KAMPALA INTERNATIONAL UNIVERSITY

CYBER CRIME AND THE LAW IN UGANDA'S JUSTICE SYSTEMS: A CRITIQUE

BY ABIKO CHARITY

LLB/41321/133/DU

BACHELOR OF LAWS

A DISSERTATION SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE AWARD OF THE DEGREE OF BACHELOR OF LAWS OF KAMPALA INTERNATIONAL UNIVERSITY

MAY 2017

DECLARATION

I declare that this thesis is the work of ABIKO CHARITY alone, except where due acknowledgement is made in the text. It does not include materials for which any other university degree or diploma has been awarded

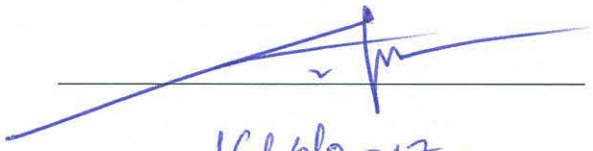
Signature: _____

Date: 16/06/2017.

APPROVAL BY SUPERVISOR

I certify that I have supervised this study and that in my opinion it conforms to the acceptable standards of scholarly presentation and is fully adequate in scope and quality as a dissertation in partial fulfilment for the award of Degree of Bachelors of Laws of Kampala International University.

Name of Supervisor: Mr. WANDERA ISMAIL

Signature: 

Date: 16/6/2017.

DEDICATION

I dedicate this thesis to my paternal aunt, Night Anicia, whose outstanding academic and career achievements have always inspired me to strive to excel; she has been my rock in the most difficult and enduring times and I am truly indebted to her with her unending love and support. The prayers and best wishes from my parents Anguzu David and Adiru Zilly motivated me to work harder. And to my relatives and friends who have been with me through the hustle till this time.

ACKNOWLEDGEMENT

Special thanks to the Almighty God for his blessings and grace that has brought me to the end of this tedious period. To my aunt, Anicia Night, my parents Anguzu David and Adiru Zilly for the unconditional support and words of encouragement, and seeing me through academically regardless of the situation.

I thank my siblings Patricia, Kevin, Perry, Vicky, Moses, and Ewuditt for believing in me and being supportive of the decisions I have taken, you motivated me in a great way.

My heart felt gratitude goes to my supervisor, Mr. Wandera Ismail, for being patient and very supportive of me, your criticism helped me improve and develop my thought process and your encouragement kept me going even when at times I felt I had hit a deadlock. I also thank you, David Banduyo, for your guidance and support that has enabled me successfully complete this project.

I also thank all my friends and relatives who have always been there for me when I needed them – thank you!

Table of Contents

LIST OF STATUTES

The Constitution of the Republic of Uganda, 1995

The Electronics Transactions Act, 2011

The Electronic Signatures Act, 2011

The Uganda Communications Act, 2013

The Regulation of Interception of communications Act, 2010

The Computer Misuse Act, 2011

The Penal Code Act

The Copyright Act

The Information Technology Act, 2000 (India)

Electronic Communications Act, 2005 (South Africa)

LIST OF ACRONYMS

AIDS	Acquired Immune Deficiency Syndrome
ATM	Automated Teller Machine
BoU	Bank of Uganda
CERT	Computer Emergency Response Team
EAC	East African Community
HIV	Human Immunodeficiency Virus
ICT	Information and Communication Technology
ISP	Internet Service Provider
IT	Information Technology
NITA-U	National Information Technology Authority - Uganda
UCC	Uganda Communications Commission
UK	United Kingdom
UN	United Nations
UPF	Uganda Police Force
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
WWW	Worldwide Web

ABSTRACT

This dissertation is based on research about cybercrime and analysis of the laws on cybercrime in Uganda. The data was collected from relevant books and online resources, followed by a critical discussion of the cyber laws in Uganda. The study will help to fill the gap between laws and cyberspace in Uganda and bring benefits to the responsible institutions to initiate legislation specific for cybercrime and amend the laws to meet requirements in a life of digital technology and to give recommendation on issue required to solve the challenge on current legislation. In order to address the research problem, the research explores the rapid growth of cybercrime in the world in general, and statistical evidence of occurrence of cybercrime in Uganda. This paper presents study on the rapid growth of cybercrime situations in Uganda in specific, and finally presents the results and discussions, conclusion and recommendations of the best approach to deal with cybercrimes affecting the information systems.

CHAPTER ONE

1.0 Introduction

Cybercrime is a generic term that refers to all criminal activities done using the medium of computers, internet, cyberspace and the worldwide web.[1]

The council of Europe convention on cybercrime to which United States is a signatory defines cybercrime as a wide range of malicious activities including the illegal interception of data, system interferences that compromise network integrity and availability and copyright infringements.[2]

Accordingly, cybercrime also called computer crime, is any illegal activity that involves a computer or network-connected device such as a mobile phone.

Other forms of cybercrimes include illegal gambling, and sale of illegal items, like weapons, drugs, or counterfeit goods, as well as the solicitation, production, possession or distribution of child pornography.

Cyber-crime is not a new mania in the world, this is due to the fact that the abacus which thought to be the earliest form of computer has been around since 3500 BC. In India, Japan, and China. And thus history reveals that cyber-crime originated far off from the year 1820, as the first landmark instance on cybercrime came up in the year 1820 where a man known as Joseph-Marie Jacquard a textile manufacturer in France produced the loom, this device allowed the repetition of series of steps in weaving of special fabrics. This resulted in fear among

[1] Nfuka, E. N., Sanga, C., & Mshangi, M. 'The Rapid Growth of Cybercrimes Affecting Information Systems in the Global: Is this a Myth or Reality in Tanzania?' (2014) *International Journal of Information Security Science*, *3*(2), 182–99.

[2] Barlow, C. (2016). Cybercrime: Where is it Really Coming From? San Francisco, California.

Jacquards employees that their traditional livelihoods were being threatened, they committed acts of sabotage to discourage Jacquard from further use of the new technology. This is the first recorded cyber-crime.[3]

As those ages of cybercrime have been rapidly increasing in the world, different countries started considering it as a serious legal issue as it emerged to be a natural issue and thus enactment of laws on cybercrimes was of significance to provide for legal recognition of e-commerce, and e-transactions to facilitate e-governance and prevent computer based crimes, as a good example is India where in 2000 they enacted the Information Technology Act.[4] Another country is South Africa, where after many years of uncertainty in the year 2002, there parliament enacted the Electronic Communications Act[5] which comprehensively deals with cybercrimes and has now created legal certainty as to what may and may not constitute cybercrime

Governments have recognized internet as an important tool that can be used in the fight against poverty, disease and environmental degradation, As the world invents deep in to this unknown technological digital revolution, it is becoming inevitable to exclude the challenges that it may come along with, which can manifest themselves through cyber terrorism, electronic bullying and stalking, hacking for fun, identity theft, network intrusions and software piracy.

Cybercrime can be divided in to three categories: crimes in which the computer device is the target, for example to gain access; crimes in which the computer is used as a weapon, for example to launch a denial of services attack; and crimes in which the computer is used as an accessory to a crime for example using a computer to store illegally obtained data.

---

[3] Lefebo, B. B. (2016). History of Cybercrime. Accessed April 21, 2017, from http://www.bezaspeaks.com/cybercrime/history.htm

[4] *The Information Technology Act*, 2000 (India)

[5] *Electronic Communications Act*, 2005 (South Africa)

It is worth noting that the growth of internet has enabled an increase in the volume of cybercrime activities because there is no longer a need for the criminal to be physically present when committing a crime. The internet speed, convenience, anonymity and lack of borders makes computer based varieties of financial crimes such as theft, money laundering or fraud and hate crimes like stalking and bullying easier to carry out.

Cybercrime may be committed by individuals or small groups as well as by criminal organizations that are often spread around the world and committing crimes on an unprecedented scale, cybercrime has the unusual characteristic that the victim and the perpetrator may never come in to direct conduct, in many cases perpetrators and victims are separated by thousands of miles to further reduce the chances of detection and prosecution, cyber criminals often choose to operate in countries with weak or nonexistent cybercrime laws.

The true cost lost to cybercrime is difficult to accurately assess but the world has lost millions of dollars to cybercrime. In addition to this economic impact, cybercrime may have public health and national security implications making computer use a threat to many developing countries. And there is need for a country like Uganda to come up with strict measures on the available statutes or enact a separate statute strictly to cater for cybercrime activities and to punish the perpetrators of the crime.

Cybercrime was first started by hackers trying to break in to computer systems and networks. Some did it just for the thrill of accessing high level security networks but others sought to gain sensitive classified material. Eventually criminals started to infect computers systems with computer viruses which led to break downs on personal and business computers.

1.1 Development of Computer Crime and Cybercrime

The criminal abuse of information technology and the necessary legal response are issues that have been discussed ever since the technology was introduced. Over the last fifty years, various

solutions have been implemented at the national and regional levels. One of the reasons why the topic remains challenging is the constant technical development, as well as the changing methods and ways in which the offences are committed.

1.2 The 1960s

In the 1960s, the introduction of transistor-based computer systems, which were smaller and less expensive than vacuum-tube based machines, led to an increase in the use of computer technology.[6] At this early stage, offences focused on physical damage to computer systems and stored data, for example, in Canada, where in 1969 a student riot caused a fire that destroyed computer data hosted at the university. In the mid-1960s, the United States started a debate on the creation of a central data-storage authority for all ministries. Within this context, possible criminal abuse of databases and the related risks to privacy were discussed.[7]

1.3 The 1970s

In the 1970s, the use of computer systems and computer data increased further at the end of the decade, an estimated number of 100,000 mainframe computers were operating in the United States. With falling prices, computer technology was more widely used within administration and business, and by the public.[8] The 1970s were characterized by a shift from the traditional property crimes against computer systems that had dominated the 1960s, to new forms of crime. While physical damage continued to be a relevant form of criminal abuse against computer systems, new forms of computer crime were recognized. They included the illegal use of computer systems and the manipulation of electronic data. The shift from manual to

[6] Bosworth, S., Kabay, M. E., & Eric, W. (2009). *Computer Security Handbook.* (S. Bosworth, M. E. Kabay, & W. Eric, Eds.) (5th ed.)
[7] Mamandi, K., & Yari, S. (2014). A Global Perspective on Cybercrime. *Humanities and Social Sciences*, *2*(2), 33
[8] ibid

computer-operated transactions led to another new form of crime – computer-related fraud. Already at this time, multimillion dollar losses were caused by computer-related fraud. Computer-related fraud, in particular, was a real challenge, and law enforcement agencies were investigating more and more cases. As the application of existing legislation in computer-crime cases led to difficulties, a debate about legal solutions started in different parts of the world. The United States discussed a draft bill designed specifically to address cybercrime. Interpol discussed the phenomena and possibilities for legal response.[9]

1.4 The 1980s

In the 1980s, personal computers became more and more popular.[10] With this development, the number of computer systems and hence the number of potential targets for criminals again increased. For the first time, the targets included a broad range of critical infrastructure. One of the side effects of the spread of computer systems was an increasing interest in software, resulting in the emergence of the first forms of software piracy and crimes related to patents. The interconnection of computer systems brought about new types of offence. Networks enabled offenders to enter a computer system without being present at the crime scene In addition, the possibility of distributing software through networks enabled offenders to spread malicious software, and more and more computer viruses were discovered. Countries started the process of updating their legislation so as to meet the requirements of a changing criminal environment. International organizations also got involved in the process.

1.5 The 1990s

The introduction of the graphical interface in the 1990s that was followed by a rapid growth in the number of Internet users led to new challenges. Information legally made available in one

[9] ibid
[10] ibid

country was available globally – even in countries where the publication of such information was criminalized.[11] Another concern associated with online services that turned out to be especially challenging in the investigation of transnational crime was the speed of information exchange. Finally, the distribution of child pornography moved from physical exchange of books and tapes to online distribution through websites and Internet services. While computer crimes were in general local crimes, the Internet turned electronic crimes into transnational crime. As a result, the international community tackled the issue more intensively. UN General Assembly Resolution 45/121 adopted in 1990 and the manual for the prevention and control of computer-related crimes issued in 1994 are just two examples.

1.6 The 21st Century

As in each preceding decade, new trends in computer crime and cybercrime continued to be discovered in the 21st century. The first decade of the new millennium was dominated by new, highly sophisticated methods of committing crimes, such as phishing, and botnet attacks, and the emerging use of technology that is more difficult for law enforcement to handle and investigate, such as Voice-over-IP (VoIP).[12] It is not only the methods that changed, but also the impact. As offenders became able to automate attacks, the number of offences increased. Countries and regional and international organizations have responded to the growing challenges and given response to cybercrime high priority.[13]

1.7 Problem Statement

Cyber-crime is a global problem that is engulfing the world at an alarming rate and Uganda is not immune from it. Cybercrime is a unique threat that can be carried out from anywhere

[11] ibid
[12] Gercke, M. (2012). Cybercrime Understanding Cybercrime: Phenomena, Challenges and Legal Response. *ITU Publication.*
[13] Mamandi, above

against any computer system or user in the world. It is a global evil and is becoming increasingly difficult to control. As a result, governments, businesses, and individuals all over the world are facing serious financial impacts and new challenge of combating cybercrimes, its presence and impact has been felt in the country for a considerable period of time, as importantly cyber-crime is not only affecting the governments but citizens as well, it is highly reported that cyber-crimes have been increasing especially in the banks and mobile money transactions where people without knowledge or limited awareness on these technologies have been targeted by cyber criminals.

There is a feeling that internet crime is an advanced type of crime that has not yet infiltrated developing countries in East Africa. The care free nature of the internet in which anybody publishes anything at any time passes a serious security threat for any nation. Unfortunately, there are no formal records about this type of crime for Uganda, there are no mechanisms put in place to regulate such crimes. This has jeopardized justice and peace, and shaken the confidence of citizens in the enjoyment of technology.

The increase of these offences brings a bigger question as to why nothing has so far been done to have lasting legal machinery to combat the situation. The legal environment in Uganda is still inadequate for cyber security in the country. This is because the existing laws do not provide expressly for this evil that is invading the country. This situation poses a serious challenge to Uganda to accommodate modern cybercrimes such as fraud, theft of data, laundering, transmission of harmful codes, unauthorized access of information to impersonation. The government of Uganda is aware of the inadequacy of the legal framework for cybercrimes in the country, yet nothing tangible has been done to curb the situation.

1.8 Hypothesis

The motivation behind this research is analyze the various legislations on cybercrime and to look in depth the status of cybercrime in Uganda.

1.9 Purpose of the Study

i. To discuss the various cybercrime legislations
ii. Find causes of cybercrime in Uganda
iii. To find out a better way of curbing the ongoing internet atrocities among the people of Uganda

1.10 Scope of the Study

This research will look at the current situation in Ugandan laws on cyber-crime that are in place and suggest the best way in which implementation can be greatly effective. This study was confined to the status of cybercrime in Uganda, with reference made to other counties.

1.11 Methodology

This study was done using secondary data. This was made possible thorough documentary review of relevant materials on the subject which included text books, articles, reports, journals, as well as online resources.

CHAPTER TWO

2.0 LITERATURE REVIEW

2.1 Introduction

A literature review is a body of text that aims to review the critical points of current knowledge including substantive findings as well as theoretical and methodological contributions to a particular topic. Literature reviews are secondary sources, and as such, do not report any new or original experimental work. No study can be undertaken without reviewing and analyzing the literature available related to the field of study. Review of literature is an important component of research by which multifaceted understanding of the phenomenon becomes the part of researcher's cognitive personality. Review of literature on cybercrime is to find out what research has already been undertaken in this area; what type of theoretical explanations have been given about this new technological crime which is spreading fast all over the globe; what have been the causes behind occurrence of online crime; and what effect it reflects on the society. Besides all this, it is also worthwhile to find out what laws and legislations are present to deal with cybercrime.

The study of cybercrimes in Uganda is relatively new and as such there is no sufficient amount of literature available on the subject. The review of literature is based on the limited accessible writings and available information. In general, the urgency of harmonizing cybercrime-related reforms in Uganda does not appear to have received the right attention.

Many prominent classical sociologists have contributed towards social thought on social order, effects of science and technology and crime in society. To begin with governments have

invested in the reduction of cybercrime in their respective states. Researchers and engineers have worked out ways that can effectively reduce such crimes and improve their state economy.

Some crimes are new and have evolved with time and technological developments, the rise of unemployment and taste for adventure from people whose target is to terrorize the people with the aim of earning a living with pervasive correlation of human activities with electronic resource and infrastructure comes the ever present use of computer technology

Scholars have done extensive research on cybercrime, though in different perspectives. It is worthwhile to note their viewpoints before reviewing the current literature on technology and crime. The following is the perspective of other researchers and writers.

2.2 Researchers and Authors on Cybercrime

Adam Mambi[14] views cyber security issue from a legal perspective; the author argues that legal framework is an essential aspect for a sustainable cyber security. The premise from this is that as ICT becomes perverse, knowledge and skills advance, traditional and new skills committed are also in increase. Such a situation requires a comprehensive legal environment to ensure that crimes are understood and accommodated through laws, policies, regulations, and guidelines. The legal environment in Uganda is still inadequate for cyber security in the country. This is because the existing laws were developed before the development of computer technology this situation poses a serious challenge to Uganda to accommodate modern cybercrimes such as fraud, theft of data, laundering, transmission of harmful codes, unauthorized access to information, impersonation, etc. This can be achieved by (i) adopting an effective legal framework to combat cybercrime and other misuses of information technology, (ii) enact

[14] Mambi, A. (2012). 'Cyber Security, Challenges and Legal Issues'. In J. Yonazi (Ed.), *Cyber Security in Tanzania*.

enforceable cyber laws in well-defined geographical boundaries that are either national or regional, (iii) fostering international cooperation, information sharing, and investigative assistance.

Martha L Arias, Director of Internet Business Law Services (IBLS)[15] gives a historical background of electronic data discovery and how evidence based on electronic storage was not admissible in court because of lack of skills. The scholar in this case does not suggest ways in which sensitization can be achieved on electronic storage and how electronic storage can be admissible or be used as source of evidence and that it can be relied on.

David Bakibinga, a one-time state prosecutor in Luwero, goes further to expound on the jurisdiction in which such crimes can be committed. He states that globalization of telecommunication significantly enhances the ability of offenders to commit crimes in one country which will affect individuals in variety of other countries and this has profound implications for detecting, investigation, and prosecution of offenders. Therefore, the security of computer and communication systems and their protection against cybercrime is of essence.[16]

Durkheim[17] stressed upon the scientific approach in social thought and viewed a higher rate of crime as inevitable for a modern organic society. He even calls crime as 'functional' because it brings all organs of society together to find a common solution.

According to Marx[18], crime arose as a symptom of the contradictions within capitalism .The contemporary society is dominated by globalized capitalism which has brought in new forms of crime.

[15] Arias, M. L. (2008). Internet Law - Is your Yahoo ID a Means of Identity under the Identity Theft Statute.
[16] Nassali, S. (2010). African governments embark more on setting up Cyber crime prosecution units. Retrieved March 29, 2017, from http://community.telecentre.org/profiles/blogs/african-governments-embark
[17] Durkheim, E., & Halls, W. D. (1984). *The Division of Labour in Society*. London: Macmillan.
[18] Marx, K., & Fowkes, B. (1982). Capital A Critique of Political Economy. Volume 1

Max[19] analyzes society as a 'rational society' built around logic and efficiency rather than on morality or tradition. A modern society is rational society which has seen the emergence of technological specialization, social change and new forms of crime. These classical thinkers expressed their views on technology, crime and its effects on society with a focus on concerns about the changes resulting from technology. Besides they also felt that advancement of technology would result in new forms of crime which are now visible in modern society.

Beck[20]labels the contemporary world as both industrial society and risk society. The indiscriminate use of technology has associated risks which are yet not traceable. Due to the complexity of society and technological advancement, new crimes especially cybercrime have grown creating new type of risk for individuals, organizations and for society.

Castells[21] believes that technology is instrumental and that technology is neither good nor bad, nor is it neutral, it is a force. Technology has changed the societal structure from industrial to network. Network Society is based on nodes of interaction among people all around the globe. However, it has also brought 'Organized global crime'. It is very easy for criminals to plan and conduct crimes with the help of technology.

Wall[22] discusses about the burst of virtual bubble i.e. the new technology which generates great anxiety. According to him internet is a concept that is invented by the media. Therefore, it is the job of criminologist to understand the behaviour that it describes and to assist the understanding of others. The internet influences the criminal and crime in three main ways; first the Internet is a vehicle for communication which sustains existing patterns of harmful activity such as drug trafficking, second, the Internet has created a transnational environment

[19] Weber, M. (1978). *Economy and Society. An Outline of Interpretive Sociology*. (G. Roth & C. Wittich, Eds.). Berkeley: University of California Press

[20] Beck, U. (1992). *Risk Society Towards a New Modernity*. New Delhi: SAGE

[21] Castells, M. (1997). *The Rise of the Network Society*. Oxford: Wiley-Blackwell

[22] Wall, D. (2005). *Crime and the Internet*. Journal of Information Ethics (Vol. 14). London: Routledge

that provides new opportunities for criminals. Wall explains the negative use of technology but he has not given any probable solutions which need to be taken by policy makers to curb it.

Dr. Amos Nungu in his paper outlined two major things. First is that the government has the role and duty of ensuring that there is an adequate legal and practice environment (policies, laws, standards, regulations are available and enforcement mechanism) to allow secure and safe cyber transaction. And secondly, the industry must implement and comply with the international and contextual legal frameworks and industry standards to create for secure digital operations.[23]

Majid[24] provides a sound and concise view of cyber-crime. New crimes appear at a rapid pace and old crimes disappear or change their form and what counts as a crime varies across societies. As Majid Yar highlights, 'academic criminology has been slow to reorient itself to developments arising in the cyber world'. He has discussed at length the emergence and growth of the Internet and the role it plays in a new range of everyday activities, the extent of cyber-criminal activities and what are the problems associated with measuring them. Numerous examples on how cybercrime has posed negative consequence on society are quoted by the author. Various Forms of cybercrime as hacking, pornography, piracy, and online hate speech, e-frauds, and identity theft are discussed at large. One of the important points raised by the author is that crime and deviance cannot always be strictly separated in criminological inquiry. The dynamics in which the boundaries between criminal and deviant are socially negotiated are a recurrent feature of contemporary developments seen around due to the Internet. Cybercrime has posed new challenges for policing and criminal justice as it is an inherently de-territorialized phenomenon. Besides this, new problems arise because of constraints of limited resources and insufficient expertise. An important question which is unanswered by the

[23] Nungu, A. (2009). 'Law Reform Commission of Tanzania'. *Law Reformer Journal*, *2*(1)
[24] Yar, M. (2006). *Cybercrime and Society*. London: Sage Publications.

author is whether information and communications technologies are crime enablers or crime enhancers. Not only this, some of the most recent high tech crimes are not included by Yar. Risks by individuals and organized groups exposed to critical infrastructure that may be due to political or religious motivations and the risks associated with the new payment system. As we are increasingly moving ahead in the technical world, we need to address these upcoming issues.

Jaishankar signifies the fact that criminal justice still lacks suitable and updated knowledge concerning the modern cyber-crime reality. His 'Space Transition Theory' is important to understand cybercrime.[25] Anonymity has further become more criminogenic in virtual space. It has aggravated Deviance and Criminal Subculture in Cyberspace. Social networking victimization especially adolescent victimization has been associated with Routine Activity Theory and Lifestyle Theory. Teenagers explore new technologies because of the freedom these technologies bring, but it also makes them vulnerable to online crime. Although cyber bullying is discussed but within a psychological framework and its social implications are not stated.

Hawthorne[26] explains the increasing use of women in creating a cyber-culture which depict females as cyber babies and cyber-sex objects. The authors have discussed Pornography in detail which is a social trauma. Pornography as one of the first successful e-commerce product has been the foremost crime on the internet. The authors correlate feminism with cyber realm. But other types of cybercrime have not been taken into account by Klien and Hawthrone. They have just focused on women's use in cyber porn and other issues related to cybercrime especially the misuse of social networking sites is not discussed.

---

[25] Jaishankar, K. (2011). *Cyber Criminology: Exploring Internet Crimes and Criminal Behavior*. Boca Raton, FL: CRC Press.

[26] Hawthorne, S., & Klien, R. (2009). *CyberFeminism*. Melbourne: Spinifex Press

Philip[27] warns on the use of pornography on the Internet. According to him, 'Why is so much attention focused on quite innocuous forms of adult material, while something as pernicious as child pornography circulates with such relative case?' It is media, politicians and law agencies who have over responded to online obscenity but have failed to grasp the more serious form of electronic market on child porn. Although other forms of deviant acts have their reputable defenders who assert that these activities should not be severely penalized, but for child pornography, there is no such tolerance. Feminists have long argued that 'Pornography is the theory; rape is the practice'; a corollary declares that 'child pornography is the theory, molestation is the practice'. The writer highlights on the modern history of child porn, which dates from the general relaxation of censorship standards in the 1960s. The writer has examined various laws related to pornography and also questioned about democratizing porn. He argues that the policies outlined are open to debate because other approaches would not have any real effect and might do more harm than good. Even the traditional strategies for deterrence had little impact in this area. The author had little insight on how to eliminate child porn. He left it at the mercy of society. The role of society in the elimination of child porn is very important, but author has not touched upon this issue. The technical and legal aspects have been given more importance as compared to social aspects.

Clarke draws attention on cyber terrorism. He warns that computer can be used for 'Net War' as malicious software can be installed in it even without approval and the users might not know that it is being used against their own country.[28] Cyber terrorism has new scope to reach into cyberspace from physical dimension. It leads to destruction of giant electrical generators, derailing of trains, burning of high power transmission lines, explosion of gas pipelines, crash

---

[27] Jenkins, P. (2001). *Beyond Tolerance: Child Pornography on the Internet*. New York: New York University Press.

[28] Clarke, R. A., & Knake, R. (2009). *Cyber War: The Next Threat to National Security and What to Do About it*. New York: Harper Collins

of aircrafts, and malfunctioning of weapons. Cyber war has the means to launch attack in any part of the world with electronic means. Large scale attack can be easily conducted through internet by abuse of technology. The author surely warns us but he is unable to provide with probable solution to cyber-attacks.

Higgins observes the use of computers and the change in technology due to new advancements.[29] He also cautions the security of internet users and relates this to emergence of cyber-crime. He also examines Cyber pornography which is very much rampant. The author also develops a contextual framework on flow of information on a global level. He discusses hacking as based on technical virtuosity. The advent of computer networking and the popularity of the internet have also given rise to excessive hacking. Not only this, Privacy is at stake because of online transactions are dealt in detail. Higgins suggests that a future effort to safeguard information that is frequently stored in electronic media needs to be analyzed. The knowledge on abuse of technology is very much essential to combat the recent surge in internet related offenses.

Holt emphasizes on four major types of cyber-crimes, namely: cyber trespass, cyber deception/ theft, cyber porn and obscenity and cyber violence.[30] He has discussed various criminological theories in the light of changing trends and patterns of crime. He examines hacking and its various forms. He also analyzed child porn in the light of recent legal developments. In addition, he evaluates the law which addresses cyber bullying and cyber stalking. In his views more researches are needed for creating awareness among the common people who search or 'Google' for anything and almost everything.

---

[29] Higgins, G. (2009). *Cybercrime: An Introduction to an Emerging Phenomenon*. New York: McGraw-Hill.
[30] Holt, T. J. (2011). *Crime Online Correlates, Causes, and Context*. Durham, NC: CAP Press.

2.3 Cybercrime in Africa

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.

A Deloitte survey published in the year 2011, found that banks in Kenya, Rwanda, Uganda, Tanzania and Zambia alone had lost US $245 million to cyber fraud which is quite a lot of money for countries without highly developed banking systems[31]. The aim of this study was to assess the efforts being made by African countries in fighting cybercrime. Towards this direction, specific structures put in place by East and West African countries were reviewed with Africa's capacity to win the fight against cybercrime as an overriding concern. The research revealed that the way forward is for Africa to learn from the experience of developed countries in fighting cybercrime. The fight against cybercrime requires coordinated effort among all stake holders such as government bodies, educational institutions, business organizations and law enforcement authorities.

According to computer security experts, a lot of cybercrime emanates from the African continent, and these 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 programs or specialized training for the law enforcement agencies. Many watchers are warning that Africa is becoming a major source of cyber-crimes; for example, Nigeria is

[31] Quarshie, H. O., & Martin-Odoom, A. (2002). *Fighting* Cybercrime in Africa. *Computer Science and Engineering*, *2*(6).

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.[32]

Cybercrimes are crimes committed on the internet using the computer as either a tool or a targeted victim.[33]. 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.[34] 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. The damage caused is largely psychological and intangible, making legal action against the variants more difficult. These are the crimes which have existed for centuries offline. Scams, theft and other fraudulent activities have existed even before the development of high-tech equipment. The same criminal has simply been given a tool which increases his/her potential pool of victims and makes him all the harder to trace and apprehend. There are numerous crimes of this nature committed daily using the computer and the internet. In achieving the aim of the study, assessing the efforts being made by African countries in fighting cybercrime, the authors interrogated the pervasive nature of the phenomenon of cybercrime. Factors that contributed to the thriving state of this kind of crime was looked at across the African continent, citing the East and West African blocks. The study sought to establish the need for collaboration with developed countries that achieved better results in the fight against cybercrime. Lack of legal framework and the existence of weak infrastructures for dealing with cybercrime in the studied African countries justifies the need for such a study. The involvement

[32] Ibikunle, F., & Odunayo, E. (2013). Approach to Cyber Security Issues in Nigeria: Challenges and Solution. *International Journal of Cognitive Research in Science, Engineering and* Education, *1*(1).

[33] Dalla, S. H., & Geeta, M. (2013). Cyber Crime – A Threat to Persons, Property, Government and Societies. *Ijarcsse*, *3*(5), 997–1002

[34] ibid

of top level government officials, policy makers and implementation groups must be highlighted at all levels of discussion and coupled with cross-border collaboration, is a justifiable route for success in fighting cybercrime.[35]

2.4 Overview of statistics on cybercrime in Uganda[36]

Cybercrime has increased by 14.9% from the previous year. The report indicates that cybercrime focuses on mobile money and Automated Teller Machines (ATM) fraud. MTN alone has transacted through its Mobile Money service a total of US$245 million. Cybercrime targeting mobile money and ATMs accounted for a loss of over $1million country wide. Around $100,000 was transferred without the knowledge or authority of telecom service providers between August and November of 2012. Despite the challenges attributed to crime statistics, the figures reported above are a pointer towards the seriousness of the problem of cybercrime and the danger posed to electronic transactions.

Despite the colossal amounts involved in the mobile money transfer service, there is no statutory framework governing the transactions. The mobile network operators have no obligations to report or disclose info on mobile money services to Bank of Uganda (BoU) as a regulator. There is a general lack of capacity among the police and other law enforcement agencies to detect, investigate and assist in prosecution under the Computer Misuse Act, 2011. This has been a challenge in the prosecution of some high profile cases in the country like ***Uganda Vs Kato Kajubi***[37] and ***Uganda Vs Dr. Aggrey Kiyingi***[38] cases that relied on electronic evidence. In *Kato Kajubi* following a retrial, the accused was convicted. Following the terrorist

[35] Quarshie, H. O., & Martin-Odoom, A. (2002). Fighting Cybercrime in Africa. *Computer Science and Engineering, 2*(6).
[36] Uganda Police Crime Report (2012)
[37] *Uganda v Kato Kajubi Godfrey* (2010) HCT-O6-CRSCO16/2OO9 [2010] UGHC 4
[38] *Uganda v Dr Aggrey Kiyingi And 2 Others* (2006) Criminal Session Case No. 0030 Of 2006 UGHC 52

attack on Kampala on 11th July 2010, the police with the help of the Federal Bureau of Investigation (FBI) were able to uncover emails linking the bombings to the suspects.

There is lack of capacity and funding to enable special skills training required to counter the ever evolving and increasing cybercrime nationally and globally. Uganda does not have adequate data protection laws. Across the East African sub region and the African continent, there is a lack of a harmonized legislative regime to tackle cybercrime. Finally, there is insufficient knowledge about the law and inadequate sensitization of the public and other potential victims of cybercrime

Ugandan laws have not yet been modified to expressly define and condemn computer crimes. The study of cybercrime in Uganda has confirmed that internet users are both victims and perpetrators of internet crimes and all victims do not report to the police. In January 2005 a multibillion dollar scam involving a fraudulent internet bank transfer between standard chartered Bank Nairobi and Barclays Bank Kampala was unveiled.[39]

In July 2004 one lady by the names of Grace Muwagunzi lost her passport and 500 dollars to a fake company claiming to arrange visa and free transport and accommodation in Canada, they used an existing project by the ministry of health by which some official were to travel to Toronto for Training of Trainers course on HIV/AIDS Management, she thought it was a genuine deal when she saw website on the internet concerning the details of the conference.

One company confessed about an incidence of email spoofing in which a supposed employee sent an email to their clients threatening that the aircraft they were using for business was in poor condition and passengers should use it at their own risk. The case was settled outside court after a thorough investigation by an IT specialist and their systems administrator.

[39] Nganda, S. I., & Halima, A. (2005, January). 'Interpol pursues Zzimwe fraud case', *The Weekly Observer*.

In July 2005 the New Vision newspaper[40] broke a story about two pornographic sites hosted in Canada but selling thousands of pictures and videos of Ugandan women having sex. From a report given by a journalist from the Daily Monitor newspaper the titled 'Internet kimansulo targets Ugandans' published on 23rd July 2005 and quoted by Tushabe[41] said "most of the models on the thousands of the nude pictures on kimansulo.com are not actors and many did not know that their pictures were taken while having sex. They were not models nor prostitutes, they were ordinary office workers and university students who go for party, get drunk and end up having a fling with someone they thought was a friend, unknown to them concealed video cameras rolling away recording the minute details of their actions and facial expressions". By the end of August 2005 they had closed their website due to public outcry.

The above statistic shows Ugandans and internet users in Uganda are initiating and falling victims of cybercrimes. The public are not responding to the relevant authorities either because of nonexistent sensitization programs or hopelessness due to the unavailability of e-laws that would bring them justice.[42]

Over 90% reported to have been a victim of at least one cybercrime incident and twenty five percent confessed that they commit at least one wrongful act while in the cyberspace. The victims are mainly prey of SPAM, virus attacks and pornography, while the perpetrators are mostly SPAM senders, intellectual property infringers and hackers. Most Internet crimes are not reported at all because the country does not have a standing law for computer and internet crimes. The public are therefore not protected against these kinds of crimes.

The various trends of the use of internet, experienced cybercrimes, and cybercrimes being involved in is illustrated by the graphs below. Majority of cyber users in Uganda use the

[40] Weddi, D., & Steven, C. (2005, July). 'Porn website sells Ugandans', *Sunday Vision*.
[41] Tushabe, F., & Baryamureeba, V. (2005). Cyber Crime in Uganda: Myth or Reality? In Proceedings of World Academy of Science Engineering and Technology; vol. 8 (pp. 66–70).
[42] ibid

Internet for communication and research. E-mail was the leading activity (48%), followed by research (38%).

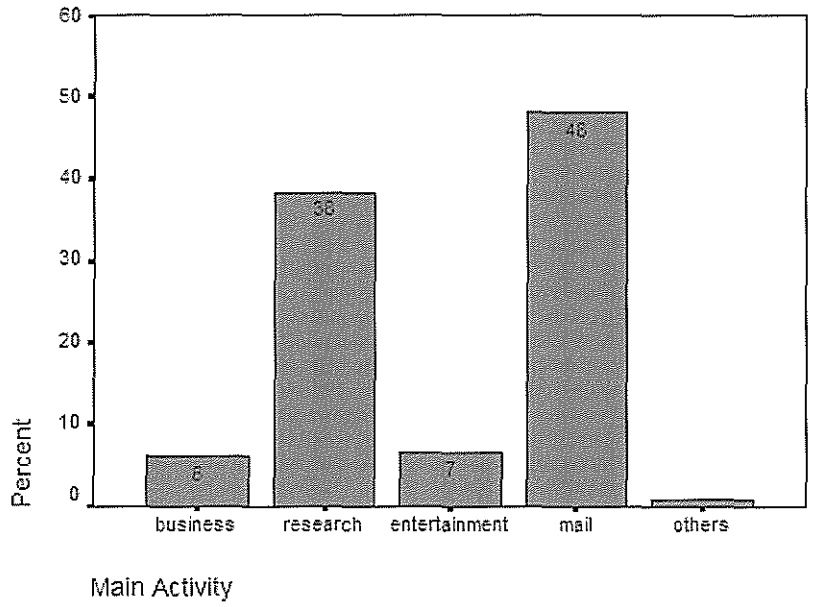
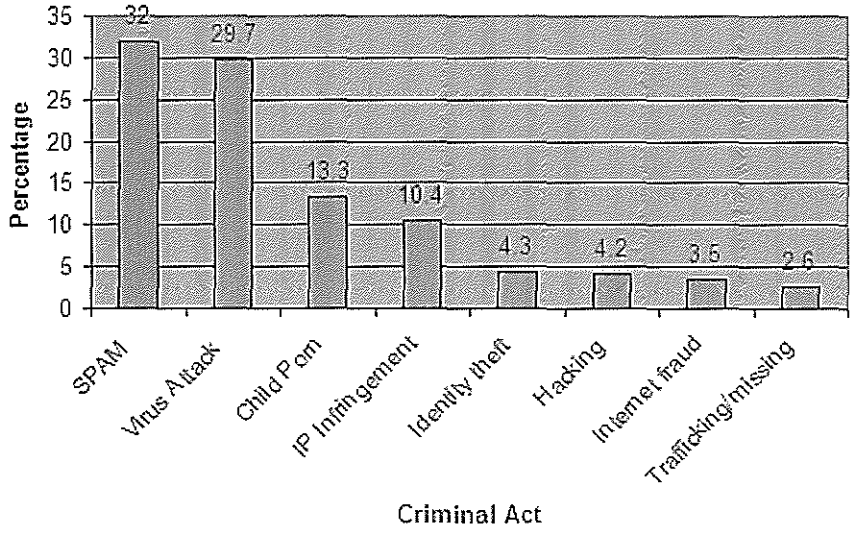


Figure 1: What most cyber citizens in Uganda do while on line[43]

Most internet users have fallen victim of cybercrime with 92% of respondents having been victim of at least one cybercrime. SPAM and virus attacks are the leading incidents reported by victims.



[43] ibid

Figure 2: Experienced cybercrimes[44]

53% of the victims had never told anybody, 34% reported incidences to the System Administrators while 13% told their friends. Most victims prefer to keep quiet because they do not think reporting would help them since preserving evidence is unknown to them. The ones who lost important data are the ones who reported to the system administrators in an attempt to recover it. Internet users in Uganda perform and initiate some wrongful incidents. 25% reported at least one incident they have planned and successfully implemented. SPAM spreaders, intellectual property infringers and hackers are the most rampant.

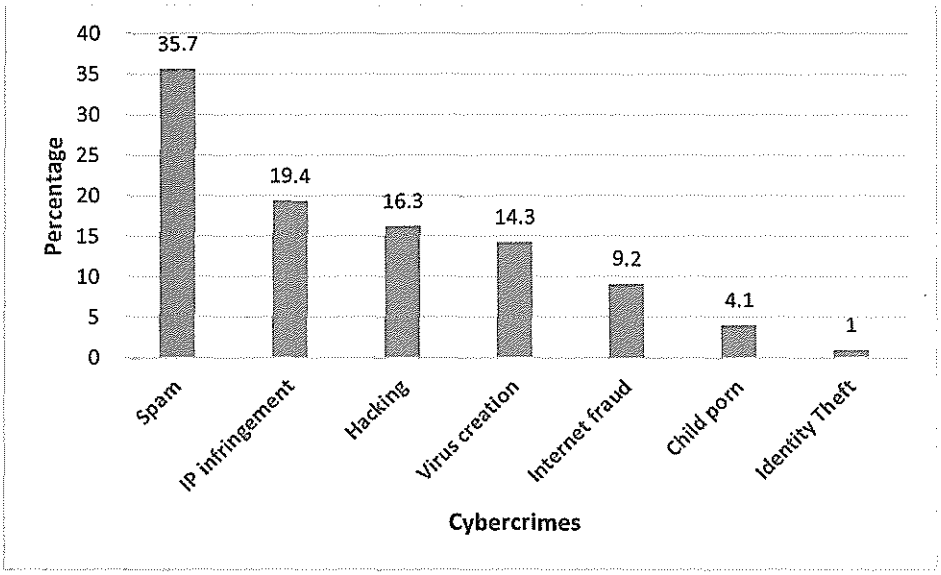


Figure 3: Performed cybercrimes[45]

Internet users are ignorant of ways to detect a computer incident when it occurs. Only 60% are aware of at least one way in which to detect a computer incident and half of these do not have regular system checks. Most perpetuators said that they find it easy to commit these acts because they are protected by a feeling of invisibility while online, the acts are relatively simple to conduct and also for adventure. These statistics show that Ugandans and internet users in

[44] ibid
[45] ibid

Uganda are initiating and falling victim of cybercrime, although the public are not reporting to the relevant authorities either because of non-existent sensitization programs or hopelessness due to the unavailability of e-laws that would bring them to justice.

2.5 Conclusion

From the preceding literature review, it appears that the role of technology is neither good nor bad in itself. It is used as a force to generate energy in society. Nevertheless, cybercrime is the product of technological development. Social networking has become so predominant in our lives because we all are living in 'Network Society'. We are in touch with the world constantly. Although a massive amount of literature has been generated on cybercrime, the ambiguity persists on the impact of technology on society because the effect is still in the infancy stage and much needs to be done.

CHAPTER THREE

3.0 Introduction

This chapter looks at the background to cybercrime in Uganda, the laws that have been enacted in response to cybercrimes, and an analysis of these laws.

3.1 Background of Cybercrime in Uganda.

"Uganda is a developing Country that is facing tremendous economic, political, and social developments, following the first internet connectivity to Uganda, international criminals have intensified on company information systems to destabilize their business operations", Mr Joseph Barungi, General Manager of Africa Online is quoted to have said.[46]

Police records in Uganda do not have any complaint about computer crime and there are no other formal reports about cybercrime rates in Uganda. Does this mean that Internet users in Uganda have not been victims or perpetrators of Internet crimes? Informal and scanty reports about computer crime in Africa and in Uganda particularly result in a misconception that those crimes do not feature there. This deprives decision makers, lawmakers and other stakeholder's vital information that could be exploited for better planning and decision-making.

The cyberspace is the virtual world that internet users inhabit when they are online. It has been defined by Kizza as the concept of an environment made up of invisible information.[47] When computer users log onto the Internet, they are able to perform various tasks and services like

[46] Walter, W. (2010). Uganda on cyber alert. Retrieved May 5, 2017, from http://www.monitor.co.ug/Business/Technology/688612-879612-k8cf2uz/index.html

[47] Kizza, J. M. (2013). Ethical and Social Issues in the Information Age. London: Springer.

browsing the World Wide Web, chatting with fellow cyber citizens, transferring files from one computer to another, remote logging to another computer, sending electronic mail, conducting electronic commerce, video conferencing and more. The many functionalities and freedom of use while in the cyberspace brings an equal ease of committing immoral acts.

The hacking in to networks increased after the arrival of two high speed and capacity fiber optics cables previously with low bandwidth, hackers lacked interest in breaking in to domestic networks because internet connectivity was so slow so they were not interested in wasting their time on systems that too long to respond, but now with first internet, at a click of the buttons the hacker is in to the system.

In the year 2009, the Ministry of Defense was forced to shut down its website after malicious hackers posted anti-Israel statement on the platform.[48]

Informal and scanty reports about computer crimes in Africa and in Uganda in particular in misconception that those crimes do not feature, this deprives the decision of law makers and other stake holders' vital information that could be exploited for betterment and decision making.

The many functionality and freedom of use while in cyber space brings in the commission of immoral acts and crimes. Cyber space crimes are the crimes that arise while in cyber space, and they include crimes like terrorism, intellectual property rights infringement, hacking, industrial espionage, online child exploitation, internet usage policy abuses, illegal purchase of goods, sexual assault, internet fraud, software piracy, viruses, impersonation and many more.

The cybercrimes are universal and hence are similar to the crimes in the rest of the countries in Africa and the world at large

[48] Walter, above

Laws protecting cyber space would protect the victims of cybercrimes to a certain extent by acting as a deterrent measure and also as a means of possible compensation.

Cyber security is a relatively new field as its study is directly related to the rise of digital technologies. This also means that cyber security has evolved apart from most other concepts of security. This notion of security includes protection from disruptions in confidentiality, integrity, availability and often non repudiation of digital technologies and information.

Uganda has recently passed three laws related to the East African Community (EAC) Legal Framework: The Computer Misuse Act, 2011; the Electronic Transactions Act, 2011 and the Electronic Signatures Act, 2011.

The Computer Misuse Act is the principal legislation covering cybercrime. It provides for the safety and security of electronic transactions and information systems, the prevention of unlawful access, abuse or misuse of information systems including computers and for securing the conduct of electronic transactions in a trustworthy environment. The act creates offences with respect to the unauthorized use, access, abuse of computers or data. It also has provisions on electronic fraud, child pornography, cyber harassment, and cyber-stalking.

The Electronic Transactions Act provides for the use, security, facilitation and regulation of electronic communications and transactions as a functional equivalent to the already existing forms of communication. The Act gives legal certainty in respect of validity, legal effect and enforceability of information in electronic form with respect to relations between parties especially establishing contractual obligations. In 2007, prior to the enactment of this Act, the High Court in *Hansa, Emmanuel Onyango vs Aya Investments Ltd, Mohammed Hamid* relied on the exchange of emails between the parties to determine the contractual relations.

The Electronic Signatures Act, 2011 provides for the use of electronic signatures and their regulation. All the three laws have been published and are now in force.

The principal player agencies are: the Ministry of Information Communication Technology, the Uganda Communications Commission, the National Information Technology Authority-Uganda (NITA-U), the Uganda Police Force; and the Judiciary.

As a country, we have gone further to set up a Computer Emergency Response Team (CERT) with all the aforementioned Government agencies being represented on the committee. The Uganda Communications Commission (UCC) has set up its own CERT to compliment the national team and this was set up on the 6th of June 2013.

This CERT prowls the Internet to monitor and report hi-tech crime including cyber terrorism, computer intrusion, online sexual exploitation and cyber fraud. The team also coordinates all other multi sectoral agencies in this fight against cybercrime; liaises with other law enforcement agencies in the prosecution of cyber related crimes and collaborates with other regional and international agencies with similar remits.

3.2 Analysis of the Laws of Uganda on Cybercrimes

Cyber security in Uganda is a relatively new field as its study is directly related to the rise of digital technologies. This also means that cyber security has evolved apart from most other concepts of security. This notion of security includes protection from disruptions in confidentiality, integrity, availability and often non repudiation of digital technologies and information.

Cybercrime explains a criminal activity done using the computer over the internet to perform illegal acts.[49] It is associated with offences to do with computers and the internet, inclusive of misuse of computer systems and data.[50]

[49] Simcoe, T. (2006). Open Standards and Intellectual Property Rights. *Open Innovation: Researching a New Paradigm*, 161–183

[50] Wold, G. (2007). Computer Crime: The Undetected Disaster. *Disaster Recovery Journal.*

In Uganda, the Electronic Signature Act, Computer misuse Act and Electronic Transactions Act have recently been enacted to protect against cybercrime while promoting a safe and environmentally healthy electronic transacting environment. However, with the available legal and institutional framework, the country continues to experience increasing cyber-crimes.[51] Crimes such as cyber terrorism, intellectual property infringement, internet usage policy abuses, internet fraud, industrial espionage and altering of data, on-line child exploitation and pornography, illegal goods purchasing, piracy, impersonation and hacking, remain a challenge.[52] This is yet to involve more undiscovered crime given the pace of advancing technology and while the future of technology remains rich with innovation. In Uganda, a significant percentage of transactions and processes are adopting networking technology.[53] Institutions such as the Ministry of Information and Telecommunication and the Uganda Police Force (UPF) have policy frameworks designed to address cybercrime. UPF is legally mandated by the Constitution to prevent and detect crime[54] in order to ensure that the rule of law prevails.

However, the institution knows little about computer crimes especially in detecting cyber-crimes, and yet these are committed by highly skilled and technical personnel.

In January 2005 for example, Andrew Zzimwe Kasagga together with two Congolese were wanted by Interpol (Kenya) for involving in a multi-million-dollar scam. They were accused of masterminding when they engaged in fraudulent intranet bank transfer between Standard Charted Bank, Nairobi and Barclays Bank Kampala. The Kenyan Standard Chartered Bank staff wired $5million in three installments to separate bank accounts in Kampala. Suspected conmen got the Nairobi based bank to wire one million dollars to Zzimwe's Barclays Bank account in Kampala and another $2 million from Kenya was intercepted at Crane Bank. It had

[51] Ministry of Information and Communications Technology (2011)
[52] Tushabe, F., & Baryamureeba, V. (2005). Cyber Crime in Uganda: Myth or Reality? In Proceedings of World Academy of Science Engineering and Technology; vol. 8 (pp. 66–70).
[53] Florence Tushabe (2004), *Computer Forensics for Cyberspace Crimes*, University of Colombo
[54] The Constitution of the Republic of Uganda 1995, Article 212 (iii)

allegedly been sent to another suspect, Kampala lawyer, Paul Kalemera. While further investigations and trials were being conducted, another $3 million being swindled from Kenya was detected before it was sent to forex bureau via the DFCU bank in Kampala.[55]

To make matters worse, organizations that make use of cyberspace services also lack sufficient information on security controls. This complicates the process of prevention and detection of crime to duly seek police assistance.[56]

This portrays that much as UPF is mandated to combat crime, it requires informational support which is not available because the level of risk identification and evaluation is poor. For example in July 2004, Grace Muwanguzi lost a passport and 500 dollars to a fake company arranging visas, free transport and accommodation in Canada. The company camouflaged under an HIV/AIDS project of Trainer of Trainers course (ToT) by the Ministry of Health where officials were to travel to Toronto. Grace viewed their website over the internet with details of the conference, and met the requirements. On the expected day of returning passports and visas the perpetrators disappeared affecting many others like Grace.[57]

The Ministry of ICT is also mandated to address cybercrime. In Uganda, telecommunications service was monopolized by Uganda Post and Telecommunication Company, prior to the telecommunications sector reforms. Today many private companies such as Airtel, Warid, MTN, UTL and others have come up to offer services with cheap access to internet subscriptions and roaming services. By nature, the services are unregulated and subscriptions are rented out to different subscribers. The Ministry of Information and Communications[58] the regulatory independence of the private companies is making it difficult for law makers and enforcement to address cybercrime while technology keeps changing and requiring timely

[55] Nganda, S. I., & Halima, A. (2005, January). Interpol pursues Zzimwe fraud case. *The Weekly Observer*.
[56] Florence Tushabe (2004), *Computer Forensics for Cyberspace Crimes*, University of Colombo
[57] Kizza, J. M. (2013). Ethical and Social Issues in the Information Age. London: Springer
[58] National Information Security Strategy (2011)

reviews for counter measures moreover under scarcity of funds. This is in addition to lack of technical expertise by those responsible of detecting and combating crime.[59] For example in a recent report by New Vision, MTN lost millions from its Mobile Money Network account by way of scam while Centenary Bank had to issue new ATM cards to its customers to minimize fraud.[60]

In a fully competitive environment of internet providers in Uganda, there would be limited need for regulation, but regulatory authorities still have a critical role to play. The dynamic competitive role of the information and communications sector and the unsettled issues introduced by new technologies affect the regulatory environment. This has prompted the Ministry of Information and Communications Technology to permeate national consciousness for the security ramifications of online activity.[61] Indeed the universal access policies operating among diversity and isolated communications introduce legal challenges in addressing issues of social and political cohesion.[62]

The legal framework is also still limited in scope with changing technology. The Electronic Transaction Act (Electronic Transaction Act 2011 19 (1993) QB 94.C.A provides for the use, security, facilitation and regulation of electronic communications and transactions in addition to encouraging the use of e-government services and providing for matters connected therewith to broadly remove existing legal impediments that can prevent a person from transacting electronically because of the omissions of the traditional laws; making provisions for functional equivalency making paper transactions and electronic transactions to be treated similarly; establishing rules that validate and recognize contracts formed through electronic means and setting out default rules for contract formation and governance of electronic contract

---

[59] The International Telecommunication Union (2002), *Trends in Telecommunication Reform: Effective Regulation*, ITU Regulatory Kit

[60] Nganda, S. I., & Halima, A. (2005, January 13). Interpol pursues ZZimwe fraud case. *Weekly Observer*.

[61] National Information Security Strategy (2011)

[62] The International Telecommunication Union (2002), above

performance; providing the characteristics of a valid electronic writing and an original document; in addition to supporting the admission of computer evidence in courts and arbitration proceedings. However, this will affect the position of judges as prosecutions for Cyber-crime will requires judges to possess enough technical knowledge to be able properly to adjudicate on Cyber-crime cases or else inappropriate acquittals will be exercised as seen in ***R V Cropp***[63] where the jury was misled by trial judge in the application of the Computer Misuse Act, 1990 (UK).

The Electronic Signatures Act[64] regulates the use of electronic signatures and ensures that transactions are carried out in a secure environment; enhances authenticity and security of documents by establishing a public key infrastructure; recognizes different signature creating technologies; and provides effective administrative structures for certification of authorities.

The Computer Misuse Act[65] especially part IV of the Act regulates cybercrime to promote safety and security of electronic transactions and information systems; prevents unlawful access, abuse and misuse of electronic devices like mobile phones including computers and secures the conduct of electronic transactions in a trustworthy electronic environment in addition to providing for other related matters. The cyber laws provide tough penalties for offenders where companies and individuals involved may be de-licensed and if charged in court risk serving up to three years in prison.

However, with supportive laws in place to address cyber-crime, police records in the country reflect few complaints about computer crime with no formal reports about cyber-crime[66] but this does not imply that internet users in Uganda have not fallen victims or perpetrators of major internet crimes. According to Tushabe, the crimes have been on the increase since the

---

[63] *R v Cropp* (1990) Snaresbrook Crown Court 05/07/1991 [1991] 7 CLSR 168, [1991] CL&P July/August 270 Computer Weekly 11 July 1992

[64] *The Electronic Signatures Act*, 2011

[65] *The Computer Misuse Act*, 2011

[66] Tushabe, F., & Baryamureeba, V. (2005). Cyber Crime in Uganda: Myth or Reality? In *Proceedings of World Academy of Science Engineering and Technology; vol. 8* (pp. 66–70)

early 2000 but with informal and scanty reports, thus public gets to know less of it.[67] This reflects a challenge to the law making and enforcement institutions, decision makers and stakeholders in advancing better protective mechanisms.

The Ministry of Information and Communication Technology has also shown a level of interest in developing and protecting abuse of technology. The ministry proposed strategies to establish a national computer incident response team with a 24/7 call center, constituency computer incident response teams, a watch and alert center, and reporting mechanisms. In its framework is to develop a strategy within the government to ensure access and full time availability of organized information and its integrity; keeping abreast with modern, safe and better technologies of information security by considering the trend of globalization; recognizing the contribution of the businesses and organizations in enhancing information security in addition to promoting information protection schemes and mechanisms for assurance.[68] (Despite, this interest, the ministry has little known about the actual issues involved in securing networks and electronic assets. For example, much as internet users are experiencing malicious spread of viruses through emails and these have proved much more than a release of e-mail attachment with greater consequences. Support to secure systems is still difficult. Malicious spread of internet virus is leading to potential losses in productivity by corrupting intellectual assets.[69] Worse still individuals with technical knowledge of networks and networking devices continue to steal sensitive information and money through online access to bank accounts or credit card numbers used by online retailers or conduct a host of juvenile pranks like erasing backup files, raising the temperature in buildings, turning off phone and traffic systems.[70] For instance In ***Uganda v Garuhanga and Mugerwa***[71] computer data was manipulated resulting into 3.8

[67] ibid
[68] National Information Security Strategy (2011)
[69] Racine, G. P. (2005). Legal and Institutional Framework. ITU
[70] National Information Security Strategy (2011)
[71] *Uganda v Garuhanga and Mugerwa* (2004) Unreported, Buganda Road Court, CR 17

Billion Shillings loss for Shell Uganda Ltd. The accused were charged with embezzlement and false accounting as there was no enabling law by then, for charges of computer forgery and computer fraud.

The Ministry also faces challenges in its institutional framework due to non-uniform uptake of ICT by different government ministries, agencies, departments as well as local governments. The level of IT remains different. This being the case different entities have advanced technology differently and their systems therefore vary. While some have information security strategies and policies others do not and while others have higher levels of ICT development and implementation, others do not and require hiring IT services to install, implement and update systems. This leads to infringements of information security. In addition, the lack of top management support and too little financial support in implementing information security measures is also prevalent among agencies and organization making institutional policy difficult.[72]

Much as the country is experiencing various losses and damages caused by fraud, theft, willful neglect, gross negligence, vandalism, sabotage, extortion there is still a general failure to secure adequate funding for information security; a failure to comply with the national laws, contracts, standards in which business operations should be conducted. This has destroyed plans, management and monitoring of performance of technology-related projects, products, services, processes, staff and delivery channels and instead fueled negative effects of public opinion, customer opinion and market reputation. Under such circumstances there is unauthorized disclosure and modification of information due to loss of employee integrity and making inappropriate use of information. For example the money scam faced by MTN.[73] The Ministry

[72] National Information Security Strategy (2011)
[73] Computer Misuse Act, 2011

therefore finds difficulties in managing cohesive issues that arise, more so when support funds remain limited.

Much as the law protects against abusive use of computer,[74] children continue to be exposed to abusive and risky environments. Children are involved in the consumption of pornographic materials as networked by invisible persons. The active online technologies have overlapped the ability of policy implementers to enforce observation of the law while the online environment remains filthy and children below 18 years of age continue to access information and movies meant for adult consumption while perpetrators cannot be brought to justice.[75]

Underreporting affects the performance of police in combating cyber-crimes. The public does not report to authorities because its hope for justice is low having to deal with an invisible criminal. Moreover the perpetrators also feel protected by a feeling of their invisibility.[76]

Indeed, cyber bullying is becoming critical in cybercrime yet its impact is overlooked because it is hard to monitor.[77] For example one company confessed about an incident of email spoofing in which one supposed employee sent an email to their clients threatening that the aircraft they were using for business was in poor condition and passengers should use it at their own risk. Many passengers began canceling their flights for no apparent good reason. The company sought an IT specialist and together with their system Administrator, carried out the investigation which traced the bad email to an employee in a competitor's company. The case was settled out of court.[78]

While all is said and done, Uganda's legal and institutional framework desires a lot to be done. Cybercrime remains on the increase due to continuous use of online computer systems; ability

[74] ibid
[75] Kizza, J. M. (2013). Ethical and Social Issues in the Information Age. London: Springer
[76] ibid
[77] Gardner, W. (2010, June). Protecting and Empowering Children Onlne. Cyber Security Forum
[78] Kizza, J. M. (2013). Ethical and Social Issues in the Information Age. London: Springer

of criminals to hack into the systems, lack of control techniques; in the face of advancing technology.

CHAPTER FOUR

4.0 Challenges Facing the Countering of Cybercrimes in Uganda

4.1 Introduction

This research looked at the current situation regarding the Ugandan laws with respect to cybercrime. In the review of literature on the same subject, we found that cybercrime is the product of technological development. Technology, in and of itself, is neither good nor evil but becomes so depending on the use for which it is made. Cybercrime is cross-boundary and therefore, international. This simple fact has made it quite difficult to control or track down cyber criminals.

The purpose of this chapter is to highlight some of the challenges facing the fight against cybercrimes in Uganda.

4.2 Insufficient Funding

Much as the country is experiencing various losses and damages caused by fraud, theft, willful neglect, gross negligence, vandalism, sabotage, and extortion, there is still a general failure to secure adequate funding for information security. Support, in terms of funding to secure systems, is still low. The ministry in charge of ICT does not have a sufficient operating budget to monitor cyber activities. As such, it is difficult to monitor online devices, especially mobile ones like smartphones and tablets. This makes it easy for children even under the age of eighteen to access adult content without restrictions.

4.3 Non-uniform uptake of ICT

The Ministry of ICT faces challenges in its institutional framework due to non-uniform uptake of ICT by different government ministries, agencies, departments as well as local governments. The level of ICT remains different. This being the case different, entities have advanced technology differently and their systems therefore vary. While some have information security strategies and policies others do not and while others have higher levels of ICT development and implementation, others do not and require hiring IT services to install, implement and update systems. This leads to infringements of information security.

4.4 Reporting of Cyber incidences

Another challenge that is crippling the implementation of these cyber laws is that the public does not report incidences to the authorities. This has happened as a result of lack of confidence in the ability of the relevant authorities to deal with their specific issues. Secondly, the police are not well equipped; the number of smartphones that are stolen in Kampala every day and rarely recovered, paints a bad picture of the ability of the Ugandan police to track cyber criminals.

4.5 Advance in Technology

As technology keeps advancing and changing, so does the perpetrators of cybercrimes. Hackers are getting smarter and using ingenious ways to bypass security systems. This is a challenge in countering cybercrimes in Uganda. An example of this happened during the recent presidential elections, where Uganda Communications Commission (UCC) had issued a directive to service providers to block all social media. Many

Ugandans were able to bypass this measure by using Virtual Private Networks (VPNs) to access WhatsApp, Facebook, and Twitter.[79]

4.6 Difficulty of gathering evidence

Investigators are faced with the challenge of ensuring that the integrity of computer evidence is not distorted as distortion may bring to doubt the entire evidence.[80] There is a lot of caution needed when gathering such evidence and then presenting it in such a way that it will be admissible during a trial. It is quite difficult also to know if any data was not tampered with from a crime scene.

4.7 Lack of ICT forensic experts

With technology advancing at a fast pace, there comes new ways of committing cybercrimes, as mentioned in an earlier point. Legal experts need to acquaint themselves with the ever evolving ways cybercrimes are being committed so that proper legislation can be formulated to counter the new attacks. An example is the recent case of ransomware which was used to attack a big part of the health management system in the United Kingdom (UK).[81] "Ransomware is malicious code that is used by cybercriminals to launch data kidnapping and lockscreen attacks".[82] The motive for ransomware attacks is monetary, and unlike other types of attacks, the victim is usually notified that an exploit has occurred and is given instructions for how to recover from the attack. Payment is often demanded in virtual currency to protect

[79] Musisi, F. (2016, May 13). Uganda: Government Shuts Down Social Media Again. *Daily Monitor*.
[80] Wanyama, E. (2013). The Upsurge of Cyber Crime in Uganda: Where the Gaps and Loops lie; Analysis of the Need for Legislative and Policy Framework. *Makerere Law Journal*, *1*(1), 85–97.
[81] CNN. (2017). UK prime minister: Ransomware attack has gone global. Retrieved May 13, 2017, from http://edition.cnn.com/2017/05/12/health/uk-nhs-cyber-attack/index.html
[82] Techtarget. (2016). Definition of Ransomware. Retrieved May 13, 2017, from http://whatis.techtarget.com/definition/ransomware-cryptovirus-cryptotrojan-or-cryptoworm

the criminal's identity. Although this attack happened in the UK, it could happen anywhere, even here in Uganda.

4.8 Difficulty in apprehending cyber criminals

The Computer Misuse Act, 2011, makes provision for the safety and security of electronic transactions and information systems; to prevent unlawful access, abuse or misuse of information systems including computers and to make provision for securing the conduct of electronic transactions in a trustworthy electronic environment and to provide for other related matters. However, it is a challenge to apprehend cyber criminals since they work anonymously and frequently make use of stolen computers. Also due to the global character of the Internet, a criminal does not need to be in Uganda to commit a crime, which makes it nearly impossible to apprehend the perpetrators of these crimes. In fact, offenders who commit a cybercrime or a computer crime are acting in a new realm, which is now called cyber-space, which is different from the physical world, and which has different jurisdictions and different laws that we can apply.[83]

Finally, digital technologies provide ample opportunities for impersonation by way of identity disguise so as make it difficult if not impossible to ascertain who the perpetrator of cybercrimes is.[84] An innocent person could easily be prosecuted if they are victims of identity theft.

[83] Masadeh, A. M. S. Combating Cyber Crimes – Legislative Approach: A Comparative Study (2015)
[84] Ajayi, E. F. G. (2016). Challenges to enforcement of cyber-crimes laws and policy. *Journal of Internet and Information Systems*, *6*(1), 1–12.

4.9 Conclusion

While Uganda has enacted a number of cyber laws to protect her citizens, the legal and institutional framework desires a lot to be done. Cybercrime remains on the increase due to continuous use of online computer systems; ability of criminals to hack into the systems, lack of control techniques; in the face of advancing technology. Effective ways of apprehending criminals and punishing them need to be sought out if confidence in the legal framework is to be restored.

CHAPTER FIVE

5.0 Conclusion and Recommendation

5.1 Recommendations

I believe that prevention is the best solution to curbing the increasing number security violations on the net. However, it may not be feasible to prevent all incidents, and that is when two major factors come in play. Firstly, forensic knowledge and expertise, followed by the relevant laws that would empower victims to seek justice. This section discusses some few recommendations to that effect.

5.1.1 Sensitization

There is need for setting up a public facility (preferably with a presence on the internet) where victims can report incidences. The public need a lot of sensitization and training on what computer crimes are, in which forms they can manifest, how to detect them, what to do after detection and how to prevent and minimize them. The Police should also endeavor to build trust and confidence in the population by using the media and otherwise, so that more such incidents are reported to them for proper and unified record keeping.

5.1.2 Internet Filtering

Countries implementing Internet filtering at client, Internet Service Provider (ISP) and government levels would prevent access to illegal websites like those promoting concepts like drug use, gambling, immorality, and pornography, bomb making recipes, terrorism and the

like. Legislative organs can mandate a body to filter all incoming web traffic before it is accessed by Internet users in that country and block away websites that pose security threats to the users. Internet Service Providers are also in position to protect their clients against most cyber-attacks like distributed denial of service attacks, email spoofing, SPAM and the like if they were only allowed to do it.

5.1.3 Regulation of Cyber Cafes

A crime committed in a public facility like an internet café will be very hard to detect and identification of the culprit impossible. Setting up policies like supervision of children or always logging onto system resources using the unique identifiers (like smart cards, passports or national identity cards) as usernames will simplify process of tracking the culprits.

5.1.4 Amendment of Laws

Enacting global cyber laws that deal with harmonization and standardization of computer crime would bring us closer to attaining total justice to cybercrime victims. Much as Uganda has enacted some laws namely The Electronics Transactions Act, 2011, The Electronic Signatures Act, 2011, The Uganda Communications Act, 2013, The Regulation of Interception of communications Act, 2010 and The Computer Misuse Act, 2011, these acts do not expressly condemn cybercrime and their implementation has not yielded any fruits as far as cyber-crime prevention is concerned. Although a number of countries have enacted cyber laws and have punished criminals within their jurisdiction, they are dominated by the developed countries. Most developing countries have not yet enacted e-laws and we recommend that they urgently incorporate them into the Laws of the land. Harsh punishments should be given to defaulters

so that people fear to commit these acts and victims motivated to report them. This would prevent escalation of cases and further loss of money, time, data and equipment.

5.1.5 International Co-operation and Further Research

Countries should actively work together and strengthen research activities that will explore new techniques and procedures that will combat the rate at which cybercrime spreads and the ease at which they can be conducted.

5.2 Conclusion

Our study has revealed that cybercrime is silent but common even in the developing countries like Uganda. Cybercrime instances are mainly discussed socially and the victims suffer in silence, while the perpetrators continually hide under the invisibility of the cyber world. As much as 90% of Internet users in Uganda have suffered losses caused by Internet crimes. Furthermore, 25% have confessed to having initiated cybercrimes. It is hard to convict cyber criminals because of two major reasons. Firstly, few countries have enacted e-laws and the existing ones are not sufficient in convicting culprits because of jurisdiction anomalies especially when the investigation transcends international borders. Secondly, obtaining evidence of computer crime that would stand in courts of law is lacking in many countries since the field of computer forensics is still relatively new and lacks sufficient literature and expertise. Cybercrime is a serious threat to the security of cybercitizens and all countries should take it seriously.

REFERENCES

Table of Cases

Uganda

Uganda v Kato Kajubi Godfrey (2010) HCT-O6-CRSCO16/2OO9 [2010] UGHC 4

Uganda v Dr Aggrey Kiyingi and 2 Others (2006) Criminal Session Case No. 0030 Of 2006 UGHC 52

Uganda v. Garuhanga and Mugerwa (Unreported, Buganda Road Court, CR 17 of 2004)

United Kingdom

R v Cropp (1990) Snaresbrook Crown Court 05/07/1991 [1991] 7 CLSR 168, [1991] CL&P July/August 270 Computer Weekly 11 July 1992

Other References

Ajayi, E. F. G. (2016). Challenges to enforcement of cyber-crimes laws and policy. *Journal of Internet and Information Systems*, *6*(1), 1–12.

Arias, M. L. (2008). Internet Law - Is your Yahoo ID a Means of Identity under the Identity Theft Statute. Retrieved March 26, 2017, from https://www.ibls.com/internet_law_news_portal_view.aspx?s=latestnews&id=2378

Barlow, C. (2016). Cybercrime: Where is it Really Coming From? San Francisco, California.

Beck, U. (1992). *Risk Society Towards a New Modernity*. New Delhi: SAGE.

Bosworth, S., Kabay, M. E., & Eric, W. (2009). *Computer Security Handbook*. (S. Bosworth, M. E. Kabay, & W. Eric, Eds.) (5th ed.). New Jersey: John Wiley & Sons.

Castells, M. (1997). *The Rise of the Network Society*. Oxford: Wiley-Blackwell.

Clarke, R. A., & Knake, R. (2009). *Cyber War: The Next Threat to National Security and What to Do About it*. New York: Harper Collins.

CNN. (2017). UK prime minister: Ransomware attack has gone global. Retrieved May 13, 2017, from http://edition.cnn.com/2017/05/12/health/uk-nhs-cyber-attack/index.html

Dalla, S. H., & Geeta, M. (2013). Cyber Crime – A Threat to Persons, Property, Government and Societies. *Ijarcsse*, *3*(5), 997–1002.

Durkheim, E., & Halls, W. D. (1984). *The Division of Labour in Society*. London: Macmillan.

Gardner, W. (2010, June). Protecting and Empowering Children Onlne. *Cyber Security Forum*.

Gercke, M. (2012). Cybercrime Understanding Cybercrime: Phenomena, Challenges and Legal Response. *ITU Publication*.

Hawthorne, S., & Klien, R. (2009). *CyberFeminism*. Melbourne: Spinifex Press.

Higgins, G. (2009). *Cybercrime: An Introduction to an Emerging Phenomenon*. New York: McGraw-Hill.

Holt, T. J. (2011). *Crime Online Correlates, Causes, and Context*. Durham, NC: CAP Press.

Ibikunle, F., & Odunayo, E. (2013). Approach to Cyber Security Issues in Nigeria: Challenges and Solution. *International Journal of Cognitive Research in Science, Engineering and Education*, *1*(1).

Jaishankar, K. (2011). *Cyber Criminology: Exploring Internet Crimes and Criminal Behavior*. Boca Raton, FL: CRC Press.

Jenkins, P. (2001). *Beyond Tolerance: Child Pornography on the Internet*. New York: New York University Press.

Kizza, J. M. (2013). *Ethical and Social Issues in the Information Age*. London: Springer.

Lefebo, B. B. (2016). History of Cybercrime. Retrieved April 21, 2017, from http://www.bezaspeaks.com/cybercrime/history.htm

Mamandi, K., & Yari, S. (2014). A Global Perspective on Cybercrime. *Humanities and Social Sciences*, *2*(2), 33.

Marx, K., & Fowkes, B. (1982). *Capital A Critique of Political Economy. Volume 1*. New York: Vintage Books.

Masadeh, A. M. S. Combating Cyber Crimes – Legislative Approach: A Comparative Study (2015)

Ministry of Law, J. A. C. A. (Legislative D. (2000). The Information Technology Act, 2000. *Jyaistha*, *19*.

Musisi, F. (2016, May 13). Uganda: Government Shuts Down Social Media Again. *Daily Monitor*.

Nassali, S. (2010). African governments embark more on setting up Cyber crime prosecution units. Retrieved March 29, 2017, from http://community.telecentre.org/profiles/blogs/african-governments-embark

Nfuka, E. N., Sanga, C., & Mshangi, M. (2014). The Rapid Growth of Cybercrimes Affecting Information Systems in the Global: Is this a Myth or Reality in Tanzania? *International Journal of Information Security Science*, *3*(2), 182–99.

Nganda, S. I., & Halima, A. (2005, January). Interpol pursues Zzimwe fraud case. *The Weekly Observer*.

Nungu, A. (2009). Law Reform Commission of Tanzania. *Law Reformer Journal*, *2*(1).

Quarshie, H. O., & Martin-Odoom, A. (2002). Fighting Cybercrime in Africa. *Computer Science and Engineering*, *2*(6).

Racine, G. P. (2005). *Legal and Institutional Framework*.

Republic of South Africa. (2006). Electronic Communications Act, 2005. *Government Gazette*, *490*(28743).

Simcoe, T. (2006). Open Standards and Intellectual Property Rights. *Open Innovation: Researching a New Paradigm*, 161–183.

Techtarget. (2016). Definition of Ransomware. Retrieved May 13, 2017, from http://whatis.techtarget.com/definition/ransomware-cryptovirus-cryptotrojan-or-cryptoworm

Tushabe, F., & Baryamureeba, V. (2005). Cyber Crime in Uganda: Myth or Reality? In *Proceedings of World Academy of Science Engineering and Technology; vol. 8* (pp. 66–70).

Wall, D. (2005). *Crime and the Internet. Journal of Information Ethics* (Vol. 14). London:

Routledge.

Walter, W. (2010). Uganda on cyber alert. Retrieved May 5, 2017, from http://www.monitor.co.ug/Business/Technology/688612-879612-k8cf2uz/index.html

Wanyama, E. (2013). The Upsurge of Cyber Crime in Uganda: Where the Gaps and Loops lie; Analysis of the Need for Legislative and Policy Framework. *Makerere Law Journal*, *1*(1), 85–97.

Weber, M. (1978). *Economy and Society. An Outline of Interpretive Sociology*. (G. Roth & C. Wittich, Eds.). Berkeley: University of California Press.

Weddi, D., & Steven, C. (2005, July). Porn website sells Ugandans. *Sunday Vision*.

Wold, G. (2007). Computer Crime: The Undetected Disaster. *Disaster Recovery Journal*.

Yar, M. (2006). *Cybercrime and Society*. London: Sage Publications.