CYBER CRIME IN UGANDA, AN ANALYSIS OF THE LEGAL FRAMEWORK

BY

RACHEAL ROSE WANYANA

1153-01024-01036

A RESEARCH REPORT SUBMITTED TO THE SCHOOL OF LAW IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE AWARD OF BACHELORS DEGREE IN LAWS OF KAMPALA INTERNATIONAL UNIVERSITY

JUNE 2019

DECLARATION

I **Racheal Rose Wanyana** do hereby certify that this material, which I now submit for assessment on the programme of study leading to the award of the bachelors degree in laws is entirely my own work, that I have exercised reasonable care to ensure that the work is original, and does not to the best of my knowledge breach any law of copyright, and has not been taken from the work of others save and to the extent that such work has been cited and acknowledged within the text of my work. I also do declare that this report has never been submitted in any University for any award of a degree.

Sign---------- Date---4/7/2019---

The research work has been done under my supervision and now submitted for examination with my approval as the supervisor;

Mr. KALENGE MUBARAK Date .....9/7/19.....

ACKNOWLEDGEMENTS

This Study could not have materialized without certain people, firstly my Supervisors, Mr. Kalenge Mubarak for his inspiration, encouragement, relentless and tireless technical guidance

DEDICATION

To my Parents Mr. & Mrs. Mwanja Paul and Mr.Baciseze Luc who have seen me through my education journey.

TABLE OF CONTENTS

LIST OF ACROYMNS

CERT- Computer Emergency Response Team

ICT- Information and Commnucation Technology

MoICT- Ministry of Information and Communications Technology

NITA-U- National Information Technology Authority – Uganda

UCC- Uganda Communications Commission

VoIP- Voice over Internet Protocol

ABSTRACT

The study investigated the adequacy of the Cyber crime legal framework in Uganda. The research objectives were to; identify the elements of cyber crime in Uganda; identify the gaps in the cyber crime legal framework in Uganda. A cross-sectional survey research design was used adopting both quantitative and qualitative approaches. The research used a sample of 25 respondents. Purposive sampling was used. Method of data collection was by interviews. Qualitative data was analyzed through content analysis. Findings of the study revealed that Cyber criminals in Uganda take advantage of weaknesses in cybercrime legislation and the nascent systems of law enforcement leading to a proliferation of illicit activities; mainly cross-border prosecutions of Cybercrime are still a challenge for law enforcement agencies. They added that the differences in laws between Uganda (where the victim might be residing) and other countries (where the crime might have originated) were a major limitation. The researcher concluded that there is a failure to regulate cyber crime in Uganda which allows the loss of a lot of resources from the economy. The study recommends that in addition to the criminalization of Cybercrime and the improvement of the ability of law enforcement to combat Cybercrime crime preventions measures need to be developed.

CHAPTER ONE

INTRODUCTION

1.1 Introduction

Cyber crime is not an old sort of crime to the world. It is defined as any criminal activity which takes place on or over the medium of computers or internet or other technology recognized by the Information Technology Act.[1] Cyber crime is the most prevalent crime playing a devastating role in the Modern world. Not only the criminals are causing enormous losses to the society and the government but are also able to conceal their identity to a great extent.[2] There are number of illegal activities which are committed over the internet by technically skilled criminals.[3] This study investigated the adequacy of the Cyber crime legal framework in Uganda. Special attention was given to elements of cyber crime. This chapter presents the background to the study, the statement of the problem, objectives of the study, research question, scope of the study, significance of the study, justification and operational definition of terms and concepts.

1.2 Background

Historically, the introduction of computer-related services or Internet-related technologies has given rise to new forms of crime, soon after the technology was introduced. One example is the development of computer networks in the 1970s; the first unauthorized access to computer networks occurred shortly afterwards.[4] Similarly, the first software offences appeared soon after

[1] Prof. R.K.Chaubey, *"An Introduction to Cyber Crime and Cyber law"*, Kamal Law House, 2012
[2] Ibid.
[3] Ibid.
[4] BBC News, Hacking: A history, 27.10.2000, available at: http://news.bbc.co.uk/1/hi/sci/tech/994700.stm.

the introduction of personal computers in the 1980s, when these systems were used to copy software products.[5]

The process of formulating cyber laws in Uganda was initiated in 2003 when a national taskforce led by the Uganda Law Reform Commission was set up to undertake the exercise.[6]

The formulation and development of cyber laws was part of a wider reform of the commercial justice system in Uganda that started in 2000.[7] The process was undertaken largely to make the law responsive to the changing needs of society.

In Uganda, the advent and development of ICT came with new crimes and this provided a platform for the commission of existing crimes such as fraud, terrorism, money laundering, murder and theft.[8] Although these crimes could be prosecuted under the Penal code Act, ICT related crimes such as hacking and theft of computer programmes or software poised a challenge to the legal system, hence the need to enhance cyber security.

While the Uganda Communications Act and the Electronic Media Act have been in place since 1996,[9] the two laws regulate the telecommunications and broadcasting subsectors without much emphasis on the cyber world. The Electronic Transactions Act, 2011, the Electronic Signatures Act, 2011 and the Computer Misuse Act, 2011 now form the backbone of the legal framework for e-commerce, electronic transactions and computer- or ICT-related communication in Uganda. The three laws became effective on 15th April 2011.[10] However, even with such laws in place

[5] Ibid.
[6] Ibid.
[7] Uganda Law Reform Commission: A Study Report on Electronic Transactions Law, ULRC Publication No. 10 of 2004.
[8] P. Mwaita and M. Owor, Workshop report on effective Cybercrime legislation in Eastern Africa, Dar es salaam, Tanzania, 22-24 August 2013.

[9] Chapter 104 and 106 of the Laws of Uganda, Revised Edition (2000)
[10] By virtue of section 1 of the Act the Minister responsible for ICT was given power to appoint a date when the Act would become effective as law. The Minister appointed 15th April, 2011.

Cyber crime has increased by 14.9% since 2013. The report indicates that cyber crime 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.[11] Cyber crime 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.[12] 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. Therefore this study investigated the adequacy of the Cyber crime legal framework in Uganda.

1.3 Problem Statement

The existence of cyber laws notwithstanding, cyber crime continues to rise. The lack of capacity among law enforcement units of government coupled with the lack of awareness on the part of the community and the fact that our virtual borders are open raises questions regarding Uganda's capability to combat cyber crime. Therefore this study investigated the adequacy of the Cyber crime legal framework in Uganda.

1.4 General Objective

The study aimed to investigate the adequacy of the Cyber crime legal framework in Uganda.

1.5 Specific Objectives

i. To identify the elements of cyber crime in Uganda.

[11] P. Mwaita and M. Owor, Workshop report on effective Cybercrime legislation in Eastern Africa, Dar es salaam, Tanzania, 22-24 August 2013.

[12] Ibid.

ii. To identify the gaps in the cyber crime legal framework in Uganda.

iii. To make necessary recommendations towards regulation of cyber crime in Uganda.

1.6 Research Questions

This study was guided by the following research questions:

i. What are the elements of cyber crime in Uganda?

ii. What are the gaps in the cyber crime legal framework in Uganda?

iii. What are the necessary recommendations towards regulation of cyber crime in Uganda?

1.7 Scope

1.7.1 Geographical Scope

The study was done in Kampala Capital City Authority situated 0◦15_N and 32◦30_E and is located 45 km north of the Equator. Kampala is located on the northern shores of Lake Victoria in the South East of Uganda and is bordered by Wakiso District to the North, East, West and South-west, covering an area of 195 km2.[13] This area was chosen because of proximity and ease of access to information.

1.7.2 Content Scope

The study was confined to analyzing the laws that have a bearing on Cyber crime to find out whether these laws were adequate. The study was specifically focused on elements of cyber crime and the gaps in the cyber crime legal framework in Uganda.

[13] Humphrey, H. and Water, T.: 2010, *Solid Waste Disposal, Kampala*. Revised Draft Report Seven Towns Project by GTZ/World Bank. Ministry of Water and Mineral Development and Ministry of Local Government.

1.7.3 Time Scope

The information collected covered a period of 10 years (2008-2018) because many cyber crime legal frameworks were enacted[14]

1.7 Significance of the Study

The study findings will be used in the formulation of policies and the laws to regulate and reduce Cyber crime in Uganda.

The study finding will help the various stakeholders to appreciate the laws on enhancing and creating a Cyber crime free country.

1.8 Justification of the Study

The need to protect the current population of about 37 million Ugandans from threats like terrorism and economic crime most especially now as the crime rate associated to computers is at 14.8%, cannot be over stated.[15] It is imperative therefore that a concerted joint effort, both nationally and internationally is taken to ensure that compromise to ICT is either eliminated or reduced to the minimum levels in Uganda and that no country in East Africa is used as a hub to infringe the virtual borders of member states.

1.9 Operational Definitions

Cybercrime: relates to offences committed with the use of a computer, a phone and internet networks.

---

[14] ibid

[15] P. Mwaita and M. Owor, Workshop report on effective Cybercrime legislation in Eastern Africa, Dar es salaam, Tanzania, 22-24 August 2013.

Electronic evidence: electronic evidence originates from the drives of electronic devices or computers and may be volatile (retrievable) and non- volatile forms of electronic evidence.

Threats: threats include: cyber crime attackers committing economic crimes which affect the population. There is also a potential for the commission of political crimes with serious governance consequences. Cybercrime can cause damage to computer systems through virus attacks (sabotage).

CHAPTER TWO

LITERATURE REVIEW

2.1 Introduction

This chapter contains a discursive prose about the adequacy of the Cyber crime legal framework; it is organized around the study themes of; cyber crime legal framework; and elements of cyber crime respectively.

2.2. Cyber crime Legal Framework

2.2.1 The Anti-Terrorism Act, 2002

The Anti-Terrorism Act (ATA) was adopted in 2002 and includes provisions that provide for obtaining information in respect of acts of terrorism. This includes the authorizing of the interception of the correspondence and the surveillance of persons suspected to be planning or to be involved in acts of terrorism.

Section 9(1) states that any person who establishes, runs or supports any institution for promoting terrorism, publishing and disseminating news or materials that promote terrorism or training or mobilising any group of persons or recruiting persons for carrying out terrorism or mobilising funds for the purpose of terrorism commits an offence and shall be liable on conviction, to suffer death.[16] It is further laid down in Section 9(2) of the ATA that any person who, without establishing or running an institution for the purpose, trains any person for carrying out terrorism, publishes or disseminates materials that promote terrorism, commits an offence and shall be liable on conviction, to suffer death.[17]

[16] The Anti-Terrorism Act, 2002
[17] The Anti-Terrorism Act, 2002

2.2.2 The National Information Technology Authority, Uganda Act, 2009

This law establishes the National Information Technology Authority in Uganda (NITA-U). It is a government agency under the general supervision of the minister responsible for information technology (Section 3 (3) and Section 2).[18] The goals of the NITA-U listed in Section 4 include diverse ways to promote information technology in Uganda and most of these aims are commendable. The functions of the NITA-U listed in Section 5 are many (18) and rather broadly formulated.[19] Section 5 (18) extends the functions of the authority to undertake any other activity necessary for the implementation of the objects of the authority.

2.2.3 The Regulation of Interception of Communications Act, 2010

The Regulations of Interception of Communications Act (RICA) is probably the most problematic law when it comes to guaranteeing the Internet freedom of Ugandan citizens. Section 3 of RICA provides for the establishment of a Monitoring Centre for the interception of communications under the act.[20] The minister responsible for security is mainly responsible for establishing and running the centre.

An application for the lawful interception of any communication may be made by the Chief of Defence Forces, the Director General of the External Security Organisation, the Director General of the Internal Security Organisation, the Inspector General of Police or their nominees (Section 4 (1)), also referred to as authorized persons (Section 1). A warrant to intercept communications shall be issued by a designated judge, by which is understood a judge designated by the Chief Justice to perform the functions of a designated judge for purposes of RICA (Section 1).

[18] The National Information Technology Authority, Uganda Act, 2009
[19] Ibid.
[20] The Regulation of Interception of Communications Act, 2010

2.2.4 The Electronic Signatures Act, 2011

The Electronic Signatures Act (ESA) regulates the use of electronic signatures in Uganda. While promoting the use of electronic signatures can generally be regarded as a positive development, there are some aspects of ESA that can be seen as creating risks in relation to individuals' right to privacy and freedom of expression.[21] ESA for example includes provisions on advanced electronic signature that are uniquely linked to signatory, reliably capable of identifying the signatory and linked to the data to which it relates in such a manner that any subsequent change of the data or the connections between the data and signature are detectable (Section 2).[22] In case the security of these types of signatory systems is not adequate, the anonymity of a person's online behaviour can be threatened due to the possibility to identify the individual through his or her signature. 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.

2.2.5 The Computer Misuse Act, 2011

The Computer Misuse Act (CMA) prescribes liability for offences related to computers. For example child pornography, cyber harassment, offensive communications, and cyber stalking are penalized under CMA.[23] The maximum penalties for these offences range from one to five years of prison, with the exception of child pornography, which can generate the maximum prison sentence of 15 years.[24] The conditions required for these offences to be at hand are, however, often rather vaguely defined. This both contravenes the requirement of unambiguous and foreseeable provisions in international law and can have a hampering effect on freedom of expression.

[21] The Electronic Signatures Act, 2011
[22] The Electronic Signatures Act, 2011
[23] The Computer Misuse Act, 2011
[24] The Computer Misuse Act, 2011

2.2.6 The Electronic Transactions Act, 2011

The Electronic Transactions Act (ETA) provides for the use, security, facilitation and regulation of electronic communications and transactions. As regards possible threats to Internet freedom, ETA contains above all pertinent provisions concerning the liability of Internet service providers. It is stipulated in Section 29 that a service provider shall not be subject to civil or criminal liability in respect of third-party material which is in the form of electronic records to which he or she merely provides access if the liability is founded on the making, publication, dissemination or distribution of the material or a statement made in the material or the infringement of any rights subsisting in or in relation to the material.[25]

2.2.7 The Uganda Communications Act, 2013

The Uganda Communications Act (UCA) regulates the Ugandan communications services. It provides for the establishment of the Ugandan Communications Commission (UCC) (Section 4).[26] Functions of the UCC include e.g. to monitor, inspect, licence, supervise, control and regulate communications services (b), to receive, investigate and arbitrate complaints relating to communications services and take necessary action (j) and establish an intelligent network monitoring system to monitor traffic, revenue and quality of service of operators (u) and to set standards, monitor and enforce compliance relating to content (x) (Section 5).[27] The UCC shall exercise its functions independently (Section. 8) while the Minister may, in writing, give policy guidelines to the Commission regarding the performance of its functions and it shall comply with these guidelines (Section 7).

[25] The Electronic Transactions Act, 2011
[26] The Uganda Communications Act, 2013
[27] Ibid.

2.2.8 The Anti-Pornography Act, 2014

The Anti-Pornography Act (APA) was adopted in 2014 and criminalizes all forms of pornography. According to Section 13(1), a person shall not produce, traffic in, broadcast, procure, import, export, sell or abet any form of pornography. An offence under this paragraph can result in a prison sentence of maximum ten years (Section 13 (2)).[28] Section 14(1) criminalizes the same actions concerning child pornography in which case the maximum sentence is fifteen years.[29] The realization of APA is overseen by the Pornography Control Committee established in Part II.

2.3 Institutional Framework

The principal player agencies are: the Ministry of Information Communication Technology, the Uganda Communications Commission, the National Information Technology Act-Uganda (NITA-U), the Uganda Police Force; and the Judiciary. Uganda has 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 cyber crime; liaises with other law enforcement agencies in the prosecution of cyber related crimes and collaborates with other regional and international agencies with similar remits.

[28] The Anti-Pornography Act, 2014.

[29] Ibid.

2.4 Elements of cyber crime in Uganda

The Concept of cyber crime is very different from the traditional crime.[30] Also due to the growth of Internet Technology, this crime has gained serious and unfettered attention as compared to the traditional crime. So it is necessary to examine the peculiar characteristics of cyber crime.

Cyber crimes can only be committed through the technology, thus to commit this kind of crime one has to be very skilled in internet and computers and internet to commit such a crime. The people who have committed cyber crime are well educated and have deep understanding of the usability of internet, and that's made work of police machinery very difficult to tackle the perpetrators of cyber crime. In cyberspace the geographical boundaries reduced to zero. A cyber criminal in no time sitting in any part of the world commit crime in other corner of world. For example a hacker sitting in India hack in the system placed in United States.

In cyberspace the geographical boundaries reduced to zero. A cyber criminal in no time sitting in any part of the world commit crime in other corner of world. For example a hacker sitting in India hack in the system placed in United States. It is very difficult to collect evidence of cyber crime and prove them in court of law due to the nature of cyber crime. The criminal in cyber crime invoke jurisdiction of several countries while committing the cyber crime and at the same time he is sitting some place safe where he is not traceable.[31]

The cyber crime has the potential of causing injury and loss of life to an extent which cannot be imagined. The offences like cyber terrorism, cyber pornography etc has wide reach and it can

[30] Aghatise E. Joseph, "Cyber Crime Definition", Cyber Crime Research Centre (Last modified on June 28, 2006), *available at:* http://www.scribd.com/document/195552552/Cybercrime-Definition (visited on Feb. 22. 2017).

[31] David Decary Hetu and Carlo Morselli, "Gang Presence in Social Network Sites", *International Journal of Cyber Criminology,* vol. 5 No. 2, July- Dec., 2011, p. 876, *available at:* http:// www.cybercrimejournal.com/davidcarlo2011julyijcc.pdf (visited on Oct. 8, 2012).

destroy the websites, steal data of the companies in no time.[32] This section gives an overview of the most commonly occurring offences included in this category.

2.4.1 Illegal access (hacking, cracking)

The offence described as "hacking" refers to unlawful access to a computer system, one of oldest computer-related crimes.[33] Following the development of computer networks (especially the Internet), this crime has become a mass phenomenon.[34] Famous targets of hacking attacks include the US National Aeronautics and Space Administration (NASA), the US Air Force, the Pentagon, Yahoo, Google, eBay and the German Government.[35] Examples of hacking offences include breaking the password of password-protected websites and circumventing password protection on a computer system. But acts related to the term "hacking" also include preparatory acts such as the use of faulty hardware or software implementation to illegally obtain a password to enter a computer system[36], setting up "spoofing" websites to make users disclose their passwords[37] and installing hardware and software-based keylogging methods (e.g. "keyloggers") that record every keystroke – and consequently any passwords used on the computer and/or device.[38]

---

[32] M. Dasgupta, *Cyber Crime in India- A Comparative Study*, 2009, p.8.
[33] See *Levy*, Hackers, 1984; Hacking Offences, Australian Institute of Criminology, 2005, available at: www.aic.gov.au/publications/htcb/htcb005.pdf;
[34] *Sieber*, Council of Europe Organised Crime Report 2004, page 65.
[35] For an overview of victims of hacking attacks, see: http://en.wikipedia.org/wiki/Timeline_of_computer_security_hacker_history; *Joyner/Lotrionte*, Information Warfare as International Coercion: Elements of a Legal Framework, EJIL 2002, No5 – page 825 *et seq.*; Regarding the impact, see *Biegel*, Beyond our Control? The Limits of our Legal System in the Age of Cyberspace, 2001, page 231 *et seq.*
[36] *Musgrove*, Net Attack Aimed at Banking Data, Washington Post, 30.06.2004.
[37] *Sieber*, Council of Europe Organised Crime Report 2004, page 66.
[38] *Sieber*, Council of Europe Organised Crime Report 2004, page 65. Regarding the threat of spyware, see *Hackworth*, Spyware, Cybercrime and Security, IIA-4.

2.4.2 Illegal data acquisition (data espionage)

Sensitive information is often stored in computer systems. If the computer system is connected to the Internet, offenders can try to access this information via the Internet from almost any place in the world.[39] The Internet is increasingly used to obtain trade secrets. The value of sensitive information and the ability to access it remotely makes data espionage highly interesting. In the 1980s, a number of German hackers succeeded in entering US government and military computer systems, obtaining secret information and selling this information to agents from a different country.[40]

2.4.3 Illegal interception

Offenders can intercept communications between users[41] (such as e-mails) or other forms of data transfers (when users upload data onto webservers or access web-based external storage media) in order to record the information exchanged. In this context, offenders can in general target any communication infrastructure (e.g. fixed lines or wireless) and any Internet service (e.g. e-mail, chat or VoIP communications).[42] Most data-transfer processes among Internet infrastructure providers or Internet service providers are well protected and difficult to intercept.[43] However, offenders search for weak points in the system.

---

[39] BBC News, "UN's website breached by hackers", available at: http://news.bbc.co.uk/go/pr/fr/-/2/hi/technology/6943385.stm

[40] Annual Report to Congress on Foreign Economic Collection and Industrial Espionage – 2003, page 1, available at: www.ncix.gov/publications/reports/fecie_all/fecie_2003/fecie_2003.pdf.

[41] *Jakobsson*, The Human Factor in Phishing, available at: www.informatics.indiana.edu/markus/papers/aci.pdf; *Gercke*, Computer und Recht 2005, page 606.

[42] *Braverman*, VoIP: The Future of Telephony is now...if regulation doesn't get in the way, The Indian Journal of Law and Technology, Vol.1, 2005, page 47

[43] ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 30, available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

Wireless technologies are enjoying greater popularity and have in the past proved vulnerable.[44] Nowadays, hotels, restaurants and bars offer customers Internet access through wireless access points. However, the signals in the data exchanges between the computer and the access point can be received within a radius of up to 100 metres. Offenders who wish to intercept a data-exchange process can do so from any location within this radius. Even where wireless communications are encrypted, offenders may be able to decrypt the recorded data.

2.4.5 Data interference

Computer data are vital for private users, businesses and administrations, all of which depend on the integrity and availability of data.[45] Lack of access to data can result in considerable (financial) damage. Offenders can violate the integrity of data and interfere with them by deleting, suppressing or altering computer data.[46] One common example of the deletion of data is the computer virus.[47] Ever since computer technology was first developed, computer viruses have threatened users who failed to install proper protection. Since then, the number of computer viruses has risen significantly. Not only has the number of virus attacks increased, but also the techniques and functions of viruses (payload) have changed.[48]

2.4.6 System interference

The same concerns over attacks against computer data apply to attacks against computer systems. More businesses are incorporating Internet services into their production processes,

---

[44] *Kang*, Wireless Network Security – Yet another hurdle in fighting Cybercrime, in Cybercrime & Security, IIA-2, page 6 *et seq.*

[45] ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 32, available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

[46] *Sieber*, Council of Europe Organised Crime Report 2004, page 107.

[47] *Spafford*, The Internet Worm Program: An Analysis, page 3; *Cohen*, Computer Viruses – Theory and Experiments, available at: http://all.net/books/virus/index.html

[48] *Kabay*, A Brief History of Computer Crime: An Introduction for Students, 2008, page 23, available at: www.mekabay.com/overviews/history.pdf.

with benefits of 24-hour availability and worldwide accessibility.[49] If offenders succeed in preventing computer systems from operating smoothly, this can result in great financial losses for victims.[50] Attacks can be carried out by physical attacks on the computer system. If offenders are able to access the computer system, they can destroy hardware. For most criminal legal systems, remote physical cases do not pose major problems, as they are similar to classic cases of damage or destruction of property. However, for highly profitable e-commerce businesses, the financial damages caused by attacks on the computer system are often far greater than the mere cost of computer hardware.[51]

2.4.7 Erotic or pornographic material

Sexually-related content was among the first content to be commercially distributed over the Internet, which offers advantages to retailers of erotic and pornographic material including: exchange of media (such as pictures, movies, live coverage) without the need for cost-intensive shipping;[52] worldwide access, reaching a significantly larger number of customers than retail shops; the Internet is often viewed as an anonymous medium (often erroneously); an aspect that consumers of pornography appreciate, in view of prevailing social opinions.[53]

---

[49] *Power*, 2000 CSI/FBI Computer Crime and Security Survey, *Computer Security Journal*, Vol. 16, No. 2, 2000, page 33 *et seq.*

[50] *Campbell/Gordon/Loeb/Zhou*, The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence From the Stock Market, Journal of Computer Security, Vol. 11, page 431-448.

[51] *Campbell/Gordon/Loeb/Zhou*, The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence From the Stock Market, Journal of Computer Security, Vol. 11, page 431-448.

[52] *Haraszti*, Preface, in Governing the Internet Freedom and Regulation in the OSCE Region, available at: www.osce.org/publications/rfm/2007/07/25667_918_en.pdf.

[53] *Ropelato*, Internet Pornography Statistics, available at: http://internet-filter-review.toptenreviews.com/internetpornography-statistics.html.

Recent research has identified as many as 4.2 million pornographic websites that may be available on the Internet at any time.[54] Besides websites, pornographic material can be distributed through file-sharing systems and instant messaging systems. Different countries criminalize erotic and pornographic material to different extents. Some countries permit the exchange of pornographic material among adults and limit criminalization to cases where minors access this kind of material, seeking to protect minors.[55]

2.4.8 Illegal gambling and online games

Internet games and gambling are one of the fastest-growing areas in the Internet.[56] Linden Labs, the developer of the online game Second Life, reports that some ten million accounts have been registered.[57] Reports show that some such games have been used to commit crimes, including the exchange and presentation of child pornography, fraud, gambling in virtual online casinos and libel (e.g. leaving slanderous or libellous messages). Some estimates project growth in estimated online gambling revenues from USD 3.1 billion in 2001 to USD 24 billion in 2010 for Internet gambling (although compared with revenues from traditional gambling, these estimates are still relatively small).[58]

---

[54] *Ropelato*, Internet Pornography Statistics, available at: http://internet-filter review.toptenreviews.com/internetpornography-statistics.html.

[55] ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 36, available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

[56] *Brown/Raysman*, Property Rights in Cyberspace Games and other novel legal issues in virtual property, The Indian Journal of Law and Technology, Vol. 2, 2006, page 87 *et seq*.

[57] *Harkin*, Get a (second) life, Financial Times, available at: www.ft.com/cms/s/cf9b81c2-753a-11db-aea1-0000779e2340.html.

[58] *Olson*, Betting No End to Internet Gambling, Journal of Technology Law and Policy, Vol. 4, Issue 1, 1999, available at: http://grove.ufl.edu/~techlaw/vol4/issue1/olson.html.

2.4.9 Fraud and computer-related fraud

Computer-related fraud is one of the most popular crimes on the Internet,[59] as it enables the offender to use automation and software tools to mask criminals' identities. Automation enables offenders to make large profits from a number of small acts. One strategy used by offenders is to ensure that each victim's financial loss is below a certain limit. With a "small" loss, victims are less likely to invest time and energy in reporting and investigating such crimes. One example of such a scam is the Nigeria Advanced Fee Fraud.[60]

Although these offences are carried out using computer technology, most criminal law systems categorize them not as computer-related offences, but as regular fraud.[61] The main distinction between computer related and traditional fraud is the target of the fraud. If offenders try to influence a person, the offence is generally recognized as fraud. Where offenders target computer or data-processing systems, offences are often categorized as computer-related fraud. Those criminal law systems that cover fraud, but do not yet include the manipulation of computer systems for fraudulent purposes, can often still prosecute the above-mentioned offences. The most common fraud offences include online auction fraud and advanced fee fraud.

2.4.10 Misuse of devices

Cybercrime can be committed using only fairly basic equipment.[62] Committing offences such as libel or online fraud needs nothing more than a computer and Internet access and can be carried out from a public Internet café. More sophisticated offences can be committed using specialist software tools. The tools needed to commit complex offences are widely available over the

[59] *Sieber*, Council of Europe Organised Crime Report 2004, page 113.
[60] *Reich*, Advance Fee Fraud Scams in-country and across borders, Cybercrime & Security, IF-1, page 1;
[61] *Smith/Holmes/Kaufmann*, Nigerian Advance Fee Fraud, Trends & Issues in Crime and Criminal Justice, No. 121
[62] *Mitchison/Wilikens/Breitenbach/Urry/Poresi,* Identity Theft – A discussion paper, 2004, page 5, available at: www.prime-project.eu/community/furtherreading/studies/IDTheftFIN.pdf.

Internet, often without charge. More sophisticated tools cost several thousand dollars.[63] Using these software tools, offenders can attack other computer systems at the press of a button. Standard attacks are now less efficient, as protection software companies analyse the tools currently available and prepare for standard hacking attacks. High-profile attacks are often individually designed for specific targets.[64] Software tools are available that enable the offender to carry out DoS attacks, design computer viruses, decrypt encrypted communication or illegally access computer systems.[65]

2.5 Summary of Literature Review

The literature reviewed indicated that some form of cyber crime regulation was in place in many, if not yet all, countries. It tried to assess how well the existing legal framework for cyber crime regulation in Uganda. However it was found that no study had been conducted to asses the adequacy of the existing legal framework in combating cyber crime in Uganda. Therefore this study evaluated the legal provisions whether they were dysfunctional in practice, or poorly observed or enforced.

---

[63] *Ealy*, A New Evolution in Hack Attacks: A General Overview of Types, Methods, Tools, and Prevention, available at: www.212cafe.com/download/e-book/A.pdf.

[64] The Crimeware Landscape: Malware, Phishing, Identity Theft and Beyond, page 23 *et seq.*, available at: www.antiphishing.org/reports/APWG_CrimewareReport.pdf; *Berg*, The Changing Face of Cybercrime – New Internet Threats create Challenges to law-enforcement agencies, Michigan Law Journal 2007, page 21, available at: www.michbar.org/journal/pdf/pdf4article1163.pdf.

[65] *Gercke,* Cyberterrorism, How Terrorists Use the Internet, Computer und Recht, 2007, page 62 *et seq.*

CHAPTER THREE

METHODOLOGY

3.1 Introduction

This chapter presents the research design, study population, sampling techniques, data collection methods, data collection instruments, validity and reliability, data collection procedure, data analysis and ethical considerations.

3.2 Research Design

The study used cross-sectional survey research design. The cross-sectional survey research design was used because the method gathers data from a relatively large number of different categories of respondents at a particular time. According to Mugenda & Mugenda (1999) this design was used when the study is aimed at collecting data from the respondents without the need to make a follow up of the same respondents thus saves time to collect the necessary information. This study employed a qualitative approach to allow for a deeper analysis of the subject under investigation (Ravallion, 2003, p.77).

3.3 Study Population

The study population was 25 respondents limited to residents of Kampala city consisted of UCC managers, law makers, lawyers and judicial officers around Kampala Capital City Authority.

3.4 Data Collection methods

Interview guides with open ended questions were administered to the UCC managers, law makers, lawyers and judicial officers because they were quite knowledgeable about cyber crime. It was a way of accessing people's perception, meaning and definitions of situations and

construction of reality (Amin, 2005). These were designed according to the theme of the study. The respondents participated in an oral interview to enable a deeper analysis. The interview method was quite flexible and could be easily adapted to a variety of situations (Sekaran, 2003).

3.5 Data Collection Instrument

With Interviews guides open ended questions were administered according to the theme of the study to the selected respondents. They were specifically administered to the UCC managers, law makers, lawyers and judicial officers. Interview guides helped to standardize the interview situation and to obtain data required to meet the specific objectives of the study (Amin, 2005). Both structured and unstructured interviews were used. The structured interviews helped to guide the researcher and kept the respondents on the subject (Amin, 2005). The unstructured interview helped solicit for more in depth information, first hand information and opinions. The interviews helped to enrich the research findings by providing more information (Mugenda & Mugenda, 1999).

3.6 Data Analysis

Qualitative data responses collected through interviews was analyzed using the content analysis technique. Here the responses were transcribed into themes and categories, in order to answer the research questions set. Detailed information was scrutinized, analysed, collected and presented in form of paraphrases or quoted upon permission of the respondents. This analysis was done manually and responses were summarised in a narrative form as a representation of the major findings of the study.

3.7 Ethical Consideration

Permission to do the study was sought from Kampala International University. The researcher first sought the consent of the respondents to conduct the study. Strict confidentiality was observed. Names of study participants were not recorded on the questionnaires and interview guides.

CHAPTER FOUR

PRESENTATION OF FINDINGS

4.1 Introduction

This chapter presents, analyzes and interprets the findings on the adequacy of the Cyber crime legal framework in Uganda. The presentation is made along the following themes; elements of cyber crime and the gaps in the cyber crime legal framework in Uganda. Analysis and interpretation are presented following the findings.

4.2 Response Rate

The researcher ascertained the nature of the different respondents and found out that out of a sample size of 25 people, 22(88%) people managed to respond to the interviews while 2(12%) were not in position. This lack of response from the respondents may be attributed to factors like failure to get time due to their tight work schedules. This feedback from the respondents (88%) was enough to facilitate this study.

4.3 Elements of cyber crime in Uganda

The study found that illegal access or hacking is one of the leading cyber crimes in the Uganda. Respondents indicated that this crime is rampant on social media accounts especially Facebook and emails such as yahoo and Google personal accounts.

The study revealed that data interference is a cyber crime that is common in Uganda, majority of respondents said that offenders can violate the integrity of data and interfere with them by deleting, suppressing or altering computer data through the use of computer viruses which has affected them through the losses of data and financial losses.

This study found that distribution of pornographic material is a very serious cyber crime occurring especially among the young youthful population of Uganda. One key informant interviewed said "*After the distribution of internet and the advance of computers and smart phones, access to pornographic material has become easy even for minors.*" This implies erotic material is a common cyber crime in the country.

This study revealed that computer-related fraud is one of the most popular crimes on the Internet in Uganda, respondents indicated that offender to use automation and software tools to mask criminals' identities and cheat un suspecting members of the public colossal sums of money through trickery activities such as promising delivery of goods after effecting payments online.

Additionally among the forms of cyber crime that were found to have a high prevalence rate within Ugandan organisations include Fraud Committed by the Consumer, Business Misconduct, Asset Misappropriation, Cybercrime and Bribery and Corruption. Business Conduct/Misconduct refers to frauds or deception by companies upon the market or general public. It involves deceptive practices associated with the manufacturing, sales, marketing or delivery of a company's products or services to its clients, consumers or the general public. It is the second most prevalent form of economic crime in Uganda. Whereas Cybercrime has only the third highest incidence rate in Uganda at 31% (tying with Asset Misappropriation), it continues to be one of the biggest potential threats to organizations in the future. At 30%, Cybercrime scored the highest among Uganda's respondents as the form of economic crime likely to be most disruptive to their organizations in the next 24 months, both monetarily and otherwise.

4.4 The gaps in the cyber crime legal framework in Uganda

The purpose of this objective was to identify the gaps in the cyber crime legal framework in Uganda. A judicial officer interviewed said

> "Uganda has a number of legislations in place, which address Internet misuse (the Computer Misuse Act5, the Electronic Signatures Act6, The Electronic Transactions Act7, Electronic Misuse Act, the Access to Information Act8 and the Regulation of Interception of Communications Act9). Different stakeholders were involved in drafting these legislations for example the Ministry of Information and Communications Technology (MoICT) in conjunction with Ministry of Justice and Constitutional Affairs (MoJCA), Uganda Communications Commission and National Information Technology Authority (NITA-U) of Uganda jointly coordinated the drafting of the Data Protection and Privacy Bill"

In agreement another key informant said

> "There are existing laws which are being applied to prosecute digital crimes in Uganda today. Some of these prosecution cases have been based on the Computer Misuse Act, the Electronic Signature Act, and the Electronic Misuse Act, and applied as cyber Laws.''

From the findings it was found that Cyber criminals in Uganda take advantage of weaknesses in cybercrime legislation and the nascent systems of law enforcement leading to a proliferation of illicit activities. On this respondents noted that mainly cross- border prosecutions of Cybercrime are still a challenge for law enforcement agencies. They added that the differences in laws between Uganda (where the victim might be residing) and other countries (where the crime might have originated) were a major limitation. This therefore implies gaps in the laws on cyber crime in Uganda.

Another key respondent interviewed said

> "With the growing number of people connected to the Internet, the number of targets and offenders increases therefore proper legislation is the foundation for the investigation and prosecution of cybercrime. However, lawmakers must

continuously respond to Internet developments and monitor the effectiveness of existing provisions, especially given the speed of developments in network technology".

Such a finding implies the cyber crime legislations are not catching up with the speed of change in the levels of technologies and there after cyber crime globally and in Uganda.

A magistrate interviewed said that Section 5 (3) of the National Information Technology Authority, Uganda Act, 2009, mandates NITA-Uganda to co-ordinate, supervise and monitor the utilization of information technology in the public and private sectors, however this provision can be interpreted to threaten privacy and freedom of expression by allowing supervising and monitoring, the scope of which is not clearly and unambiguously defined. Moreover, it is unclear if by "utilization" of information technology is understood access to Internet on a more general level or a more content-specific use of the Internet. The latter interpretation would open up considerable powers to supervise and monitor e.g. individuals' Internet traffic.

Another judicial officer commented that Section 5 (4) of the National Information Technology Authority, Uganda Act, 2009, mandates NITA-Uganda to regulate and enforce standards for information technology hardware and software equipment procurement in all Government Ministries, departments, agencies and parastatals, however this provision opens up for the NITA-U to stipulate standards for hardware and software in public computers that can restrict freedom of expression and privacy. It could for example be interpreted to allow for regulations requiring installation of filters, blocking mechanisms or spyware in public computers. The judicial officer added that Section 22 of the National Information Technology Authority, Uganda Act, 2009 stipulates that confidentiality is the main rule as regards for example data set or part of data stored in a computer or any other electronic media. However, this does not affect the fact that the

NITA-U as a public authority has a possibility to get access to personal data concerning individuals.

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.

Another advocate interviewed said

> "The Ugandan cyber legislation gives government and its agencies unlimited powers with regard to procuring surveillance equipment and criminalizing gadgets (computers) as well as Internet content. Their powers range from illegally ordering Internet service providers to block certain social platforms to signing secret memorandum of understanding among government agencies to share information about Internet users and published content in order to enforce the Ugandan cyber legislation. Harassment of online activists by police has also been reported"

In agreement with the above another advocate interviewed commented that 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. All these are gaps that are clearly visible in the Ugandan legal framework on cyber crime.

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* and *Uganda Vs Dr. Aggrey Kiyingi* cases that relied on electornic evidence. In *Kato Kajubi* following a retrial, the accused was convicted. Following the terrorist attack on Kampala on 11th July 2010, the police with the help of the 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 cyber crime 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.[66] Finally, there is insufficient knowledge about the law and inadequate sensitization of the public and other potential victims of cybercrime.

Specific departments are needed within national law-enforcement agencies, which are qualified to investigate potential cybercrimes. The development of computer emergency response teams (CERTs), computer incident response teams (CIRTs), computer security incident response teams (CSIRTs) and other research facilities have improved the situation.

On enforcement and implementation of laws, the study found that there is no centralized budget for cyber security. Every Ministry allocates its budget separately and depends on previous experience and future plans to allocate budget for cyber security. In agreement, an advocate interviewed said

[66] P. Mwaita and M. Owor, Workshop report on effective Cybercrime legislation in Eastern Africa, Dar es salaam, Tanzania, 22-24 August 2013.

> "There is limited capacity by the law enforcement agencies to investigate computer-related crimes, in-line with known global best practices. This has been attributed largely due to lack of sufficient technical expertise in digital forensic in Cybercrime cases."

A key informant said that the National Information Security Strategy (NISS) does not provide specific actionable directives that relate to cyber security. He added "*Risks may exist but the strategies are not aligned with national goals; at the moment every Agency has their own list of incidents and have different priorities. Different institutions place different levels of importance to technology, depending on their priorities.*"

From the review of document, the study established that Uganda does not have an official list of Critical National Infrastructure (CNI) sectors in Uganda. This is mainly attributed to the lack of clear understanding of what constitutes a CNI sector list and the difficulty in recognizing what needs to be protected. Experts believe they generally have the ability to recognize what is important for Uganda and will take the appropriate & necessary measures to protect Uganda's CNI. The National Information Security (NIS) Policy defines the concept of critical information infrastructure (CII), but does not clear address the CNI issue in detail. According to the National Information Security Policy ''*the information and communication technologies (ICTs), that form CII, increasingly operate and control critical national sectors such as health, water, transport, communications, government, energy, food, finance and emergency services*''. This is an areas that needs to be developed further.

4.4 Conclusion

Overall, cyber security capacity in Uganda lies between an initial and formative stage of maturity. This expresses a state of maturity where some features have begun to grow and be formulated, but may be ad-hoc, while these can be clearly evidenced.

transactions in Uganda; and there was limited capacity by the law enforcement agencies to investigate computer-related crimes in Uganda.

5.3 Conclusions

5.3.1 Elements of cyber crime in Uganda

Basing on the findings, this study concluded that illegal access or hacking is one of the leading cyber crimes; data interference; the use of computer viruses; and distribution of pornographic material; and computer-related fraud was one of the most popular crimes on the Internet in Uganda.

5.3.2 Gaps in the cyber crime legal framework in Uganda

This study concluded that the laws on cyber crimes in the country are quite many but have a number of loopholes that can be manipulated by criminals to cause loss of colossal amounts of money from the people of Uganda. Nevertheless even where the laws seem to be adequate, there are persistent issues with enforcement of such laws.

5.4 Recommendations

Basing on the study findings, the study recommends that in addition to the criminalization of Cybercrime and the improvement of the ability of law enforcement to combat Cybercrime crime preventions measures need to be developed. Within the process of developing such measures, that can range from technical solutions to increasing user awareness, it is important to identify those groups that require specific attention such as youth, technologically challenged people (such as people from isolated villages that are technologically unaware) and women.

The study recommends that crime prevention measures should also apply to more advanced users and technology-affiliate players such as critical infrastructure provider (such as the tourism or financial sector). The debate about necessary measures should include the whole range of instruments such as awareness raising, making available and promoting free of charge protection technology (such as anti-virus software) and the implementation of solutions that enable parents to restrict the access to certain content. Such measures should ideally be available at the time of an introduction of a service/technology and maintained through out it's operation.

To ensure a wider reach of such measure a broad range of stakeholders should be involved that range from Internet Service Provider to governments and regional bodies and explore various sources for funding.

It was noted that there is a need for Uganda to have a National Cyber security Strategy in order to identify and include other national risks and priorities areas of Cybersecurity. For example, the current rick register needs to be enhanced so that it can include all cri tical sectors in Uganda. It was suggested that NITA-U could coordinate the update, review and collation of all sectorial risk register in the country. There are general risks, which can be listed as internal and external at national level and their respective impacts needs to be considered.

In regard to Substantive and Procedural law the parliament of Uganda should amend the Evidence Act to expressly provide for the admissibility of electronic evidence; amend the Computer Misuse Act to impose an obligation on citizens/persons to report any incidents of cyber crime; amend Section 9 Computer Misuse Act - on preservation orders, to fit within the

confines of the relevant provisions in the Budapest Convention. The section should be broadened to cover content data as data that may be subject to preservation orders.

References

Laws

The Anti-Terrorism Act, 2002

The National Information Technology Authority, Uganda Act, 2009

The Regulation of Interception of Communications Act, 2010

The Electronic Signatures Act, 2011

The Computer Misuse Act, 2011

The Electronic Transactions Act, 2011

The Uganda Communications Act, 2013

The Anti-Pornography Act, 2014.

Chapter 104 and 106 of the Laws of Uganda, Revised Edition (2000)

Journal Articles

P. Mwaita and M. Owor, Workshop report on effective Cybercrime legislation in Eastern Africa, Dar es salaam, Tanzania, 22-24 August 2013.

R.K.Chaubey, *"An Introduction to Cyber Crime and Cyber law"*, Kamal Law House, 2012

Uganda Law Reform Commission: A Study Report on Electronic Transactions Law, ULRC Publication No. 10 of 2004.

Humphrey, H. and Water, T.: 2010, *Solid Waste Disposal, Kampala.* Revised Draft Report Seven Towns Project by GTZ/World Bank. Ministry of Water and Mineral Development and Ministry of Local Government.

Aghatise E. Joseph, "Cyber Crime Definition", Cyber Crime Research Centre (Last modified on June 28, 2006), *available at:* http://www.scribd.com/document/195552552/Cybercrime-Definition

David Decary Hetu and Carlo Morselli, "Gang Presence in Social Network Sites", *International Journal of Cyber Criminology,* vol. 5 No. 2, July- Dec., 2011, p. 876, *available at:* http:// www.cybercrimejournal.com/davidcarlo2011julyijcc.pdf

M. Dasgupta, *Cyber Crime in India- A Comparative Study*, 2009, p.8.

Levy, Hackers, 1984; Hacking Offences, Australian Institute of Criminology, 2005, available at: www.aic.gov.au/publications/htcb/htcb005.pdf;

Sieber, Council of Europe Organised Crime Report 2004, page 65.

Biegel, Beyond our Control? The Limits of our Legal System in the Age of Cyberspace, 2001, page 231 *et seq.*

Musgrove, Net Attack Aimed at Banking Data, Washington Post, 30.06.2004.

BBC News, "UN's website breached by hackers", available at: http://news.bbc.co.uk/go/pr/fr/-/2/hi/technology/6943385.stm

Jakobsson, The Human Factor in Phishing, available at: www.informatics.indiana.edu/markus/papers/aci.pdf; *Gercke*, Computer und Recht 2005, page 606.

Braverman, VoIP: The Future of Telephony is now...if regulation doesn't get in the way, The Indian Journal of Law and Technology, Vol.1, 2005, page 47

Kang, Wireless Network Security – Yet another hurdle in fighting Cybercrime, in Cybercrime & Security, IIA-2, page 6 *et seq.*

Kabay, A Brief History of Computer Crime: An Introduction for Students, 2008, page 23, available at: www.mekabay.com/overviews/history.pdf.

Power, 2000 CSI/FBI Computer Crime and Security Survey, *Computer Security Journal*, Vol. 16, No. 2, 2000, page 33 *et seq.*

Reports

Annual Report to Congress on Foreign Economic Collection and Industrial Espionage – 2003, page 1, available at: www.ncix.gov/publications/reports/fecie_all/fecie_2003/fecie_2003.pdf.

ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 30, available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.