efforts have also been undertaken to strengthen cybersecurity. Chiefly, Yingying and Zhengqing (2016:1) shares that the internet history in Africa is short, but this new technology is spreading fast on the continent. Along with this, cybercrime in Africa is becoming increasingly rampant, while the relevant legal institutions and law enforcement capacity are lagging behind, with public and private cyber security awareness being relatively weak.

Markedly, majority of cybercrime emanates from the African continent and the associated threats spread easily because many computer systems are not properly protected. The fight against cybercrime requires a cohesive and coordinated approach, but in Africa, poverty and underdevelopment are the major causes for growth of cybercrime in the region. The potential for internet abuse in Africa is also high. This is due to the lack of security awareness programmes or specialised training for the law enforcement agencies. Many watchers are warning that Africa is becoming a major source of cyber-crimes; for example, Nigeria is ranked as the leading State in the region as the target and source of malicious internet activities; and this is spreading across the West African sub-region. Cybercrimes are crimes committed on the internet using the computer as either a tool or a targeted victim. Cybercrimes involve both the

computer and the person behind it as victims, depending on which of the two is the main target. Hence, the computer could be looked at as either a target or a tool. For example, hacking involves attacking the computer's information and other resources. When the individual is the main target of cybercrime, the computer can be considered as the tool rather than the target. These crimes generally involve less technical expertise as the damage done manifests itself in the real world and human weaknesses are generally exploited (Quarshie & Martin- Odoom, 2012:98). Cybercrime can assume various forms and the way hackers can capture information differs widely: identity theft, phishing emails which attempt to lure customers into clicking on attachments which then give the hackers access to account and personal information and ransomware, where files are encrypted and rendered unusable until an affected user pays for their 'release'. The use of data in innovative and clandestine ways is the leitmotif of the digital economy and give rise to terms like 'surveillance capitalism and platform capitalism' (Davies, 2018:20).

Comparatively; Yingying and Zhengqing (2016:3 & 4) provides that by the end of June 2014, African countries that have higher internet penetration rate include Madagascar (74.7%), Mali (72.1%), Malawi (70.5%), Morocco (61.3%), Seychelles (54.8%), Egypt (53.2%) and South Africa (51.5 %), which are all higher than that (47.4%) in the same period in China. But Africa is also the continent that has largest number of countries whose internet penetration rate is less than 2%, including Ethiopia (1.9%), Guinea (1.8%), Niger (1.7%), Sierra Le one (1.7%), Somalia (1.6%). Another feature of African internet development is that the mobile terminal is the main access route. Most places in Africa have not experienced fixed line network in the development stage and have directly rushed into the mobile internet era, and the majority of Africans use the internet for the first time through their mobile phones. This is related to factors like the continent's unique geographical environment, underdeveloped land cable, unstable power supply and lower price of mobile than that of Personal Computer (PC) and so on. At present, Africa has the most rapid growth in the global mobile internet. Data from the International Telecommunication Union (ITU) shows that from 2011 to 2014, the growth of mobile internet subscribers in Africa went over 40%, which is twice than that of the global average level; in 2014, fixed line internet penetration rate in Africa was only 0.4%, while Africa Mobile internet penetration rate grew from 2% in 2010 to nearly 20%.

Recently (2019), According to the British Consulting Firm Ovumone [Sa] (in Kshetri, 2019:7), a billion people in Africa will have internet access by 2022. Analysing the trend of cybercrimes across countries, analysts have suggested 10-15% internet penetration as the threshold level for the generation of significant hacking activities (Kshetri, 2013). Internet penetration rates in many African economies have already reached this level. It is noted that *"cybercrime is shifting towards the emerging economies. This is where the cyber criminals believe the low-hanging fruit is".* Unsurprisingly many African economies have become important sources as well as victims of cyber-threats. Identically; Accounting and Business Magazine (2019:1) reports that according to the Kenyan-based IT and Business Advisory Firm *[Serianu]*, cybercrimes cost African economies $3.5 [R61 645 850 000,00] billion in 2017. In that year, annual losses to cybercrimes were estimated for Nigeria at $649 [R11 424 768 850,00] million, and Kenya at $210 [R 3 696 333 900,00] million. Likewise, according to the SABRIC, South Africa loses $157 [R 2 763 449 630,0] million annually to cyberattacks (Kshetri, 2019:7). Twelve African countries with the most infected IT infrastructure are: Libya (98%), Zimbabwe (92%), Algeria (84%), Cameroon (83%), Nigeria (82%), Ivory Coast (81%), Kenya (78%), Senegal (78%), Tunisia (74%), Morocco (66%) and Mauritius (57%). The net result is that the African continent has become a nest of cybercriminals of all kinds … Other criminals operate on a larger scale, using sophisticated crime networks. Notably, three African countries are among the world Top 20 countries with the highest ratio of computers infected by *Malware*, namely: Somalia - 6th, Algeria - 14th and Rwanda - 16th (SciDev.Net, 2020:1).

The numbers provided by the 'Cybersecurity Venture' Annual Crime Report [ACR] (2019) (in Crane, 2019:1), is double [Cybercrime damages are anticipated to cost $6 trillion -R 106 015 800 000 000,00 - per year by 2021], compared to their 2015 prediction of $3 - R53 066 250 000 000,00- trillion in

cybercrime costs annually in a global scale [African countries included]. Another report *'Serianu'* estimated the loss to African businesses from cybercrime at US$3.5 billion [R 62 022 450 000,00], up from USD $2 billion [R35 479 720 000,00] in 2018. Nigeria was the hardest hit with losses of US$649 million [R11 513 169 140,00], followed by Kenya with US$210 million [R3 725 370 600,00] and Tanzania with USD $99 million [R 1 756 246 140,00]. Meanwhile, more than 95% of public and private organisations across the continent spent less than USD $1,500 million [R 26 645 805,00] a year on cybersecurity measures, with Small and Medium-sized Enterprises (SMEs) in particular failing to invest, the *Serianu's* Africa Cyber Security Report (2017) (Accounting and Business Magazine (2019:1), approximately 96% of cybercrime incidents in Africa go unreported or unsolved, thus, the vulnerability of African businesses to cybercrime is clearly acknowledged, further rendering it a mounting concern.

Surely, in Nambia, the Namibian Electronic Transactions and Communications Bill is presently being tabled before the Namibian parliament. Namibia has also experienced misuse of ICTs such as identity theft and the use of pornographic images on cell phones; hence the need for such legislation. In Botswana, although the incidence of cybercrime is low, it is said to be increasing. Initially, the general criminal law applied to cybercrime cases. However, legislation has now been introduced to address cybercrime. The Cyber Crime and Computer Related Crimes Act (No. 22 of 2007) was passed in December 2007. The aim of the law is 'combat cybercrime and computer related crime, to counteract criminal actions perpetrated through computer systems and to facilitate the collection of electronic evidence 133. In Zambia, ignorance has been mooted as one of the main reasons why many African people fall victim to online frauds. Therefore, the Zambian government is trying to educate consumers about cybercrime. It has introduced the National Policy Framework on Cyber Crime, which criminalises cyber security criminal activities and computer misuse offences. However, this country has been criticised for lacking skills, equipment and organisational abilities to fight cybercrime (Cassim, 2011:134).

Specifically; Correia (2011:69) presents that from 2011; Angola went through major revisions of bringing laws in line with the new Constitution adopted in February 2010. These laws dealt with new realities such as age of the information society. In this country, laws are often approved in 'packages' of related Bills. The ICTs related package came before parliament in May 2011, containing a Bill seeking to criminalise daily activities using internet and ICT equipments. Opposition to this Bill spearheaded by the *Sindicato de Jornalistas Angolanos* [SJA] (I.e. Angolan Journalists' Trade Union) managed to get the Bill chucked out of the package, which went through without it. They were specifically concerned with the provisions in Article 17 as the biggest threat to freedom of the media and the work of a journalist. Article 17 is indeed unfathomably draconian. It criminalises the use of any recorded material without the express permission of those on it. Therefore, no sound bites no photos at events, no video material.

Truly; as debated in 2011; the Angolan Law on Combating Crime in the Domain of Information and Communication Technologies and on Information Society Services, is part of a package of laws on ICTs, together with the Law on Electronic Communications and Information Society Services and the Law on the Protection of Personal Data. This Bill highlights the lofty ideals it aims to protect and makes the right noises about protection of copyright and combating child pornography. However, beneath the veneer, the real intent of the law is quite apparent. In their eagerness, the drafters elevated it above the Penal Code, stating in Article 6 that provisions in the Penal Code also apply to ICT crimes, *"provided they do not contradict"* the provisions of this Bill. Article 79 states that all legislation contradictory to the provisions of the bill are henceforth repealed. Interesting, as quite a few provisions are in conflict with the Constitution, as pointed out during the debate to block the Bill. This Bill targeted primarily legal persons, which makes sense, as most people do not have internet at home (Correia, 2011:70).

Considerably, State institutions are exempt from the law and to add injury to insult, criminal investigators of the police and the judiciary (Angola has an inquisitorial legal system) enjoy carte blanche to search and confiscate data and in some cases even delete it without due oversight. Penalties range from

a few days to years, with most often eight or 12 years - three times that in the case of terrorist organisations. Fines are calculated based on potential monthly earnings. Someone earning R15 000 a month, sentenced to eight years, would have to pay a fine of R1.45 million. A legal person will be fined three times that - R4.3 million. Besides the astronomical fines, a company can have its operations suspended or even closed down or have its assets sold to pay the fines – and the owners will still be responsible for paying salaries while out of business. Article 4(b) makes bosses responsible for the cybercrimes committed by their workers if this happens because of 'lack of surveillance' (Correia, 2011:70).

Equally, Cassim (2011:134) presents that in East Africa, Kenya enacted cyber legislation to combat cybercrime during 2009. The Kenyan Information Communications Amendment Act 2009 was passed by the Kenyan parliament and signed by the President during January 2009 and addresses cybercrime in sections 83 W-Z and 84 A-F. These sections deal with, *inter alia*, unauthorised access to computer data, access with intent to commit offences, unauthorised access to and interception of computer services, damaging or denying access to computer systems, unlawful possession of a device and data, electronic fraud, tampering with computer source documents and publishing obscene material in electronic form. In Uganda; this country has been criticised for its inability effectively to address cybercrime because of its inadequate infrastructure and poorly trained prosecution and law enforcement personnel. Criticism has been levelled in the following areas: *Uganda does not have adequate forensic labs for its cybercrime investigators. Prosecutors also lack proper training in cybercrime issues and this could hamper effective combating of cybercrime and Uganda may also become a cybercrime haven as the country cannot offer other countries mutual legal assistance with regard to cross-border crime.* In Rwanda; Rwanda has also prepared draft information, communication, and criminal law Bills on cybercrime. The Bills cover e-signatures, consumer protection, privacy and content legislation. Bills on digital copyright and electronic-contracting have also been tabled before the Rwandan parliament.

In West Africa, Nigeria, There is currently no specific legislation to combat cybercrime. Most cybercrime takes place at internet access points or cyber cafés, which makes cybercrime difficult to prove, Nigeria has received worldwide attention and notoriety because of the Nigerian '419 scam' which involves a 'confidential' electronic-mail from a prominent Nigerian who wants assistance to transfer 'ill-gotten funds' offshore. This practice continues to net hundreds of unsuspecting victims every year. The 'Yahoo boys' are behind the 419 scam or advanced fee fraud. The lack of proper law enforcement and the lack of training and expertise of police officers has compounded the problem. A call has been mooted for specifically trained cyber police, the introduction of an expert body, and a comprehensive law to combat such crime, and the establishment of a comprehensive forensic commission to train forensic personnel and in Cameroon: The Economic Community of West African States (ECOWAS) has also met to discuss, inter alia, the implementation of ICT policy and legislation, access and interconnection regulation, universal access, and to provide guidelines for the gradual transition to open markets. A Bill on cybercrime and cyber security has also been tabled before parliament, to address the increase in hacking and scams on the internet, Cassim (2011:137).

In particular, Kshetri (2019:77) shares that increasing cyberattacks in the continent can be attributed to vulnerable systems and lax cybersecurity practices. According to Business Software Alliance, two countries with the world's highest software piracy rates in 2017 were from Africa: Libya and Zimbabwe. The proportions of unlicensed software in the two countries were 90% and 89% respectively. Since pirated software products cannot take advantage of updates from manufacturers, they accelerate the spread of Malware. Even financial institutions, which face biggest cyber-threats, lack proper cybersecurity practices. One study in 2009 showed that 60% of Kenyan banks had insecure systems. According to Deloitte study (2011) (in Kshetri, 2019:77), only 40% of banks in Kenya, Uganda and Tanzania were prepared against cyber threats. Another survey conducted among banks in Kenya,

Rwanda, Uganda, Tanzania and Zambia revealed that banks were at high risk from threats, such as hacking, employees with poor sense of security, malicious insiders.

To this course, the African continent faces a severe shortage of cybersecurity work force. It is estimated that Africa will have a shortage of 100,000 cybersecurity personnel by 2020. Just like in the BRICS (Brazil, Russia, India, China, and South Africa) countries, African economies have faced economic and institutional barriers in developing cybersecurity workers. For instance, Cameroon which is among the countries worst affected by cybercrime in Africa, was reported to be facing a dilemma to take measures to address the problem. It was reported in 2016 that policy makers were in the process of launching cybersecurity skill development programmes. Policy makers, however, feared that after completing the training program, the trainees could use the skills gained to commit cybercrimes (Kshetri, 2019:78).

In Nigeria; undoubtedly, the liberalisation of telecoms and internet penetration policies of government have yielded un-precedented growth in ICT, leading to increased dependence on technology for the delivery of basic as well as critical services in Nigeria amongst citizens, businesses and governments. A cybersecurity framework is therefore inevitable to compliment these great strides by government, secure, protect the underlying ICT infrastructures, and boost consumers' confidence as well as the public. Cybersecurity is a reality that has to be dealt with now, as it would determine how we are conceived in a global village. Today's world is in an important evolution such that physical transactions in all spheres of everyday life will be done online from bank transactions to controlling our hybrid power generating plants, and so on. Thus, there is a need for a cyber-activities regulation that safeguards Nigerians within and foreigners interested in investing in Nigeria (Olayemi, 2014:123). This keep evolving in this country and taking newer dimensions as its perpetrators encounter newer challenges in the crime system. Beyond the basic conning of people's financial assets, organization's data and intellectual properties, the fortification of some Nigerian cyber fraudsters has grown beyond the basics of intellectual smartness and creativity (Nnanwube, Ani & Ojakorotu, 2019:55-56).

Similarly, Cassim (2010:118) highlights that in South Africa; the Electronic Communications and Transactions [ECT] Act (No. 25 of 2002) was introduced to address *inter alia* cybercrime in South Africa. The primary objective of the Act is 'to facilitate and regulate electronic communications and transactions ... To this end this Act makes provision for every conceivable aspect pertaining to the electronic environment,' Jansen (2002:17). Furthermore, it is made clear from the outset that the implementation of an infrastructure, which facilitates, electronic transactions will be geared towards the public interest. Emanating from the fact that the South African common law has proven to be ineffective in addressing cybercrime. Consequently, (Snail, 2015:69) reveals that most of the provisions on cybercrime in the ECT Act, 2002 are noble endeavours, but their enforceability is still to be tested in our courts. Given the borderless nature of the internet and the challenges that it poses in terms of jurisdictional questions, international co-operation and uniformity, it is important that states learn from one another's efforts to deal with cybercrime and create an international cybercrime code to be applied universally if any significant success is to be achieved in combatting cybercrime.

Notably, (Moneyweb's Personal Finance, 2006:11) shares that all of South Africa's big four banks confirmed incidents where clients lost amounts ranging from tens of thousands of rands to R180, a few times over, after thieves accessed their internet bank accounts. In most cases, the clients had not adhered to security recommendations from banks. However, security precautions change regularly as banks aim to keep a few steps ahead of thieves, so it is not surprising so many clients were caught off guard. Not even private banking clients can bury their heads in the sand when it comes to internet banking. Most private banks in South Africa are connected to the retail banks: the technology is the same, as are the minimum-security requirements. Electronic banking is cheaper and more efficient than old-fashioned forms of banking, like standing in the queue in the bank hall or writing out cheques, so it is

here to stay. The bottom line is you have to keep up to speed with developments – or you run the risk of losing money without losing your wallet. As a recourse; the country also adopted the Council of Europe's Convention in Cybercrime, however, it has not ratified the treaty, propelling other researcher to suggest that this country should ratify the treaty to avoid becoming an easy target for international cybercrime (Cassim, 2010:118). Dlamini and Mbambo (2019:5) citing McNamara (2012) confirm that cybercrime is prevalent in South Africa and external attacks are on the rise causing damage to companies and organisations. There are cybercriminal organisations in South Africa that engage in causing damage to individuals, Organisations and government in the form of extortion, blackmail, spreading of viruses, malware and ransom. Many corporations and government infrastructure have poor security control regarding cybercrimes.

3.2 Strategies and Associated Challenges of Policing Cybercrime in Africa

Kshetri (2019:79) suggests that several initiatives have been launched and carried out at various levels to improve the continent's cybersecurity landscape. The most important of these is improving regulatory quality. According to a November 2016 report of the African Union Commission (AUC) and the cybersecurity firm Symantec, 11 countries in the continent had specific laws and provisions in place to deal with cybercrime and electronic evidence: Botswana, Cameroon, Côte d'Ivoire, Ghana, Mauritania, Mauritius, Nigeria, Senegal, Tanzania, Uganda and Zambia. Additional 12 countries had taken at least some legislative measures, albeit limited. Draft cybercrime laws had been prepared in many other countries and Bills had already been presented to national Parliaments in some of the countries. As of November 2018, Kenya's new data protection Bill was ready for review in the Parliament. On the plus side, this Bill had many elements of Europe's General Data Protection Regulation (GDPR).

For instance, this Bill required organisations to inform users on reasons of data collections, for what purpose that data is used and how long the organisation would store the data. This Bill also has a provision, which gives consumers the right to request organisations to delete their data. In addition, it requires organisations to have a certain level of security standards for storing data. Some analysts expressed concerns about the data localisation provision, which makes it illegal to send Kenyans' personal data outside the country. Critics have argued that if this provision is implemented, the Kenyan economy will not be able to benefit from the economic gains that arise from cross-border data flows. Furthermore, there are also sector-specific regulations. For instance, banking and financial institutions are the most affected sector. In October 2018, the Bank of Ghana issued a Cyber Security Directive for Financial Institutions. The Directive requires active involvement of senior executives and the board to strengthen cybersecurity. All banks in the country are required to appoint a Cyber and Information Security Officer (CISO) who would advise senior management and the board on cybersecurity issues, and formulate adequate measures to manage cyber and information security risks, Kshetri (2019:79).

The Central Bank of Nigeria (CBN) announced that it was developing a risk-based cybersecurity framework for banks and financial institutions. The idea in this framework is to identify the existing gaps and address them. In August 2018, the Central Bank of Kenya asked the country's payments service providers to submit their cybersecurity policies to the government. Many African economies have also strengthened enforcement measures. In 2017, South Africa's Information Regulatory Authority started the investigation of that year's biggest data breach in the country, in which more than 60 million people's personal data were stolen. The agency also made formal requests to the concerned companies to provide explanations, Kshetri (2019:79). Kshetri (2019:80) went on to reveal that private sector cybersecurity initiatives have also become prominent. In early 2017, the *Serianu* established what it calls a Cyber Immersion Centre in Nairobi. The Centre provides an environment for firms to experiment and test their cybersecurity capabilities. It also provides educational facilities to develop cybersecurity professionals. A similar centre was opened in Mauritius in mid-2017. Foreign multinationals have also worked with local organisations to help consumers understand cybercrimes and help develop ethical standards. For instance,

Microsoft teamed up with Paradigm Initiative Nigeria (PIN) to educate Nigerians on cybercrimes and to create economic opportunities. The country's EFCC announced in October 2009 that it shut down about 800 websites associated with cybercrimes and arrested. Generally, the enforcement of international law is ineffective (Brunnée, 2006) (in Siljeur, 2016:99).

Africa countries struggles to enforce its international law obligations in their respective domestic arenas. Investigating, deterring and imposing legal sanctions on cyber-criminals warrants an international legal framework for the investigation and prosecution of cybercrime. Law-enforcement officials cannot ignore the real-world limits of local, state and national sovereignty and jurisdiction. It can be a strenuous task to obtain information from foreign countries, especially on an expedited basis – more specifically when the other country is in a different time zone, has a different legal system, does not have trained experts and uses different languages. The challenges presented by the electronic realm cannot be solved merely by imposing existing criminal and criminal procedural laws, which govern the physical world on cyberspace. The electronic realm does not necessarily demand new laws, but it does require that criminal actions be conceptualised differently and not from a purely traditional perspective. Sovereignty and the principle of non-interference in the domestic affairs of another state are fundamental principles grounding the relations between states; they constitute an important mechanism in the armoury of criminals. The harmonisation and enactment of adequate and appropriate trans-border coercive procedural measures consequently play a pivotal role in facilitating effective international cooperation (Basdeo, Montesh & Lekubu, 2014:48 & 49).

In addition, Atta-Asamoah (2009:112-113:2009) mentions that a review of the scamming process provides important insights and entry points for curbing this type of crime. In the first place, it is clear that many internet users expose themselves to defraud electronic-mails (e-mails) by responding to calls to complete forms, by circulating e-mails, or by subscribing to e-mail alerts from untrustworthy websites, purely because of ignorance. Second, with increasing practice, the nature and methods of defrauding are rapidly evolving in sophistication. The more sophisticated scammers become, the more difficult it is to curb their activities. It is important that actions aimed at curbing the crime takes into account four (04) main strands of activities, namely: *Education* (internet users, particularly in developed countries, should be educated about the *Modus Operandi (MO)* of scammers and the dangers associated with visiting sites with malicious content. This will help reduce the susceptibility of internet users to harvesting and the likelihood of falling prey to scammers), *Web-based snare programmes* (One important deduction from the scamming process is that with an organised technology based approach, scammers can be trapped. This could be achieved by initiating web-based snare programmes using undercover investigators who will pose as victims.

Through undercover operations, ringleaders in the scamming cycles can be busted thereby reducing their activity), *International cooperation* (A call for strengthened collaboration and cooperation among security agencies in countries of both the victims and the perpetrators. Given the trans-border nature of the crime, it is also important that Interpol consider giving greater attention to it. International cooperation and the involvement of Interpol will help to bridge the distance between scammers, victims and law enforcers in fighting the crime), *Institution of appropriate legal framework* (To provide the framework for collective action, African countries need to harmonise cyber-related laws with which the crime can be prosecuted in the individual countries and regionally. The responses of countries in the region should be as even as possible in order to curb the redistribution of the menace through the relocation of criminals across borders). There are various laws dealing with cyber security, some with overlapping mandates administered by different government departments and the implementation of which is not coordinated (Mangena, 2016:33).

Strategically; multi-national international organisations, such as the International Criminal Police Organisation (Interpol), the Commonwealth of Nations, the Group of 8 (G8) and the Organisation for

Economic Co-operation and Development (OECD), all play pivotal roles in addressing cybercrime and their work encompasses a broader territorial environment. The Interpol has also provided technical guidance in cybercrime detection, investigation and evidence collection. The enactment of the Council of Europe's Convention on Cybercrime (COECC) is also lauded because it attempts to establish consistency in the cybercrime laws of many countries. However, many states still have to sign let alone ratify the Convention to serve as a deterrent. The unanimous participation of all nations is thus required to achieve meaningful prosecution (Cassim, 2010:122). Whereas; Mahlobo (2015) (in Dlamini & Mbambo, 2019:5 & 6) share that the Minister of State Security identified the security of cyberspace as one of government's five strategic objectives in the Department of State Security. This department is tasked with improving the Criminal Justice System (CJS), border management, domestic stability and reducing corruption. This 'Minister' also outlined a list of cybersecurity priorities to assist in the policing of cybercrimes, namely: *The need for better approaches to authenticate hardware, software, and data on computer systems and to verify user identities and the creation of methods of monitoring and detecting security compromises. The need for a holistic approach in the fight against cybercrime. An evaluation of the influence of laws and regulations on the use or abuse of electronic information. Increasing the awareness of cybercrimes and Cybersecurity. The understanding of social media networks risks and corporate espionage.*

Certainly, in view of the findings of this study, the researcher advanced number of recommendations. Firstly, proactive and intelligence-based policing should be adopted with regard to the prevention of cyber-related crime in South Africa. It is necessary that the criminal justice system improve the training of officials who would be able to prevent cyber-related crime, as the crime may be perpetrated from any cyber system in the world. South Africa should develop and enhance cyber-intelligence and cyber security measures in order to predict cyber-related threats and deter cyber criminals. Training should be initiated at local police stations to ensure that police officials, from early entry constable, acquire basic cyber-related crime skills; skills, on how to identify, categorise and open dockets for cyber -related crime offences. There should be public/private and government collaboration in the area of cyber-related crime prevention in South Africa (Ezeji, Olutola & Bello, 2018:108).

Consequently, 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? 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, South Africa [African continent in large] wishes to promote a culture of cyber-security among its citizens. Cyber security awareness and education together play a big role in cultivating such a culture. Accordingly, cyber-security awareness and education framework that would assist African countries in promoting its envisaged cyber-security culture. The implementation of this framework would afford these countries cyber-security awareness campaigns. Furthermore, making use of its subsidiary campaigns would mean that South African citizens could be the recipients of cyber-security awareness and education, suited to a South African audience (Kortjan & von Solms, 2014:39).

Eventually, the information management strategies include the different ways in which information or intelligence may be managed and analysed to achieve a specific result. To stay ahead of trends, it is crucial for security practitioners (police officers and private security officers) to take a proactive approach towards security related information. For security information to be successfully managed, it is necessary that security information be lawfully collected, and analysed, using the correct analytical methods and then effectively applied as strategies to combat crime and prevent losses. *Cyber-crime*, property related crimes, corruption, organised crime and transnational organised crime, require law enforcement and private security to respond with information management strategies. Information management strategies are central to the task of combating crime and preventing losses. Analysed data

related to the vulnerability of a target and the modus operandi, presents the opportunity to address the exploited weaknesses of an asset/victim (Govender, 2012:81 & 95).

In general, the immediate priorities as highlighted by the 'Minister' in question; included the enhancement of institutional the cybercrime and Cybersecurity capacity, the finalisation of national Cybercrime and Cybersecurity policy and legislation, the promotion of partnerships for public cybercrime awareness campaigns, strengthening cooperation with South African Development Community (SADC), AU and BRICS partners, and the establishment of a Cybersecurity Centre. Therefore, it is evident South Africa [and other affected African countries] has made significant strides towards policing cyberspace. However, achieving a safe cyberspace, through implementation of policies and strategies of policing cybercrime is a great challenge. Cybercrime with its complexities has proven difficult to combat due to its nature. Extending the rule of law into the cyberspace is a critical step towards creating a trustworthy environment for people and businesses. Since the provision of such laws to effectively deter cybercrime is still a work in progress, it becomes necessary for individuals, organisations and government to fashion out ways of providing security for their systems and data. To provide this self-protection, individuals, organisations and government should focus on implementing cybersecurity plans addressing people, process and technology issues, more resources should be put in to educate and create awareness on security practices. Therefore, there is no one measure that will cure the menace of cybercrime and ensure cybersecurity. However, it is the combination of measures together with the sincerity and rigour with which they are implemented and administered that will serve to reduce risks most effectively and efficiently. In addition, the fight against cybercrime and cybersecurity threats in Nigeria [other African countries included] requires not just knowledge of Information Technology but Information Technology intelligence on the part of all citizens (Olayemi, 2014:123).

Moreover, a dire need also arises for the introduction of more specialised institutions such as specialised cyber tribunals or courts to facilitate the prosecution of cybercrime cases on a priority basis. The internet users should also be encouraged to share the burden of securing informational privacy where feasible. Computer ethics education should also be taught to children in schools to educate them about the negative consequences of committing cybercrime. Although technological advancement is welcomed, it has created numerous challenges. The possibility of new forms of cybercrime will emerge with rapidly evolving technology; therefore, new cyber laws should be introduced to respond to these rapid changes. Thus, there should also be continuous research and training of Information Technology (IT) security personnel, finance service sector personnel, police officers, prosecutors and the judiciary to keep them abreast of evolving computer technology. At the end of the day, a balanced approach that considers the protection of fundamental human rights and the need for effective prosecution of cybercrime should be prioritised (Cassim, 2010:123).

Subsequently, Kritzinger and von Solms (2012:1) indicates that out of the top ten countries in the world with high levels of cybercrime prevalence, sub-Sahara Africa is host to four of these countries (Nigeria, Cameroon, Ghana and South Africa). The main reason forwarded for the increase of cybercrime particularly in Africa is the sudden increase in the use of ICTs in a number of African countries. The Global Information Infrastructure creates unlimited opportunities for commercial, social and other human activities. However, it is increasingly under attack by cybercriminals; as the number, cost, and sophistication of attacks are increasing at an alarming rate (2014). Cyber threat is a big issue in Africa. A lot of cybercrime emanates from the continent, and threats spread easily because many servers and computers are not properly protected. Africa, as a continent, is vulnerable to a range of online criminal activities, including financial fraud, drugs and human trafficking, and terrorism (Quarshie & Martin-Odoom, 2012:98).

With the given background, cybercrime differs from traditional crimes. It can be committed easily, it requires few resources, and it can be committed in a specific jurisdiction without the offenders

being physically present there. Cybercrime does not require physical proximity between a victim and perpetrator. This compounds the problem of detection. Criminal laws regulating cyberspace tend to result in few prosecutions due to the jurisdictional difficulties and additional resources required in tracking down cyber criminals in different countries. The fact that African countries have long and permeable borders, compounds the problem of detection The international character of cybercrime has created problems as illustrated by the 'love bug' virus which demonstrates that the existence of cybercrime laws is a fundamental prerequisite for investigation as well as prosecution … The failure to have adequate legislation reverberated around the globe and illustrated the vulnerability of our modern networked society. Therefore, the international character of cybercrime calls for international coordination and cooperation to address computer-related offences worldwide. Police officials cannot prosecute cyber criminals unless countries have adequate laws in place outlawing such criminal activities (Cassim, 2011:125).

Accordingly; Kritzinger and von Solms (2012:2) reveal four different types of cyber problems in an attempt to address the worrying question of cybercrime in Africa, namely: *(1) Lack of Focused research in cyber security*, these authors argue that a number of cyber factors have led Africa to becoming a cybercrime hub. Their assertions are supported by Von Solms and Kritzinger, 2010) (in Kritzinger and von Solms, 2012:2-3) by indicating the following factors: ***1)*** *Increasing bandwidth, Increasing use of wireless technologies and infrastructure, Lack of cyber security awareness, Ineffective legislation and policies, and Lack of technical cyber security measures*, ***2)*** *Lack of a proper integrated framework on legal and policy aspects*; The problem in cybercrime in the African continent identifies loopholes that exist among different stakeholders in the war against cybercrime; ***3)*** *Lack of Cyber Security Awareness and Regulation;* this problem addresses mainly the aspects regarding cyber awareness and regulation. The concerning factor rests on awareness created or lack of it about cybercrime, almost 80 percent of the population in Africa lacks even basic knowledge of computers. Internet *Cafés*, though widespread, are unable to afford antivirus software, making them easy targets for hackers and botnet operators. This is a very risky situation and means therefore that there is a clear, but certainly not deliberate lack of cyber security awareness and education to make cyber users aware of all possible cyber threats and risks and; ***4)*** *Lack of Technical Security Measure;* focusing on technical aspects of cyber safety. Cyber users in Africa do not have up-to-date technical security measures like anti-virus packages, and many of the operating systems used are not regularly patched. A solution is needed to ensure that such computers are technically secured by taking the responsibility away from the user and giving it to a third party.

Cassim (2011:137) further advises that the global nature of computer technology presents a challenge to African nations to address cybercrime. Domestic solutions are inadequate because cyberspace does not recognise any geographic or political boundaries, and many computer systems can be easily accessed from anywhere in the world. It is also difficult to obtain accurate cybercrime statistics because a number of crimes go undetected and unreported. It is also a costly exercise to develop and maintain security and other preventative measures. It is thus a continuous uphill battle to develop computer crime legislation that applies both nationally and internationally. The Council of Europe's Convention on Cyber Crime (CECC) - Reference Council of Europe Convention on Cybercrime (CETS) No. 185 role is important as it attempts to establish consistency in the cybercrime laws of various countries. However, many states still have to sign, let alone ratify, the Convention before it will serve as a deterrent.

The unanimous participation of all nations is thus required to achieve meaningful prosecution. Hence, there is a growing recognition that cybercrime is thriving on the African continent because of a lack of IT knowledge by the public and the absence of suitable legal frameworks to deal with cybercrime at national and regional levels, Thus, attempts are being made to address cybercrime. When enacting legislation, African countries should follow a balanced approach that ensures the protection of fundamental human rights and the effective prosecution of cybercrime. However, African countries also

need international legal, financial and technical assistance to combat cybercrime. African countries need to impose strict penalties on cyber criminals operating from and in their countries, and they need to accede to the CECC not least because cybercrime is thriving on the African continent, Cassim (2011:138). Equally, lthough attempts by African countries to address cybercrime are to be encouraged, they need to do more. African countries need to take the following steps to combat cybercrime on the African continent:

- Introduce adequate cybercrime legislation.
- Harmonise their legal frameworks to combat cybercrime and facilitate international cooperation.
- Educate the public about the threat of cybercrime as ignorance has been mooted as one of the main reasons that Africans fall victim to cybercrime.
- There should be greater public awareness on cybercrime to educate the public about the need for caution with regard to the use of cyber space or transacting online. Children should be taught computer ethics education in schools and the public educated about the risks of transacting online.
- Regulate cyber cafés as most cybercrime occurs at these locations.
- Introduce specialised law enforcement and training skills. There should also be continuous research and training of personnel in the security, finance, judicial and police enforcement sectors to keep abreast with evolving technology.
- Improve computer forensic capabilities through the appointment of competent and experienced staff.
- Build regional partnerships and enter into multilateral agreements with other countries to combat internet crime and corruption.
- Initiate support and training within government, with the help of the private sector and international organisations.
- Ratify and accede to the CECC, as the CECC is open to accession by non-member states (Cassim, 2011:138).

Consequently, the SABRIC (2020:55) provides that the impact of crimes committed against the South African banking industry have an adverse effect on the South African economy, while the citizens are the first line of victims who experience these harmful effects and are paying the price. At an international level, investor confidence is negatively influenced to the detriment of the country and its citizens. The strategic response of the South African Police Service (SAPS), the banking industry and other stakeholders to these crimes, is of critical importance to create an environment conducive to economic growth. The SAPS and the SABRIC have entered into a strategic partnership aimed at combatting electronic (including cyber) and violent crimes aimed at banks, cash-in-transit companies and Automated Teller Machines (ATMs). The strategic relationship between the SAPS and the banking industry culminated in the compilation of an action plan with an emphasis on educational and reactive perspectives. This plan mainly targets operational police members through workshops as well as members of the community through public awareness campaigns. The action plan led to the compilation of a booklet entitled SAPS/SABRIC field guide on banking-related crimes. The primary purpose of this field guide is to provide guidance to forensic investigators and operational SAPS members on how to proactively and reactively address bank-related crimes effectively and efficiently.

4. Conclusions and Recommendations

Evidentially, it is concluded that the primary challenge facing South Africa is the lengthy development and implementation process of policies and mechanisms that combat cybercrimes. Because of high rates of evolution in cybercrime techniques and advancements in ICT, policy makers must be

quick to shorten the gap between development and efficient implementation of policy. Several government departments fail to participate in issues regarding cybercrime. Outdated policies and insufficient training given to stakeholders prevent full and effective policing of cybercrime. However, the cooperation and linkage of academia, the private sector, and the public sector is growing but still needs more work to assist in the policing of cybercrime in South Africa. In addition, spreading Cybersecurity awareness has also been a challenge, increasing the risk of negligent ICT use amongst consumers, citizens, public officials and producers The challenges faced by South Africans regarding cybercrime are not unique and are evident in other [African] developing countries, Dlamini and Mbambo (2019:5) citing (Maughan, 2007).

Dlamini and Mbambo (2019:6) went on to state that [some] of the challenges of policing of cybercrime encompasses the *investigation* (Investigation involving computers often fail due to mistakes made at the initial stage of the investigation process where essential digital evidence being ignored, destroyed, compromised or inappropriately handled), *detecting* (Law enforcement agencies are deficient or slow to respond when it comes to detecting cybercrimes, "organisations have taken to launching their own counter-attacks and, even if such can be construed to be in 'self-defence', which might be illegal in the eyes of the law or even labelled as an illicit act of Cyber vigilantism" (Kader & Minaar, 2015:9) *and combating cybercrime* (Security threats increase and diversify which means that there is a need to improve security strategies and defences must be strengthened to assist the launch of counter attacks for companies and organisations to combat cybercrime. A variety of organisations and companies - those with adequate financial resources - can undertake regular cybercrime risk assessments, and implement advanced cybersecurity technology, secure firewalls, digital evidence preservation, content identification, intrusion detection, cyber intelligence gathering, cyber surveillance of all incoming online traffic and they can monitor their network systems 24/7 (Widsup, Spitter, Hylender & Basset, 2018:600).

Alternately, the global nature of computer technology presents a challenge to many countries to address cybercrime. Local and international solutions seem to be inadequate as cyberspace has no geographic or political boundaries, and many computer systems can be easily accessed from anywhere in the world. It is also difficult to obtain accurate. The cybercrime statistics because an unknown number of crimes go undetected and unreported. It is also costly to develop and maintain security and other preventative measures. International financial organisations are also common targets for computer fraud and embezzlement schemes.30 Organised crime and terrorist groups are also using sophisticated computer technology to bypass government detection and carry out destructive acts of violence. It is thus a continuous uphill battle to develop computer crime legislation that applies to both domestic and international audiences (Cassim, 2010:122).

Conversely, as recommended by Yingying and Zhengqing (2016:20, 21, 22 & 23), [Some] of the challenges facing African internet governance are confined to the following: Firstly, the African stakeholders (particularly governments) to actively participate in international cooperation in cybersecurity management. Secondly, the African governance bodies are deeply influenced by Western countries, and almost completely accept their concepts, the core concerns and systems. Thirdly, capacity building of African cyber security management needs to be strengthened. Being limited in finance and technical capacity, the insufficiency of personnel and agencies combating cybercrime in African countries brings barriers to the implementation of institutional arrangements. Fourthly, in terms of cyber security governance, the AU has yet formed a joint force with the member states, official and unofficial agencies. For African countries, it is worth learning from that the European Union (EU) has formed a cyber-security management system with features of "one theme (cyber security), two levels (the EU and its member states), three bodies (Government, private sectors and academia)," and has preliminarily established an information sharing mechanism between different levels and different bodies. Compared with the Europe, the degree of integration in Africa is much lower and the relationship between the AU and its member states are not very close, therefore, the AU is difficult to play an organising and

coordinating role as the EU and the collective actions of African countries for dealing with cyber threats face challenges. In addition, the African Non-Governmental Organisations (NGOs) are in underdevelopment, and most of them are supported by Western countries or internet companies, so what they advocate are 'liberty' and democracy" which are western core values and do not fit well with the core concerns of African governments. This also makes it difficult for Africa to form a governance model with combination of official and unofficial channels.

References

Accounting and Business Magazine [Online]. (2019). Africa is leaving itself dangerously exposed to cyber-attacks. Retrieved from: https://www.accaglobal.com/in/en/member/ ...

Adams, A. (2013). Cybercrime puts the drugs business in the shade. Without Prejudice Forensics, December, 28-29.

Atta-Asamoah, A. (2009). Understanding the West African cybercrime process. Africa Security Review, Institute of Security Studies, 18 (4), 106-114.

Baken, DN & Mantzikos, I. (2012). The cyber terrorism shadow networks in Africa: AQIM and Boko Haram. African Renaissance, 9(1), 27-45.

Basdeo, VM., Montesh, M & Lekubu, BK. (2014). Search for and seizure of evidence in cyber environments: a law-enforcement dilemma in South African criminal procedure. 2014. Journal of Law, Society and Development, 1(1), 48-67.

Bob-Felton, FE. (2006). Automation outlook - Cyber security breaches threaten, smarter factories and engineering talent base. Siviele Ingenieurswese, Januarie 2006, 26-28.

Budhram, T & Geldenhuys, N. (2017). A losing battle? Assessing the detection rate of commercial crime. South African Crime Quarterly No. 61, September, 7-18.

Bwanga, O. (2020). How to conduct a qualitative systematic review to guide evidence-based practice in Radiography? International Journal of Sciences: Basic and Applied Research, 52 (1):205-213.

Cassim, F. (2010). Addressing the challenges posed by cybercrime: A South African perspective. Journal of International Commercial Law and Technology, 5 (3), 118-123.

Cassim, F. (2011). Addressing the growing spectre of cybercrime in Africa: evaluating measures adopted by South Africa and other regional role players. Paper presented at the First International Conference of the South Asian Society of Criminology and Victimology at Jaipur, India, 15-17 January, 123-138.

Cassim, F. (2012). Addressing the spectre of cyber terrorism: a comparative perspective. Potchefstroom Electronic Law Journal, 15(2), 381-415.

Correia, R. (2011). Angola's cyber overkill. Media Freedom, Rhodes Journalism Review No. 31, 69-70.

Crane, C. (2019). 33 Alarming Cybercrime Statistics You Should Know in 2019. Retrieved from: https://www.thesslstore.com/blog/33-alarming-cybercrime-statistics-you-should-know/.

Curtin, K. (2019). Cyber Risk 101: What every business needs to know? Risk, 31 January, 26.

Cyber risk [Online]. (2015). Cyber risk and regulation rank as top risks for insurers. Retrieved from: https://www.pwc.co.za/en/press-room/cyber-risk-and-regulation-rank-as-top-risks-for-insurers.html.\

Dan, V. (2017). Empirical and non-empirical methods. Retrieved from: https://www.ls1.ifkw.uni-muenchen.de/personen/wiss_ma/dan_viorela/ .... accessed on 08 August 2021.

Davies, W. (2018). Short cuts. London Review of Books, 5 April, 40 (7): 20-21.

Desai, A. (2018). Cybercrime, cyber surveillance and state surveillance in South Africa. Acta Criminologica: Southern African Journal of Criminology, Special Edition: Cybercrime, 31(3), 149-160.

Dlamini, S & Mbambo, C. (2019). Understanding policing of cybercrime in South Africa: The phenomena, challenges and effective responses Cogent Social Sciences, 5: 1675404.

Ezeji, CL., Olutola, AA & Bello, PO. (2018). Cyber-related crime in South Africa: extent and perspectives of state's roleplayers. Acta Criminologica: Southern African Journal of Criminology Special Edition: Cybercrime, 31(3), 93-110.

Food Review. (2018). Breaches in cyber security. Plant Security and Software, February, 23.

Goga, K. (2014). Taking stock of the last 20 years - Responses to organised crime in a democratic South Africa. South African Crime Quarterly No. 48, June, 63-73.

Govender, D. (2012). Information management strategies to combat crime and prevent losses. Acta Criminologica Southern African Journal of Criminology, 25(1), 79-96.

Halder, D & Jaishankar, K. (2011). Cyber-crime and the victimisation of women. Carnegie, United Kingdom: IPR/Business books.

International Criminal Police Organisation (INTERPOL). (2021). African cyberthreat assessment report: INTERPOL's key insight into cybercrime in Africa. Singapore: International Police.

Jansen, JH. 2002. A new era for e-commerce in South Africa. De Rebus, October, 17-21.

Jegede, AE., Olowookere, EI & Elegbeleye, AO. (2016). Youth identity, peer influence and internet crime participation in Nigeria: A Reflection. Ife PsychologIA, 24(1), 37-47.

Kader, S & Minaar, A. (2015). Cybercrime investigations: Cyber-process for detecting cybercriminal activities, cyber-intelligence and evidence gathering. Acta Criminologica: Southern African Journal of Criminology Special Edition No 5/2015: Criminology in democratic South Africa: Coming of age, 4(6), 123–134.

Kortjan, N & von Solms, R. (2014). A conceptual framework for cyber-security awareness and education in SA. SACJ No. 52, July, 29-41.

Kritzinger, E. (2019). Cyber safety for all school learners. Servamus Community-based Safety and Security Magazine, October, 27-29.

Kritzinger, E & von Solms, SH. (2012). A Framework for cyber security in Africa. Journal of Information Assurance and Cybersecurity, 1-10.

Kshetri, N. (2019). Cybercrime and Cybersecurity in Africa. Journal of Global Information Technology Management, 22(2), 77-81.

Kshetri, N. (2010). Diffusion and effects of cyber-crime in developing economies. Third World Quarterly, 31 (7), 1057-1079.

Lautier, J. (2013). Southern Africa and cyber security. Africa Conflict Monthly Monitor, Consultancy Africa Intelligence (Pty) Ltd: Braamfontein, Johannesburg.

Liquid Cyber Security [Online]. (2021). The evolving cyber Security threat in Africa: IT and financial decision makers respond to critical developments in South Africa, Kenya and Zimbabwe. Retrieved from: https://liquid.tech/wps/wcm/connect/corp/00d614b5-e6cf-4552-9085_c12e47b6246c ...

Lucks, BD. (2004). Cyberstalking: Identifying and examining electronic crime in cyberspace. Unpublished Doctor of Philosophy Thesis. California: Alliant International University.

Maluleke, W. (2020). The African scare of Fall Armyworm: Are South African farmers immune? International Journal of Social Sciences and Humanity Studies, 12 (1), 207-221.

Mangena, D. (2016). Will legislation protect your virtual space? Discussing the draft cybercrime and cyber security bill. De Rebus – January/February, 33-34.

Mbanaso, UM. (2016). Cyber warfare: African research must address emerging reality. The African Journal of Information and Communication, 18, 157-164.

Moneyweb's Personal Finance. (2006). Technology – Beware of cyber-crooks. 10 August, 10-11.

Mpuru, L. (2017). Cyber security concerns in South Africa: Current legislative framework. Servamus, December, 44-45.

Nnanwube, EF. Ani, KJ & Ojakorotu, V. (2019). Emerging issues around cybercrimes in Nigeria. Ubuntu: Journal of Conflict and Social Transformation Special Issue, March, 55-71.

Olayemi, OJ. (2014). A socio-technological analysis of cybercrime and cyber security in Nigeria. International Journal of Sociology and Anthropology. 6(3), 116-125.

Quarshie, HO & Martin- Odoom, A. (2012). Fighting cybercrime in Africa. Computer Science and Engineering, 2(6): 98-100.

Rossouw, A. (2010). Cyber crooks crack the code. Occupational Risk - Safety, June, 4-5.

Schell, BH & Martin, C. 2004. Cybercrime: A reference book. California: ABC-Clio.

SciDev.Net [Online]. (2020). Cybercrime in Africa: Facts and figures. Retrieved from: https://www.scidev.net/sub-saharan-africa/icts/feature/cybercrime-africa-facts-figures.html?__cf_chl_jschl_tk_ …

Siljeur, N. (2016). Protecting children against cyber-sex in South Africa. Child Abuse Research: A South African Journal, 17(2):95-102.

Sissing, S & Prinsloo, J. (2013). Contextualising the phenomenon of cyber stalking and protection from harassment in Aouth Africa. Acta Criminologica: Southern African Journal of Criminology, 26(2), 15-29.

Snail, S. (2015). Cybercrime in the context of the ECT Act - Hacking, cracking, and other unlawful online activities. Volume 16 Part 2, 63-69.

Snail, SL & Matanzima, S. (2014). Cyber security in Africa. Without Prejudice Cyber law, October, 88-89.

South African Banking Risk Information Centre. (2020). Banking-related crime and how to respond to it. Servamus Community-based Safety and Security Magazine, February, 55.

Van Niekerk, B. (2017). An analysis of cyber-incidents in South Africa. The African Journal of Information and Communication (AJIC), 20 (1), 113-132.

Visser, B. (2015). Cyber security risks – just as relevant locally as internationally. Retrieved from: https://www.psg.co.za/news/cyber-security-risks.

Widsup, S., Spitter, M., Hylender, D., & Basset, G. (2018). Verizon data breach. Investigations report. Retrieved from: https/www.researchgate.net.publication/32445340_2018-verizon-data-breach-investigationreport.

Yannascoli, S.M., Schenker, M.I and Baldwin, K. (2013). How to write a systematic review: A step-by-step guide? Retrieved from: https://www.semanticscholar.org/paper ... accessed on 10 November 2021.

Yingying, X & Zhengqing, Y. (2016). A primary exploration on cyber security governance in Africa. West Asia and Africa, 03: 121-137.

Young, R. (2016). Cyber security today and beyond. Human Resources Future Net - Digital cyber security, 32-33.