The International Journal of Multi-Disciplinary Research

ISSN: 3471-7102, ISBN: 978-9982-70-318-5

Analysis of Cybercrime and Cyber Law Effectiveness in Zambian

(Conference ID: CFP/731/2018

[1] Nizah Lawrence Mutambo, [2] Dr. Phiri

[1]School of Engineering, Department of Information Systems, Information and Communication University [2]School of Engineering, Department of Information Systems, Information and Communication University, Lusaka Zambia.

Email: [1]nizahlm@gmail.com

ABSTRACT

Weak or lack of cyber laws in Zambia is a critical challenge to combat cybercrime. This paper argues that Zambia does not have a comprehensive legal structure to deter and prosecute cybercrime. It only depends on the international and national approaches to cybercrime, with a view of providing guidance for an effective framework capable of addressing this new crime. Although the Computer Crimes and Misuse Act no.13 0f 2004 now criminalises some cybercrimes but still it does not prohibit other major cybercrimes. Furthermore, this paper argues that the Act imposes lighter sentences for offences that require hefty punishments. The paper also argues that the statistics of cybercrime in the country do not reflect the actual level of cybercrimes due to the fact that most cybercrime related cases are not reported. This paper also considers and examines the National ICT Policy of 2007 and the seventh National Development Plan for 2017 -2021. Additionally, will also look at multitude concerns over the emphatic increase of cybercrimes in Zambia and efforts the Zambian government has put in place to reduce the vice and commitment in promoting safety on the electronic frontier especially that the government just launched the smart Zambia through utilisation of Information and Communication Technologies. The guides for future legislative reforms are highlighted meant to address cybercrime concerns as depicted in the two policy documents. Cybercrime is a major global challenge requiring coordinated international effort. This paper again advocates for the adoption of an appropriate legal and regulatory framework on the regional and international level. Further, it also assesses the efforts at COMESA, SADC and UN bodies in combating cybercrime.

Keywords: *Cybercrime, Cyber Law, Cyberspace, Information Communication Technology, Governing Laws.*

ISSN: 3471-7102, ISBN: 978-9982-70-318-5

1.0 INTRODUCTION

1.1 Background

Cybercrime originates from the time when Internet was developed; the founding fathers of Internet hardly had any inclination that Internet could also be misused for criminal activities. Today, there are many disturbing things happening in cyberspace. Cybercrime refers to all the activities done with criminal intent in cyberspace. These could be either the criminal activities in the conventional sense or could be activities, newly evolved with the growth of the digital age. Because of the anonymous nature of the Internet, it is possible to engage into a variety of criminal activities with impunity and people with intelligence, have been grossly misusing this aspect of the Internet to perpetuate criminal activities in cyberspace (Phiri W. 2016).

Cybercrimes are conducted in what is called Cyberspace which is basically the internet – a combination of computers, computer networks and technology. Cyberspace brings together the potentially exciting cocktail of technology, and its unique group of users, within the context of anonymity and an environment lacking in consistent norms. Whilst the potentially democratizing effect is to be welcomed, the potential for perverse activity is not (Lessig, 2004).

The ICT Act provides the backbone for e-commerce and as such there is the need to take into consideration the security aspects.

In Zambia, cybercrime is relatively thought of new phenomenon in the business community with offences related to information and communication technology. Today we have very few institutions that are playing key roles in combating the criminal acts just like any other developing nations that has not been spared to the ever increasing attacks. Individuals as well as organisations have experienced huge sums of money being electronically stolen from personal and company accounts. Not to mention causing disruption in the businesses through corrupting critical business systems by the cyber criminals or Hackers, as they are termed under the international cyber security bodies, for their personal gain and satisfaction. Additionally, social media is being highly misused in Zambia; it has been turned into a platform for insults, child pornography, privacy invading, data theft and many other bad things.

ISSN: 3471-7102, ISBN: 978-9982-70-318-5

1.2 Statement of the problem

The experience of many jurisdictions is that gaps and inadequacies in tradition offence provisions necessitate the consideration of more specific laws targeting cybercrime. It is in this context that the Zambian parliament passed a cybercrime specific piece of legislation called the Computer Crime and Misuse Act No. 13 of 2004. Under this Act, cybercrimes like hacking, denial of service attacks, unauthorized access and modification of data was since criminalized. On the other hand, with time utilization of ICT has greatly increased in the country. As of June 30th 2016 the number of Internet users had increased to 3,167,934 which represent 20.4% of the Zambian population. This is according to IWS. The latest figures from the Zambia Information and Communications Technology Authority (ZICTA) shows that the country has now 6.1 million internet users, representing a penetration rate of 39%. Furthermore, an increasing number of people are keeping pace with technological developments through acquisition of private home computers and mobile smart devices like phones, tablets, Laptops only to mention a few. Today many private and public institutions are increasingly deploying computer technologies in their daily operations. With this exposition, and despite the existence of the Computer Crime and Misuse Act No. 13 of 2004, this has since been in existence for the past 14 years, no record indicating prosecution under this Act. This paper will therefore address some of the reasons why the Act has not been so forceful on most cybercrimes committed in Zambia and the extent to which the Act covers possible criminal conduct on the electronic frontier and ultimately feasibility of employing other measures in fighting cybercrime other than through criminal or penal sanctions.

The launch of the National ICT policy and the Seventh National Development Plan after the cybercrime legislation was already in place, calls for a need to asses governments commitment in addressing cyber security concerns in these policy documents. This paper recognizes the rapid expansion of e-commerce that is; buying and selling services and product via the Internet, which calls for serious protection among parties and safety guaranty of the cyber space, also assuring fair dealing through the law and policy. Further, with the number of Internet users keeping going up globally, this translates into more transactional nature of cybercrime that also elevates the number of problems that includes of those of jurisdiction and international cooperation. This paper will therefore, assess Zambia's position to deal with cybercrime at reginal and international level respectively.

ISSN: 3471-7102, ISBN: 978-9982-70-318-5

1.3 Objective of the Project

The main general objective of this research paper is to examine if Zambia's legal and policy regimes are capable of combating cybercrime satisfactorily and ensuring safety on the electronic frontier. The specific objectives are as follows:

i. To examine if the formal record of cybercrime in Zambia reflects the actual level of criminal computer misconduct.
ii. To identify and discuss the new and unique challenges and response issues which may be encountered during the prevention, detection and investigation of cybercrime offense.
iii. To examine how Zambia's legal regime is in conformity with legislative responses to cybercrime in other jurisdiction.
iv. To examine and measure the adequacy or inadequacy of the National ICT policy implemented by the government to fight against cybercrime.
v. To examine the feasibility of preventing and minimizing the harm of cybercrime other than through criminal penal sanctions.
vi. To examine how Zambia's legal regime responds to the regulation of e-commerce transactions.
vii. To examine Zambia's efforts in combating cybercrime.
viii. To examine the relevance of having common standards at regional and international level in an effort to fight cybercrime.

1.4 Theoretical Framework / Model

The purpose of the study is to examine efforts Zambia is making to combat cybercrime which seem to be increasing every day and has since become a global concern. Knowing very well that the world is increasingly dependent on the utilization of the Information and Communication Technologies (ICTs) and Zambia too is not an exceptional in this development. Due to the increased dependence on the technology, most critical infrastructure of the country is computer technology operated, this has since seen the increased use of e-commerce that purely involve use of electronic gadgets and payments via the internet. Examples of these includes: ATM's, Internet Banking and DDAC transactions, only to mention a few. The Zambian government through its National ICT policy has affirmed the adoption of

ISSN: 3471-7102, ISBN: 978-9982-70-318-5

an electronic governance system that will broadly involve the deployment and exploitation of ICTs to facilitate the process of bringing the Government closer to the people through improved delivery of services and goods to the relevant stakeholder and the citizens of Zambia at large (National ICT policy 2007). The fundamental reason of transforming Government through ICTs is simply to promote efficiency, minimize operation and administrative costs and largely to streamline government procedures and processes. The Government is very much aware of the great benefits that come with e-governance hence the launch of the smart Zambia through utilization of ICTs. Further, the seventh national development plan (2017 -2021) advocates for increased use of ICT's if many objectives of the Government are to be realized (Seventh National Development plan 2017). However, this development will again mean that people's money and confidential information will be exposed for possible loss or altered. In addition, Zambia and its citizens are potential victims of cybercrimes which has no regard to jurisdiction, meaning we can be attacked from anywhere in the world. It's with this reason that this research would therefore look at Governments effort in combating cybercrime both at regional and international level.

1.5 Literature Review

Cyber law is a new phenomenon worldwide to combat cybercrime, further no distinctive and comprehensive law has been implemented at the global level to deter cybercrime. As such no much literature has been gathered relating to the subject at hand. The author was privileged to examine and acknowledged some of the works that looked at cyber laws in Zambia. Notable one was the research that was conducted with much focus on the adequacy of the Computer Crimes and Misuse Act (Act No 13 of 2004) in the fight against cybercrime (Kapumpa D. 2006). This research basically focused on the flaws in the Act and identified the inadequacies in it regarding criminalizing of unsolicited emails or spam. Further, was also identified as a shortcoming affecting the Act in the sense that it failed to address enforcement mechanisms for special unit of the policy that would specialize in cybercrime.

Though they have been some inquiry, still no research has been done yet regarding the assessment of Zambia's entire legal and policy regime in the fight against cybercrime. The research is important in this respect due to the fact that it will be identifying key traditional legislation which can be used to fight cybercrime. The diversity of this paper is also to be seen by its examination and consideration of

ISSN: 3471-7102, ISBN: 978-9982-70-318-5

the advocacy of technological advancement as well as the cyber security policy issues brought forward in the SNDP and the National ICT policy, also examining how these policy documents addresses future regimes concerning cybercrime. Additionally, this paper also discusses the viability of employing other ways of combating or reducing the harm of cybercrime through different means like technological measures, regulatory controls and civil proceedings. The paper is also distinct in that it examines the relevant regional and international obligations and standard relating to cybercrime and assesses not only their viability but also the possible concerns that they may pose for Zambia.

2.0 METHODOLOGY/RESEARCH DESIGN

2.1 Project Design / Approach

This research paper most of it was done through desk research. However, relevant published and where necessary unpublished works were consulted. Relevant pieces of legislation were also utilized to provide information which prayed a very fundamental role.

2.2 Target Population and Sample Size

Cybercrime affects all, be it on the personal or organizational level provided a computer, computer networks and the internet is involved. Information and communication Technology has taken over as the world's pillar to the economic growth. ICT has completely changed the way we live today that most interact in the cyber space which has completely disrespect for nation boundaries. A person in Zambia could break into a bank's electronic vault hosted on a computer in South Africa and transfer millions of dollars to another bank in Switzerland all within minutes. It's because of these facts that cybercrime affects all, be it at national, regional or international level respectively.

2.3 Instruments of data collection

Like earlier alluded too, this research was a desk research and as such, the main data collection instrument was publications from the Internet regarding Cybercrime and cyber law in Zambia and making calls to relevant personnel in Government for more information regarding cyber law. The Materials collected was far enough to handle and fulfil the objectives of the research.

ISSN: 3471-7102, ISBN: 978-9982-70-318-5

2.4 Ethical Considerations

- Voluntary participation: though cybercrime mainly affect Netizens, still the affected have all the rights of voluntarism in respect to contributing towards making cyber space a safer place that is free from cybercrime.
- Informed Consent: this is the most fundamental ethical principle that enables participants to fully understand the nature and purpose of the research that they give consent to participate without coercion. Usually potential participants sign an informed consent form which describes the purpose of the research, its procedures, risks and discomforts, its benefits and the right to withdraw. This makes the situation clear and provides a degree of proof that the person was informed and consented to take part.
- Privacy and Confidentiality: confidentiality involves the disclosure to the subject the use to which data will be put while ensuring that responses to personal questions, scores on tests and so on, are kept confidential and anonymous.
- The right to access to information is now enshrined in the UN Human Rights and national legislation. Individuals can communicate what information in government, bank offices, etc. can be made public
- Right to continue: Subjects who participate in this study have a right to withdraw or discontinue.
- The right and welfare of participants are protected. The research will avoid unnecessary psychological harm or discomfort to the subject.
- This research made sure the risk to participants is minimized by procedures which do not expose subject to risk.

3.0 RESULTS AND DISCUSSION

3.1 Results / Research findings

3.1.1 Computer crimes and misuse Act

Zambia had no specific legislation meant to deal with cybercrime until the year 2004 when the legislature passed the computer Misuse and Crimes Act (Act No. 13 of 2004). The act was passed

ISSN: 3471-7102, ISBN: 978-9982-70-318-5

against the background that while technological advances have brought immense benefits to society, there are also some negative developments that have come with the computer age. The legislation recognized this fact and it was felt that existing legal framework at the time could not keep pace with the new moral and ethical dilemmas that technology has posed and there was need for legislation intervention

The need to have specific cybercrime laws was also justified by an incident mentioned already in the introduction where a young Zambia hacked onto the state house website and replaced the portrait of the then serving president Fredrick Chiluba with an image of a carton. The perpetrator was arrested and charged with defaming the head of state contrary to S.67 of the penal code (Cap 88 of the laws of Zambia), unfortunately the case failed to succeed in court reason being there was no law in Zambia that dealt with cybercrimes. The above case study also goes further to give good reason for constantly keeping our law up-to-date so as to counter new forms of criminal acts that come with technological advancements.

The then Minister of Communication and Transport, Mr. Namuyamba, when introducing the computer Misuse and Crimes bill stressed that the intention was to meet the following objective:

i. To prohibit any unauthorized access, use or interference with a computer,
ii. To protect the integrity of computer systems and the confidentiality and the integrity of data,
iii. To prevent abuse of computer systems,
iv. To facilitate the gathering and use of electronic evidence, and to provide maters connected to or incidental to computer misuse and crimes.

The national assembly approved the Bill and was assented to by the President on the 2nd of September, 2004. The passing of the Act was a step in the right direction as it has criminalized several computer misconduct. The foregoing discussion therefore comparatively analyses how the Act responds to major criminal activities that have come forth as a result of computer technology. In achieving this, reference is made to responses taken by some individual countries as well as the council of Europe convention on Cybercrime (2001).

ISSN: 3471-7102, ISBN: 978-9982-70-318-5

Unauthorized Modification: the criminalization of unauthorized modification of data is meant to help safeguard the integrity of the computer system. Data can be modified through different ways. The common ones are: A person my physically make input commands to a computer and make some modification. Nevertheless, the well-known form of modification of data is via computer viruses. A computer virus is a software program that attaches or copies itself to infect a program and has the ability to replicate as well as infect other programs on the system. There are other different forms of software programs that can affect computers and cause damage. Some of the most well-known dangerous code or programs include worms, logic bombs and Trojan horse.

Legislative response world over in prohibiting unauthorized modification of computer data has been over whelming. In the US, unauthorized modification, including virus and other rogue code dissemination, could be the basis of a criminal prosecution. In a similar way even in UK, unauthorized modification of computer program or data is criminalized and conviction is punishable by imprisonment not exceeding five years or a fine, at a worst case even both. The council of Europe convention also provides that member states are to criminalize unauthorized modification or interference with data. Zambia has also legislated against unauthorized modification of computer material. The modification should be unauthorized and is indicative of a lack of consent. The perpetrator must know that his actions are unauthorized and should have the deliberate intent to impair the operation of the computer. Those convicted of this crime will be fined not exceeding fifty thousand penalty units or to imprisonment for a term not exceeding three years or both in a worst case. It was proposed that the maximum sentence for unauthorized modification is not sufficient and should be increased to ten years.

Unauthorized Access: the main criminal activity that is intended to be curbed by prohibiting unauthorized access to a computer system is hacking. Hacking has been defined as the accessing of a computer system without the express or implied permission from the actual owner of the computer system. Unauthorized access is achieved through gaining access to the system via different ways. Some hackers are in the habit of guessing passwords or do investigation in order to obtain the password to a computer system, Network or a system. There are also many software applications and devices that facilitate the unauthorized access to data.

ISSN: 3471-7102, ISBN: 978-9982-70-318-5

Most countries have legislated against unauthorized. Example of such countries is: The United Kingdom, United States of America and South Africa respectively. In the UK, unauthorized access to computer material is criminalized and causing a computer to perform any function to access a computing system without any authority is an offence. The offense is committed when unauthorized access is achieved and it is punishable on summary conviction by fine or six months imprisonment or both in a worst case. Under the council of Europe convention on cybercrime, each party is obliged to adopt such legislative and other measures as may be necessary to criminalize unauthorized access to the whole or any part of a computer system. In Zambia unauthorized access has also been criminalized. Accessing a computer system without authority or consent of the owner attracts a fine not exceeding fifty thousand penalty units or to imprisonment for a term not exceeding two years or at a worst case can attract both.

Spam (Denial of Service): unsolicited sending of bulk emails for commercial purposes is what is called spam. This is an act by the criminal who floods the bandwidth of the victim's network fill his email box with spam mail depriving him of the services entitled to access or provides. Dos stand for Denial of Service attack, a type of attack on a network that is designed to bring the network down through flooding it with unwanted traffic. Many Dos attacks such as ping of Death and Teardrop attacks, exploit limitations in the TCP/IP protocols. Due to advancement with technology, most known Dos attacks are being combated through use of software fixes that system administrators are installing to limit the damage caused by the attacks. Nevertheless, hackers are also busy coming up with new viruses and skills of breaking through some of the security features that have been implemented by the victims.

Pornography: is one aspect that has been on the rise with the coming of the digital age. Pornographic materials are widely distributed through the Internet and the major concern is that Information network and computers pray a very cardinal law in the creation, possession and distribution of pornography. In most jurisdictions, the concern is child pornography and little apprehension is expressed for pornography where adults are involved. In UK, the protection of children Act regulate child pornography through criminalizing taking, permitting to be taken or making, distribution or showing, possessing, publishing or causing to be published any indecent photograph or indecent pseudo-photograph of a child, including by electronic and other means capable of converting into a photograph

ISSN: 3471-7102, ISBN: 978-9982-70-318-5

(Protection of Children Act of 1978). The punishment for this offence is imprisonment for a period not exceeding ten years or a fine even both. The USA and South Africa are among other countries that legislated against child pornography perpetrated inter alia through electronic frontier. The council of Europe convention also criminalizes child pornography.

Hacking: this involves penetrating a secure area by subverting its security measures. Out of many ways hackers can use to hack, one of them is through programs like "War diallers" that try thousands of common passwords until one is accepted. Another method is through installation of a packet sniffer program that will be able to scan data from the target systems network ports with the view of discovering loop holes on the targeted network. Open ports will be reviewed and through them the hacker can penetrate the network and do damage or have full access of the intended files or documents of which they can be altered if so wish.

Computer Virus/worm: viruses attach themselves to a computer or file that will eventually affect the data on the computer system. Worm don't usually attach themselves to the host like virus do but rather make copies of themselves repeatedly until most space available on the computer hard drive is filled up

Piracy: this is an illegal act of reproduction and distribution of software applications, games, videos and audio media using original copies. Theft of software through the illegal copying of genuine programs or the counterfeiting and distribution of products intended to pass for the original (EOW, 2005)

Intellectual property: any act which deprives the original owner of his/her rights. This includes software piracy, copyright infringement and trademark as well as service mark violations.

Cyber Stalking: in simple terms it's online stalking. It has been defined as the use of technology, particularly the Internet, to harass someone. Common characteristics include false accusations, monitoring, threats, identity theft, and data destruction or manipulation. Cyberstalking also includes exploitation of minors, be it sexual or otherwise (Merrit, 2016)

Trojan attacks: this is an unauthorized program which gains control of another system by representing itself as an authorized program.

ISSN: 3471-7102, ISBN: 978-9982-70-318-5

Logic bombs: these are event dependent programs. They are created to do something only when a certain event occurs.

3.1.2 National ICT Policy

In view of the huge benefits that come with ICT, legislative and public policy measures may encourage communities, organizations and individuals to invest in and use information and communication technology (ICT). However, to have a better public policy and legal framework on ICT, it is necessary that much attention is paid to ensure that criminal activities like cybercrime which would flourish with the wide use of ICT are curtailed. The foregoing therefore justifies the urgency of analyzing how the National ICT policy address concerns regarding deterrence of using ICT to further criminalize activities involving computer technology as well as how the policy accommodated future legislative reforms.

The Zambian government prepared the National ICT policy of 2007 to coordinate all matters related to ICT in the country. The goals of the ICT policy are grouped into thirteen main areas which include:

i. Promoting Human Resources Development
ii. Promoting ICT in Education, Research & Development
iii. Promoting Public Access, Content Development and Cultural Heritage
iv. Developing the ICT Sector
v. Developing Telecommunication & Supporting Infrastructure
vi. Promoting Electronic Government
vii. Promoting Electronic Commerce
viii. Promoting the Integration of ICT in Agriculture Development
ix. Promoting the integration of ICT in Healthcare Delivery
x. Promoting the Integration of ICT in Tourism, Environment & Natural Resources Management
xi. Mainstreaming Youth And Women Issues
xii. Developing the Legal & Regulatory Framework
xiii. Promoting Security in the Information Society

ISSN: 3471-7102, ISBN: 978-9982-70-318-5

Most of the above mentioned goals aimed at furthering the use of ICT in the country. However, as alluded to earlier, ICT also offers opportunities to criminals to commit undesirable acts with ease and little risk of apprehension. It's with this reason that has demanded evaluation of governments commitment in the ICT policy to deal with culprits who will be found wanting. Among the goals in the National ICT policy, the last two are much of a concern in this paper i.e. "Developing the Legal & Regulatory Framework" and "Promoting Security in the Information Society". The two goals are under discussion in details in the following units.

3.1.2.1 Developing the Legal & Regulatory framework (Policy goal number 12)

The National ICT policy acknowledges that an appropriate and dynamic legal/regulatory framework is mandatory to act as the foundation for the development of the ICT sector. It is further mentioned that the current legal and regulatory framework is not adequate to address the current challenges being experienced. Therefore, it is the desire of the policy through this goal to have to develop appropriate institutional, legal and regulatory system that will support the development of a competitive national ICT sector based on convergence principles that will be supported by a fair and transparent legal and regulatory framework. In order to achieve this goal, the government has made a number of commitments though will only address the many ones. Firstly, the government aims at putting in place very effective laws and regulations aimed at adherence to national, regional and international standards. Implementing effective laws and regulation at the just mentioned levels will help combating cybercrime at national, regional and ultimately at the international level. Further, to win this battle will call for combined efforts at all levels. Another gesture of importance government is trying to address in the national ICT policy is the promotion of practicing professionalism in the ICT industry. This move is very vital and beneficial in the sense that, once implemented will then have well trained competent men and woman ready to make meaningful contribution in making the cyberspace safer for all netizens. Additionally, professionalism would provide a better foresight of different threats in the ICT sector such as those that affect the integrity of the systems. Presently, the only body that seeks to set standard for ICT personnel in the country is the Information Communication Technology Society of Zambia which unfortunately up to now does not have power to regulate the training of all ICT professionals, Register or to discipline them. However, processes have begun to have the ICT bill passed in

ISSN: 3471-7102, ISBN: 978-9982-70-318-5

parliament that will see the ICT society of Zambia to have power to regulate all its members. Once this is achieved sanity will be seen in the Zambian ICT industry.

Another aspect of great importance in the goal of developing an appropriate legal and regulatory framework for the ICT is that of creating laws to effectively and efficiently support E-Services. This is a very cardinal measure that requires much urgency in view of the increasing use of E-services. This will see exit of the conventional legal regimes that are inadequate and tailored for paper transactions. (National ICT Policy, 2007)

Another significant goal in the ICT policy is the efforts being made by government to improve the ICT sector through establishment of the ICT tribunal (Chapter 6.12.2(e)). Tribunal will be designed to address only appeal cases arising from rulings or directives of the regulator. Advantages associated to this move are quiet numerous, some of which are reduction on cases that ultimately reach our ever crowded formal court system and also will expected quick disposal of cases hence reducing on time handling the same case for a very long time. The only major challenge in formulating the same tribunal might be on clearly defining the role and power of the intended ICT Tribunal.

3.1.2.2 Promoting Security in the Information Society (Policy goal number 13)

This goal stems from the realization that Zambia like any other countries in the world is vulnerable to some of the negative implications that may hinder the mainstreaming of ICT in society (Chapter 6.14 of the National ICT Policy). The government intends to embark on various measures in trying promoting security through attainment of this policy goal of promoting security in the information society. To start with, the government intends to establish a computer crime Investigation Unity for cyber law enforcement and the National Electronic communication security centre (Chapter 6.13.2(a) of the National ICT Policy). Once these bodies are actualized, they will be under the supervision of the internal organs of specialized security agencies. The most advantageous about this move is that it will eliminate establishment of independent units that may be too costly and time consuming during establishment.

ISSN: 3471-7102, ISBN: 978-9982-70-318-5

The gesture of establishing a computer crime investigation unit is a positive move and should be supported at all costs in view of the presently lacking expertise in the enforcement of cyber laws. The unit will play a very fundamental rile in preventing, detecting and prompt response to cybercrime and misuse of the ICT that will definitely contribute in combating cybercrimes like fraud, money laundering, pornography, drug trafficking , terrorism etc. at national, reginal and global level. The National Electronic Communication Security Centre is another vital body that would complement the efforts of safeguarding information and communication infrastructure, network and systems. The two bodies will surely help in the reform process of ensuring the availability, authenticity and integrity and confidentiality of Government, public and private communication networks and systems, data and information content integrity, consumer privacy and protection not forgetting addressing security concerns triggered to damage or corrupting Zambia's cultural heritage, national image and identity.

The fact that the ICT security bodies need to be well equipped with necessary equipment should be looked into first. Thus the government's intention to deploy ICT equipment to facilitate, support and enhance the management, operation and administration of security matters as well as the command and control structure of the National Security Agencies. In addition, its highly recommended that the security personnel are also trained and this has already received acknowledgement from the government through its commitment toward implementing ICT skills development within the security agencies aimed at supporting effective deployment and application of ICT in operations and service delivery (Chapter 6.13.4(d) and (e) of the National ICT policy). ICT sector security would further be enhanced with coordination among security agencies. A move that has already been cemented in the National ICT policy aimed at ensuring cross-sectional linkages and coordination among security agencies that ICT security concerns can adequately be addressed.

The government also intends to enact and enforce legislation that allows for effective investigation and prosecution of cyber related crime (Chapter 6.13.2(c) of the National ICT policy). However in view of the fact that criminal law would not fully protect society from high tech crimes, the government has acknowledged the need to outrun that and compel all organizations providing public information services like telecommunication services, Internet, email to deliberately incorporate administrative, technological and other such practical measures to enable national security agencies to curb

ISSN: 3471-7102, ISBN: 978-9982-70-318-5

cybercrime. This is another virtue in the policy reason being the employment of administrative and technological measure would operate as preventive measures in the fight against cybercrime. This is further supported by the immerse effects that may be caused by cybercrime. For example, in May 2000 a virus that originated from Philippines and spread rapidly throughout the world, leaving many file destroyed. The virus affected NASA and the CIA just within two hours of its spreading around the world. Estimated number of users was around forty-five million in more than twenty countries and the damage estimate caused by the same virus ranged from two billion dollars up to ten billion (Goodman M. and Brenner S. 2003)

Another measure the government will undertake is the implementation of ICT Security awareness programs amongst corporate users and the general public at large (Chapter 6.13.4(b) of the National ICT policy). This will surely change the perspective toward the use of technology due to the fact that people will be made aware of the cyber laws and what is expected of them regarding computer technology usage. The awareness program would again enhance the user confidence and trust among the general public.

3.1.3 Seventh National Development Plan (SNDP)

The Seventh Nation Development plan is a policy document highlighting the areas of focus which the government intends to embark upon in the period 2017 to 2021. The SNDP was launched last year 2017 with the view of incorporating ICT the National development agenda, especially with the fact that ICT is one of the fastest growing industries in the world and this is due to its changing technology that supports business models and work relations. ICT is widely and increasingly regarded as the fourth factor of production after land, labour and capital.

The government has identified Information and Communication Technology (ICT) as a catalyst for social-economic development through promoting competitiveness as well as an enabler of good governance. However, there are several challenges regarding access to and utilization of ICT in Zambia. ICT infrastructure, both public and private, is inadequate and fragmented, resulting in poor connectivity and communication. Further the public sector in particular, lacks adequate human resource

ISSN: 3471-7102, ISBN: 978-9982-70-318-5

in the area of computing and information technology. This has surely been compounded by a weak supportive legal and institutional framework for the development and utilization of ICT.

Empirical evidence of Zambia's performance in the utilization of ICT can be found in indices produced by various international organisations. For instance, the 2017 E-Government Development Index published by the United Nations Department of Economic and social Affairs ranks Zambia at 132 out of 193 countries. Another agency of the United Nations, the International Telecommunications Union in its 2015 ICT Development Index places Zambia at 153 out of 167 countries. The 2015 Network Readiness Index or Technology Readiness Index by the World Economic Forum shows that Zambia ranks 116 out of 139 participating countries. Zambia's power performance in these indices indicates a clear need for accelerated ICT development to effectively and efficiently support the economic recovery and diversification aspirations.

Because of the above mentioned challenges, the Government intends to put much focus on increasing investment in the ICT infrastructure and human resource development. Further, the Government will also undertake policy legal and institutional reforms to facilitate universal access to ICT and ultimately promote the use of ICT in business (e-Commerce); networking of services and application across the public sector and online access to government services will be prioritized. Another aspect of importance to be addressed is the incorporation of ICT in the education curriculum that needs to be accelerated to ensure increased uptake and utilization of ICT to reduce government service delivery costs.

The SNDP seeks to address strategies government will use to attain enhanced Information and Communication Technology. The three strategies to be explored are:

1. *Strengthen legal framework of information and communication technology*
   In the strategy 1 the Government will put in place appropriate laws, policies and regulation to support the provision of electronic service and to promote private sector/citizen confidence and participation. I believe through this gesture, government will also tighten the laws that that govern the use of computer systems that cyber security concerns can as well be addressed (SNDP 7.11.1 Strategy 1).

ISSN: 3471-7102, ISBN: 978-9982-70-318-5

2. *Improve ICT infrastructure for service delivery*

   Improving ICT infrastructure calls for massive investment in upgrading telecommunication network, data centers and access devices through the SMART Zambia Master plan. This will surely improve the flow of information within and among government institutions, enterprises and citizens to bring about social and economic benefits (SNDP 7.11.2 Strategy2).

3. *Provide electronic services*

   The Government will transform its mode of delivery of public services from tradition face-to-face interaction to online channels. This move will enable citizens and business entities to access services anywhere and anytime. As a way of showing commitment towards shaping the future of ICT, Government will also facilitate skills up-scaling in ICT for public service workers and the private sector. Government will also accelerate the mainstreaming of ICT in the Zambia education curricula to ensure sustainable development and utilisation (SNDP 7.11.3 Strategy 3).

3.1.4 Proposed bills

Additionally, Government is in the process of enacting three bills in an effort to combat cybercrime. The three bills include: cyber security and cybercrime bill, electronic commerce bill and the data protection bill. The three bills are scheduled to be presented before parliament for approval this same year of 2018. The bills once enacted are meant to protect the Zambian people from cyber-attacks said the minister of Transport and communication Mr. Brian Mushimba who further announced that Government is in the process of establishing a cyber security institute to prevent cyber-attacks, especially as the country is digitalizing its economy. He further said Government wants to develop firewalls in the cyber space to prevent digital information from landing in wrong hands.

Mr. Mushimba said Government wants to have a helicopter view of its cyber space to detect possible cyber-crimes. The permanent secretary in the Ministry of Transport and Communication Mr. Misheck Lungu further added saying “As a country we are as vulnerable as other countries but we are not sitting idle. We are putting in place a cyber security strategy because we are ear-marked to be a digital society where most of our services will be internet based,” he further assured the National that Government is safeguarding the country’s cyber space and is “on top of things”.

ISSN: 3471-7102, ISBN: 978-9982-70-318-5

3.1.5 Regional and International efforts

Cybercrime affects all and it's with this reason that at the regional and international level, efforts are also being made to fight cybercrime. This comes into play to examine ways available to Zambia in dealing with cybercrime beyond its borders. In this regard, an examination of regional efforts by SADC and COMESA regional bodies is made (Zambia has membership of both SADC and COMESA bodies). At international level, particular attention is given to the council of Europe Conversion on Cybercrime (2001), highlighting its merits as well as the concerns that come forth as a result of this body. The enquiry into the regional and international is justified as earlier alluded to that cybercrime is transnational in nature in that it may be perpetrated from anywhere in the world, hence making it difficult to fight it adequately at the national level alone. The reason now for calling coordinated efforts among countries through specifying offenses and in applying the laws that are enacted to cross-border illegal acts. In the absence of measures that actively coordinate national actions and policies at the international level.

3.1.5.1 Regional efforts

SADC

At SADC the realization of the benefits of technology through implementation of the ICT systems is well advocated. The SADC member states have also acknowledged to the fact that unless much focus goes towards creation of the requisite harmonized policy environment, it's when full benefits of ICT utilization can be seen and also not forgetting the legal and regulatory frameworks to promote ICT diffusion and use (Regional Indicative Strategic Development Plan, 2006). This background lead SADC membership to develop the SADC model legislative provisions or guidelines on pertinent ICT issues to clearly define the digital landscape. The model legislative provisions unfortunately does not specifically address the cybercrime concerns, Members of SADC are taking initiatives to introduce and place into context the requirement and prerequisites of cyber registration and harmonization with the region. For example, in 2005, SADC called for a meeting whose them was "Cyber Law Development and Harmonization within SADC". After the meeting, three major issues came out which were:

ISSN: 3471-7102, ISBN: 978-9982-70-318-5

i. That independent of the issue of harmonization, SADC members need to mobilize their efforts to adapt their legal frameworks for the new technologies.
ii. That the SADC countries should work together towards harmonization of the national laws, through ways such as the development of a SADC Web-based portal to facilitate best-practice dissemination and regional networking in this domain.
iii. That member states should introduce capacity-building programmed for the judiciary, magistrates and police prosecutors, with a focus on proper methods of collecting, preserving and presenting admissible evidence in cases involving computer and its data (Cyber Law Development and Harmonization within SADC, 2005).

Members of the Legal fraternity from SADC converged in Gaborone for the 18th SADC Lawyers Association Annual Conference. On the table were a number of topics including some on Cybercrime. Titled, "A developing SADC: Measuring the impact of Cyber law and crimes on Legal Practice Initiatives and regional cooperation – How to protect yourself and your clients," the lawyers and judges present brainstormed on how the issues of electronic crime would be approached from the legal point of view. The conference was chaired by Dr. Omponye Coach Kereteletswe from Botswana and Judith Tembo from The lawyers association of Zambia. The gathering agreed that there is a significant increase in crimes involving computers and the internet that are damaging the region's security and economies. Therefore, the profession needs to learn techniques for using cyber tools and methods to investigate computer and internet related activities. "We explore the need to harmonize and standardization of legislation in SADC in order to successfully tackle cyber-crime."

The lawyers view was that, Cyber Security is a global challenge and it poses unique security challenges; global reach of ubiquitous networks, speed, jurisdictions and enforcement. "Deals and online transactions are initiated and concluded online, the e-commerce transactions were estimated to be over $16 trillion in 2013. The technologies for authenticating and methods for exchanging contractual information are rapidly changing. Appropriate legislations, technical measures, International and regional cooperation are required to ensure the protection of clients online," they said.

ISSN: 3471-7102, ISBN: 978-9982-70-318-5

Accordingly, for the SADC lawyers who were gathered in Gaborone, in this time of IoT, the internet is a global communication tool, therefore it is very important that cybersecurity legal frameworks are internationally and regionally harmonised to facilitate the investigation and prosecution of crimes in the cyberspace. Hence, the ITU assisted SADC countries and developed the following model laws: Cybercrime and Computer Crime Act, Data Protection Act, Electronics Transactions Act, Electronic Signature. Cybersecurity requires a multi-stakeholder approach and international cooperation.

For the lawyers, "Capacity building is required for the service providers, Consumer awareness and education, Children online protection initiatives, Capacity building for the legal profession and the Justice department."

Giving his presentation the BOCRA CEO Tshoganetso Kepaletswe, noted to the lawyers that "Cybercrime requires cooperation of the various stakeholder. A national cybersecurity strategy to clarify the roles of the various players. In that vein, capacity building is very important for the legal fraternity to address the issues of cybercrime; Cybersecurity awareness and consumer education of the clients is key for their protection; International and regional treaties are required to address the issues of cybercrime; The use of appropriate electronic tools such as electronic signatures will assist in protecting clients in some of the online deals." He explained that there are multiple international and regional institutions and conventions such as: Budapest Convention on Cybercrime; African Union Convention on Cybersecurity and Personal data protection; Commonwealth Cybercrime Initiative; European Cybercrime Centre; International Telecommunication Union (ITU); UNDOC, UNGA and many more.

"The key requirements of secure electronic signature are: Uniqueness, Impossibility of forgery, Ease of authentication, impossibility of denial. The Secure Electronic Signatures are based on the application to electronic data of an algorithm contained within the data stream which authenticates the identity stream of the sender by encoding the document until the intended recipient unlocks the stream."

As for the relevant act, he said the Act requirements for the Secure Electronic Signature are: The signature creation is, within the context in which it is used, linked to the signatory and to no other

ISSN: 3471-7102, ISBN: 978-9982-70-318-5

person; The signature creation data was, at the time of signing, under the control of the signatory, and to no other person; Any alteration of electronic signature, made after the signing, is detectable to provide assurance and integrity; The standard for accrediting are based on international standard (Chulu J. 2017)

COMESA

COMESA is not also quiet over the cybercrime issue, in its efforts also managed to come up the cyber security concerns enshrined in the ICT policy. The ICT policy and Model Bill for COMESA were adopted by the COMESA policy organs that meat in Khartoum, Sudan in March 2003. Member states proposed integration of their regulatory framework. ICT policy guidelines and strategies adoption included interconnection, licensing, universal access competition and pricing plus consumer protection. The ICT policy advocates for the adoption of appropriate legal and regulatory framework that would ensure and assure the safety of the cyber space.

The COMESA secretariat through the division of infrastructure recently conducted a training and awareness workshop in cyber security for key stakeholders in the performance of the Information Communication and Telecommunication (ICT) sector in Zimbabwe. As the use of cyberspace and ICT networks increases globally threats from a wide variety of sources including criminals, hackers and other agents are manifesting themselves in cyberspace with disruptive criminal activities that target individuals, businesses, national infrastructure and governments.

The main object of the training was to support Zimbabwean government's continued effort to develop strategies, policies, laws and procedures that will improve her ability to ensure the security of cyberspace and critical infrastructures such as telecommunication networks.

The training was also meant to enable participants to learn how to produce effective cyber security national strategies, policies and laws, Computer Incident Response Teams (CIRTs) and PKI (Public Key Infrastructure) laws and regulations. The workshop also enabled participants the opportunity to explore some of the legal and procedural issues related to ensuring the security of cyber networks and effective ways of combating cybercrime including the use of electronic evidence in criminal proceedings, collection and analyzing electronic evidence, searching and seizing computers and cell phones, online investigation and forensic analysis.

ISSN: 3471-7102, ISBN: 978-9982-70-318-5

COMESA secretariat with support from countries with advanced cyber-security institutions namely, Zambia and Sudan conducted the workshop as part of the intra COMESA cooperation in insttutionalising cyber-security and combating cybercrime in the region. COMESA as a regional body has developed an elaborate cyber security programme with activities being undertaken at regional and national levels with a clear road map. The model cyber security policy and bills were developed in 2009 and the main goal of the policy guidelines was to assist member countries in the development of a safe and secure cyberspace within the COMESA region and beyond. (Cyber Security awareness 2016)

AU (African Union)

African governments, the private sector and individuals increasingly rely on the Internet to conduct sensitive transactions and store important data. Most African states are lagging behind in strengthening cybersecurity and fighting cybercrime; cybercriminals have recognized this vulnerability and are targeting the continent. After a lengthy process, the African Union (AU) recently responded to the surge in cybercrime by adopting the Convention on Cyber Security and Personal Data Protection. Stakeholders have raised several concerns about the convention, including that it is too broad in scope. African states should focus on the convention's cybersecurity and cybercrime provisions first, as it is unrealistic to expect states to implement the entire convention in a timely manner. Additionally, African states must embrace capacity-building efforts and join international cybercrime agreements that reach beyond the African continent. These steps will have the most immediate effect in curbing the growth of cybercrime in Africa and worldwide (The AU's cybercrime response 2015).

The convention attempts to address a wide range of online activities, including electronic commerce, data protection, cybersecurity and cybercrime. Regarding cybercrime, it requires African states to adopt laws that criminalise the following:

i. Attacks on computer systems (e.g. fraudulently accessing a computer system)
ii. Computerised data breaches (e.g. fraudulently intercepting data)
iii. Content-related offences (e.g. disseminating child pornography)
iv. Offences relating to electronic message security measures.

Furthermore, the convention emphasises the importance of enhancing international cooperation to fight cybercrime. Article 28 requires states to harmonise cybercrime legislation and regulations to respect the

ISSN: 3471-7102, ISBN: 978-9982-70-318-5

principle of double criminal liability. In order to facilitate information sharing across borders and enhance collaboration on a bilateral and multilateral basis, the convention calls on states without cybercrime mutual legal assistance agreements to try to rectify this deficit. The convention recognizes that building capacity to fight cybercrime is essential, requiring African states to establish appropriate institutions to combat cybercrime and to offer training to those stakeholders tasked with fighting cybercrime. Additionally, it requires that African states enact cybercrime offences that are punishable by effective, proportionate and dissuasive criminal penalties. The convention thus rightly emphasizes the need to create sufficient deterrents to reverse the status quo of criminals turning to cybercrime because it is low risk. Article 32 designates the AU Commission Chairperson as responsible for overseeing the establishment and monitoring of the convention. Among other responsibilities, the Chairperson is required to:

i. Encourage African states to adopt and implement the convention's measures.
ii. Advise African states on how to promote cybersecurity and combat the scourge of cybercrime at a national level
iii. Analyse the nature and magnitude of cybercrime, including gathering information about cybercrime activity in Africa and transmitting such information to the competent national authorities
iv. Establish partnerships with African civil society and governmental, intergovernmental and non-governmental organisations in order to facilitate dialogue on combating cybercrime

3.1.4.2 International efforts

United Nations

The United Nations has done some work as well in the effort to provide some solution to the problem of cybercrime. In this regard, it has successfully hosted over twelve crime congresses and the issues of computer related crimes usually don't miss their agenda. For instance, in the Eighth United Nations Congress held in 1990 in Havana, Cuba. The congress adopted a resolution on computer related crime calling upon its member states to intensify their efforts to combat computer crime (Brenner S. and Schwerha J. 2002). The UN produced a manual also on the prevention and control of Computer related crime in 1995, which examined the law governing such crime and the need for international cooperation when doing investigations. Additionally, likewise workshops were held in the tenth and

ISSN: 3471-7102, ISBN: 978-9982-70-318-5

eleventh congresses, with some focus on public-private sector cooperation among member countries. In December 2000, the UNGA adopted Resolution 55/59, the Vienna Declaration on Crime and Justice. That will enable meeting the challenges of the Twenty-first Century, and as such called for commitment from members states to work toward enhancing their ability to prevent, investigate and prosecute computer related crimes (Chik B. 2004).

The G.8

The G8 has been formulating policy and action plans to deal with high-tech and computer related crimes for over a decade now. In December 1997, representatives from the eight major industrialized nations forming the G8 adopted ten principles and agreed on ten-point action plan to fight international computer related crimes. The leader of the G8 countries endorsed this template and G8 experts forming the Subgroup on High-Tech Crime continue to meet on a regular bases that cooperation on the implementation of the action plan can be achieved. Further, the subgroup was charged with the task of enhancing the abilities of G8 countries to prevent, investigate and prosecute crime involving computers, networked communication and other new technologies. The subgroup meetings are attended by multi-disciplinary delegations that include cybercrime experts, investigators and prosecutors. As part of the holistic strategy, the subgroup closely cooperates with private industries to achieve these ends.

3.2 Discussion and Interpretation of findings

The analysis of the National ICT policy, the Seventh National Development Plan (SNDP) and the Computer Crimes and Misuse Act show the consistency on the part of government's commitment towards improving the ICT sector, that major cybercrime concerns can be addressed. The three documents have indeed tried to address the most essential cyber security concerns and several guides for future legislative reforms. Unfortunately prompt implementation of the policy goals still remain the major challenge. However, government has a urge responsibility of ensuring that implementations of the ICT goals in the SNDP are urgently attained and those of the National ICT policy, that MDG's can

ISSN: 3471-7102, ISBN: 978-9982-70-318-5

be attained through promotion of ICT utilisation. Particularly strategy 1 in the SNDP; that calls for strengthening of legal framework of information and communication technology. Indeed once this is achieved, addressing cybercrime concerns will come to reality, more especially that currently Zambia does not have a comprehensive legal structure to deter and prosecute cybercrime. Although the computer crimes and misuse act number 13 of 2004 now criminalises some cybercrimes but still it does not stop other serious cybercrimes due to the lighter sentences for offenses that otherwise attract heavy punishment.

Finally, Zambia's cyber law legislation should not be designed and formulated in isolation from other countries. This is due to the fact that cybercrime is a serious global challenge and that it calls for well-coordinated international effort if it is to be combated, knowing very well that cybercrime penetrates all countries.

4.0 CONCLUSIONS

Various activities of cyber criminology will continue to grow in scale, complexity and severity worldwide, and the transnational nature of cybercrime will continue to pose legal and operational difficulties for law enforcement agencies. Prevention is therefore still the key strategy in countering the threat of cybercrime.

The Government should foster strong partnerships between industry, higher learning institutions, the public and law enforcement agencies, and forge a sense of shared responsibility in the graft, so that collectively a safe and secure cyberspace environment can be achieved.

It's my sincere prayer and hope that the three bills to be presented in the National Assembly this year of 2018. Will truly be in the interest of the Zambian people and that cyber space will be made a safer place for all internet users in Zambia.

ISSN: 3471-7102, ISBN: 978-9982-70-318-5

5.0 ACKNOWLEDGMENT

Firstly, I would like to thank the almighty God for this wonderful opportunity of being among students of the Information and Communication University (Zambia). In a special way, I thank most sincerely the Zambia Research and Development Centre (ZRDC) team for the partnership with ICU and indeed for this platform allowing different innovations coming forward and share the experience.

This project paper has been made possible because of the dedication from individuals and organisations that willingly assisted in gathering the data. First and foremost, many thanks to my supervisor Dr. Phiri for his contributions to this research paper. Indeed I believe this should be among the best topics of all in the sense that it affects all Zambian's in the Technological umbrella. Should a better approach to cybercrime be implemented, then cybercrime will be combated and make cyberspace safe for all Netzens to work with.

Further, special thanks go to Madam Precious, Dr. Mbulo, Madam Natasha, Choolwe, Suwilanji and Maj. Tembo for the positive contributions to my research paper. To you all I say may our good Lord continue showering abundant blessings on you.

ISSN: 3471-7102, ISBN: 978-9982-70-318-5

6.0 REFERENCE

[1] Brenner S. & Schwerha J. 2002. Transnational Evidence Gathering and Local Prosecution of International Cybercrime, Marshall J. Computer & Info.

[2] Chik B. 2004, Challenges to Criminal Law Making in the New Global Information Society: A critical Comparative study of the Adequacies of Computer-Related Criminal Legislation in the United States, the United Kingdom and Singapore.

[3] Chulu J. 2017, SADC layers discus regional impact of cyber laws. Available at: http://www.biztechafrica.com/article/sadc-lawyers-discuss-regional-impact-cyber-laws/12745/

[4] COMESA holds cyber security awareness 206. Available at: http://www.chronicle.co.zw/comesa-holds-cyber-security-awareness/

[5] Computer crimes and Misuse Act No. 13 of 2004 (Zambia)

[6] EOW, 2005. *Cyber Crime Investigation.* [Online] Available at: http://cybercellmumbai.gov.in/html/cyber-crimes/software-piracy.html

[7] https://www.sardc.net/en/southern-african-news-features/sadc-responds-to-cyber-crime/

[8] Kapumpa D. (2006) Obligatory Essay, The Effectiveness of the Computer Crimes and Misuse Act. 13 of 2004 in combating cybercrime in Zambia

[9] Merrit, M., 2016. Straight Talk about Cyberstalking. *Norton Articles,* Issue https://us.norton.com/cyberstalking/article

[10] National ICT policy of 2007 (Zambia)

[11] Protection of Children Act of 1978 (c. 37) s 1 as amended by the Criminal Justice and Public Order Act of 1994 (c. 33) and the Sexual Offences Act of 2003 (42). Available at http://www.geocities.com.pca_1978/reference/pca_1978amSOA.html

[12] Report on the Seminar held in Mbabane, Swaziland, 5-8th April, 2005 CESPAM EXECUTIVE TRAINING PROGRAM 'CyberLaw Development and Harmonization within SADC'

[13] Seventh National Development Plan for 2017 -2021 (Zambia)

[14] The AU's cybercrime response 2015. Available at: https://www.files.ethz.ch/isn/187564/PolBrief73_cyber